ANALISIS DAN IMPLEMENTASI METODE *HONEYPOT* DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 3 SIBOLGA

SKRIPSI

DISUSUN OLEH

RADINAL FITRAH SITANGGANG

NPM. 1909010009

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2023

ANALISIS DAN IMPLEMENTASI METODE *HONEYPOT* DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 3 SIBOLGA

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperolah gelar Sarjana Komputer (S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

RADINAL FITRAH SITANGGANG
NPM. 1909010009

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2023

LEMBAR PENGESAHAN

Judul Skripsi	: Analisis dan Implementasi Metode Honeypot Dalam Penerimaan Peserta Didik Baru (PPDB) Pada SD Muhammadiyah 3 Sibolga
Nama Mahasiswa	: Radinal Fitrah Sitanggang
NPM	: 1909010009
Program Studi	: Sistem Informasi

Menyetujui

Komisi Pembimbing

(Halim Maulana, S.T., M.Kom)
NIDN. 0121119102

Ketua Program Studi	Dekan
(Martiano,S.Pd., S.Kom., M.Kom)	**(Dr. Al-Khowarizmi,.S.Kom., M.Kom)**
NIDN. 0128029302	**NIDN. 0127099201**

PERNYATAAN ORISINALITAS

ANALISIS DAN IMPLEMENTASI METODE HONEYPOT DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 3 SIBOLGA

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing – masing disebutkan sumbernya.

Medan, Agustus 2023

Yang membuat pernyataan

Radinal Fitrah Sitanggang
NPM. 1909010009

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini :

Nama	: Radinal Fitrah Sitanggang
NPM	: 1909010009
Pogram Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bebas Royalti Non-Eksekutif *(Non-Exclisive Royalty Free Right)* atas penelitian skripsi saya yang berjudul :

ANALISIS DAN IMPLEMENTASI METODE HONEYPOT DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 3 SIBOLGA

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempubiikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atas sebagai pemilik hak cipt.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, Agustus 2023

Yang membuat pernyataan

Radinal Fitrah Sitanggang
NPM. 1909010009

RIWAYAT HIDUP

DATA DIRI

Nama Lengkap	: Radinal Fitrah Sitanggang
Tempat dan Tanggal Lahir	: Sarudik, 1 Januari 2001
Alamat Rumah	: Jl. Padang Sidempuan Lingk 3 Sarudik, Kab. Tapanuli Tengah, Sumatera Utara
Telepon/Faks/HP	: 082161133547
E-mail	: fitrastg64@gmail.com

DATA PENDIDIKAN

SD	: SD Negeri 152977 Sarudik	TAMAT : 2014
SMP	: SMP Negeri 1 Sibolga	TAMAT: 2017
SMK	: SMK Putra Harapan Tapanuli Tengah	TAMAT: 2019

KATA PENGANTAR

Assalamualaikum Wr.Wb

Segala Puji dan syukur dipanjatkan atas kehadirat Allah Swt Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayah-Nya sehingga Penulis dapat menyelesaikan Proposal Skripsi tepat pada waktunya. Proposal ini dibuat berdasarkan hasil dari Riset yang dilakukan di SD Muhammadiyah 3 Sibolga.

Proposal ini merupakan salah satu syarat yang harus dipenuhi dan dilaksanakan semua mahasiswa/i UMSU untuk menyelesaikan perkuliahan program SI. Proposal Skripsi ini dapat disusun penulis pada SD Muhammadiyah 3 Sibolga.

Dalam menulis proposal ini penulis banyak menerima bantuan, bimbingan, serta petunjuk dari berbagai pihak,baik langsung maupun tidak langsung,pada kesempatan iniPenulis ingin mengucapkan terima kasih kepada semua pihak yang telah memberi do'a, motivasi, dukungan dan semangat. Pada kesempatan ini disampaikan rasa homat dan terima kasih kepada :

1. Buat kedua orang tua saya yang selalu memberikan kasih sayang yang tak terhingga, bimbingan, perhatian, serta do'a, sehingga penulis termotivasi dan semangat menyusun skripsi ini.

2. Bapak Prof. Dr. Agussani, M.A.P selaku Rektor Universitas Muhammadiyah Sumatera Utara.
3. Bapak Al – Khowarizmi, S.Kom, M.Kom selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara.
4. Bapak Halim Maulana, S.T, M.Kom selaku Wakil Dekan I Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara dan sebagai Dosen Pembimbing pada penulisan skripsi ini yang dengan ikhlas telah meluangkan waktu untuk meberikan pengarahan dan bimbingan yang bermanfaat kepada penulis hingga selesainya skripsi ini.
5. Bapak Dr Lutfi Basit, S.Sos, M.I.Kom selaku Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera.
6. Bapak Martiano, S.Kom, M.Kom selaku ketua Program Studi Sistem Informasi Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera.
7. Ibu Yoshida Sari, S.Kom, M.Kom, selaku Sekretaris Program Studi Sistem Informasi Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera.
8. Bapak dan Ibu dosen serta seluruh sfaf pegawai biro yang banyak membantu penulisan dalam memberikan informasi akademik dan membantu penulis selama menjalankan pendidikan di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera.

9. Kepada teman – teman seperjuangan peneliti jurusan Sistem Informasi Universitas Muhammadiyah Sumatera Utara stambuk 2019 serta seluruh pihak yang tidak –peneliti sebutkan satu persatu. Peneliti hanya bisa berharap semoga Allah Subhanahu Wata'ala membalas kebaikan kalian semua. Aamiin.
10. Teman – teman Jurusan Sistem Informasi di Universitas Muhammadiyah Sumatera Utara, yang selalu memberikan dukungan dan motivasi.
11. Pihak – pihak yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan dan masih terdapat kekurangan serta kesalahan dari materi ataupun cara penyajiannya. Oleh karena itu, Penulis mengharapkan saran dan kritik dari semua pihak demi kesempurnaan laporan ini. Semoga laporan ini dapat bermanfaat dan berguna bagi para pembaca.

Wassalamualaikum Wr.Wb

Medan, April 2023

Penulis

RADINAL FITRAH SITANGGANG
1909010009

ABSTRAK

ANALISIS DAN IMPLEMENTASI METODE HONEYPOT DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 3 SIBOLGA

Radinal Fitrah Sitanggang
Sistem Informasi
Fitrastg64@gmail.com

Penelitian ini mengkaji implementasi metode *honeypot* dalam Sistem Penerimaan Peserta Didik Baru (PPDB) berbasis online di SD Muhammadiyah 03 Sibolga, pada permasalahan yang mungkin muncul selama proses pendaftaran namun juga dengan sistem yang aman dari serangan siber. Tujuannya adalah untuk menganalisis bagaimana sistem PPDB tersebut dapat berjalan aman dengan menggunakan sistem keamanan honeypot. Penelitian ini dilakukan melalui analisis data dari proses PPDB online yang telah berjalan, dengan menggunakan teknik studi dokumentasi dengan mengumpulkan data pada log HiHAT, teknik analisis data dilakukan secara kualitatif dengan cara berulang-ulang dan berkesinambungan antara pengumpulan dan analisis data. Hasil penelitian menunjukkan bahwa honeypot berhasil mendeteksi serangan *SQL Injection*, *XSS*, *INJECT*, dan *DIR-Change* dengan tingkat deteksi bervariasi. Selain itu, implementasi PPDB Online di SD Muhammadiyah 03 Sibolga memberikan kontribusi positif dalam mengatasi kendala administratif dan menarik minat calon peserta didik baru untuk mendaftar. Penelitian ini juga membuktikan bahwa metode *honeypot* merupakan solusi efektif dalam menghadapi risiko keamanan, terutama *SQL Injection* dan *XSS*. Program *HiHAT* yang digunakan untuk mengumpulkan data serangan pada honeypot juga berperan penting dalam menganalisis dan meningkatkan keamanan sistem. Penelitian ini memberikan kontribusi praktis bagi perbaikan keamanan PPDB serta panduan untuk menghadapi ancaman serupa di institusi sejenis.

Kata kunci: PPDB Online, *honeypot*, *SQL Injection*, *XSS*, Penerimaan Peserta Didik Baru, High Interaction Honeypot Analysis Toolkit, *HiHAT*

ABSTRACT

ANALYSIS AND IMPLEMENTATION OF THE HONEYPOT METHOD IN ADMISSION OF NEW STUDENTS (PPDB) AT SD MUHAMMADIYAH 3 SIBOLGA

Radinal Fitrah Sitanggang
Information Systems
Fitrastg64@gmail.com

This study examines the implementation of the honeypot method in the online-based New Student Acceptance System (PPDB) at SD Muhammadiyah 03 Sibolga, on problems that may arise during the registration process but also with a system that is safe from cyber-attacks. The aim is to analyze how the PPDB system can run safely by using a honeypot security system. This research was conducted through data analysis from the PPDB online process that had been running, using a documentation study technique by collecting data in the HiHAT log, data analysis techniques were carried out qualitatively iteratively, and continuously between data collection and analysis. The results showed that the honeypot was successful in detecting SQL Injection, XSS, INJECT, and DIR-Change attacks with varying levels of detection. In addition, the implementation of PPDB Online at SD Muhammadiyah 03 Sibolga made a positive contribution in overcoming administrative obstacles and attracting the interest of prospective new students to register. This research also proves that the honeypot method is an effective solution in dealing with security risks, especially SQL Injection and XSS. The HiHAT program used to collect attack data on honeypots also plays an important role in analyzing and improving system security. This research provides practical contributions to improving PPDB security as well as guidance for dealing with similar threats in similar institutions.

Keywords: PPDB Online, honeypot, SQL Injection, XSS, Admission of New Students, High Interaction Honeypot Analysis Toolkit, HiHAT

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kemajuan dan perkembangan teknologi informasi saat ini telah berpengaruh pada manusia, termasuk bidang komunikasi dan teknologi dan sudah merupakan bagian dari kehidupan manusia yang tidak dapat dipisahkan. Dan dengan kemajuan teknologi informasi dan komunikasi maka akan memunculkan masalah baru dalam hal keamanan informasi. Mengingat betapa rentanya dampak negatif yang diberikan, sehingga perlu diterapkan prosedur keamanan pada informasi khususnya informasi berupa teks, yang merupakan bentuk penting dalam informasi digital saat ini.

Penerimaan peserta didik baru merupakan salah satu program kegiatan sekolah dan termasuk dalam perencanaan peserta didik dalam lingkup manajemen peserta didik. Penerimaan peserta didik baru merupakan salah satu kegiatan manajemen peserta didik terpenting yang diadakan oleh sekolah-sekolah baik negeri maupun swasta, karena dengan masuknya peserta didik baru pada sebuah sekolah akan membawa dampak positif bagi sekolah tersebut dan proses PPDB dilakukan dalam sistem pendidikan di Indonesia dan dilakukan setiap tahun untuk menentukan siswa yang diterima di sekolah tersebut. Penerimaan Peserta Didik Baru (PPDB) merupakan hal yang sangat penting dalam suatu lembaga pendidikan, salah satu sistem PPDB yaitu dengan *online*.

Penerimaan peserta didik baru merupakan kegiatan rutin diselenggarakan setiap tahun oleh sekolah. Kegiatan ini mencakup proses pendaftaran hingga penyeleksian disertai syarat-syarat yang berlaku di sekolah.

Berikut adalah beberapa alasan mengapa PPDB penting untuk SD Muhammadiyah 03 Sibolga :

1. Merupakan langkah awal dalam membangun lingkungan pendidikan yang berkualitas: PPDB memungkinkan sekolah untuk memilih calon siswa yang sesuai dengan visi, misi, dan kebijakan pendidikan sekolah. Dengan menerapkan proses seleksi yang baik, sekolah dapat memastikan bahwa siswa yang diterima memiliki kemampuan dan potensi yang memadai untuk belajar di sekolah tersebut. Hal ini berkontribusi pada terbentuknya lingkungan pendidikan yang berkualitas.
2. Menjamin keadilan dalam pendidikan: PPDB membantu memastikan bahwa proses penerimaan siswa baru dilakukan secara adil dan transparan. Dengan adanya mekanisme seleksi yang objektif, setiap calon siswa memiliki kesempatan yang sama untuk diterima di sekolah. Ini menghindari penyelewengan dan memastikan bahwa semua calon siswa memiliki hak yang sama dalam mendapatkan pendidikan yang berkualitas.
3. Mengoptimalkan alokasi sumber daya: PPDB memungkinkan sekolah untuk merencanakan alokasi sumber daya yang tepat, seperti tenaga pengajar, ruang kelas, fasilitas, dan kurikulum. Dengan mengetahui jumlah dan profil calon siswa, sekolah dapat menyesuaikan kebutuhan pendidikan dan mengoptimalkan penggunaan sumber daya yang tersedia.

4. Memperkuat identitas sekolah: Melalui PPDB, sekolah memiliki kesempatan untuk menarik siswa yang sejalan dengan identitas dan keunggulan sekolah. Proses seleksi yang baik dapat membantu sekolah menarik siswa dengan minat, bakat, dan tujuan belajar yang sejalan dengan program sekolah. Hal ini berpotensi memperkuat citra dan reputasi sekolah di masyarakat.
5. Menghindari overload kapasitas: Dalam beberapa sekolah yang memiliki keterbatasan fasilitas dan kapasitas, PPDB menjadi penting untuk mengatur jumlah siswa yang diterima agar tetap sesuai dengan daya tampung sekolah. Dengan adanya PPDB yang terstruktur, sekolah dapat menghindari beban yang berlebihan pada infrastruktur dan memastikan kualitas pembelajaran yang optimal bagi semua siswa.

Secara keseluruhan, PPDB memiliki peran penting dalam membangun sekolah yang berkualitas, menjaga keadilan dalam pendidikan, mengoptimalkan sumber daya, memperkuat identitas sekolah, dan menghindari overload kapasitas. Dengan penerapan PPDB yang baik, sekolah dapat menciptakan lingkungan pendidikan yang mendukung pertumbuhan dan perkembangan optimal bagi semua siswa.

Pendayagunaan teknologi informasi pada alur proses PPDB adalah aksi nyata dalam memfasilitasi terbangunnya good governance dalamdunia pendidikan. Hal tersebut sesuai dengan peraturan pemerintah melalui Kemdikbud menetapkan Permendkbud nomor 17 Tahun 2017 yang mengatur tentang PPDB. PPDB dipilih disebabkan karena PPDB termasuk dalam inputan awal dari pengelolaan manajemen pendidikan yang terdapat pada

sekolah dan apabila implementasinya masih secara manual berdampak pada proses yang tidak efektif (Anton Yuhada, hal: 48, 2023).

Menurut (Marlinda Sanglise, 2022), Berdasarkan hasil dan pembahasan dari penelitian terhadap sistem informasi penerimaan peserta didik baru berbasis web pada SD Inpres Kalikodok, panitia PPDB mengelola pelaksanaan program PPDB dengan baik seperti pendaftaran peserta, dan hasil seleksi peserta dengan lebih efisien, baik dalam hal waktu, tempat, biaya, tenaga maupun kecurangan yang terjadi dalam pelaksanaan program penerimaan peserta didik baru.

Hasil dari penelitian (Al-Khowarizmi, 2020), Melalui pengembangan aplikasi berbasis web, sekolah mengatasi tantangan PPDB saat Pandemi COVID-19. Hal ini meminimalkan pertemuan fisik dan sesuai dengan pedoman Sosial Distancing yang diberikan pemerintah. Tujuannya adalah menjaga minat calon PPDB untuk mendaftar di Sekolah Dasar Alam Semangat Bangsa dan TK Kartini. Selama periode 7 hari setelah peluncuran aplikasi, tercatat peningkatan empat kali lipat dalam jumlah pendaftar dibandingkan sebelumnya.

Kemudian Menurut (Asri Ulfah Wulan Sari,) Sistem Penerimaan Peserta Didik Baru Online bagus bila diterapkan, karena semuanya akan jadi

Namun, dalam proses PPDB, terdapat risiko keamanan informasi yang harus diatasi oleh sekolah untuk menjaga kerahasiaan data siswa dan memastikan integritas proses tersebut. *Honeypot* adalah suatu metode keamanan komputer yang dirancang untuk menarik dan memantau aktivitas potensial yang mencurigakan atau serangan siber dengan cara menyediakan sistem atau aplikasi yang tampaknya rentan terhadap serangan. *Honeypot* berfungsi sebagai perangkap

yang menarik perhatian penyerang, sehingga memungkinkan pengamat keamanan untuk memahami teknik, niat, dan alat yang digunakan oleh penyerang.

Salah satu cara untuk mengatasi risiko keamanan informasi dalam proses PPDB adalah dengan menggunakan metode *honeypot*. Metode ini bekerja dengan menarik perhatian penyerang ke area yang telah dipersiapkan secara sengaja, sehingga dapat memantau dan mengumpulkan informasi tentang serangan yang dilakukan. Implementasi metode *honeypot* pada proses PPDB ini dapat membantu sekolah untuk melindungi data siswa dan mengatasi ancaman keamanan yang mungkin terjadi.

Maka dari itu penulis mengambil judul Skripsi "**Analisis dan Implementasi metode *honeypot* dalam penerimaan peserta didik baru (PPDB) pada SD Muhammadiyah 3 Sibolga**"

1.2. Rumusan Masalah

Adapun rumusan masalah yang dapat diambil dari latar belakang masalah tersebut yaitu:

1. Apakah yang dimaksud dengan metode *honeypot* dan bagaimana penerapannya dalam penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga?
2. Bagaimana hasil analisis terhadap penerapan metode *honeypot* dalam penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga?
3. Apakah implementasi metode *honeypot* dalam penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga efektif dalam mengatasi serangan siber dan memperkuat keamanan sistem?

1.3. Batasan Masalah

Agar pembahasan tidak melebar dari topik penelitian maka penulis membuat pembatasan penelitian yaitu :

1. Skripsi ini hanya membahas tentang penerapan metode *honeypot* pada sistem penerimaan peserta didik baru (PPDB) pada SD Muhammadiyah 3 Sibolga.
2. Skripsi ini hanya akan membahas tentang implementasi metode *honeypot* dalam rangka memperkuat keamanan sistem dan mengatasi serangan siber pada sistem PPDB SD Muhammadiyah 3 Sibolga.
3. Skripsi ini tidak membahas tentang metode atau teknologi lain yang dapat digunakan selain metode *honeypot* untuk memperkuat keamanan sistem.
4. Skripsi ini hanya membahas tentang penggunaan metode *honeypot* pada tingkat sistem, bukan pada tingkat jaringan atau aplikasi.

1.4. Tujuan Penelitian

Tujuan penelitian skripsi ini adalah

1. Mengetahui apa yang dimaksud dengan metode *honeypot* dan bagaimana penerapannya dalam penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga.
2. Menganalisis efektivitas penerapan metode *honeypot* dalam mengatasi serangan siber dan memperkuat keamanan sistem pada penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga.
3. Memberikan kontribusi dan solusi bagi SD Muhammadiyah 3 Sibolga dalam mengatasi masalah keamanan pada sistem penerimaan peserta didik baru (PPDB).

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Menambah wawasan dan kemampuan dalam mengaplikasikan ilmu-ilmu Teknik Informatika, khususnya dalam bidang keamanan data.
2. Memberikan pemahaman tentang teknologi *honeypot* dalam mencegah serangan keamanan.
3. Menjadi referensi bagi penelitian selanjutnya dalam mengimplementasikan metode *honeypot* pada sistem yang berbeda.

BAB 2

LANDASAN TEORI

2.1. Landasan Teori

2.1.1. Analisis

Analisis adalah suatu proses yang digunakan untuk memecah suatu entitas menjadi bagian-bagian yang saling berhubungan. Analisis melibatkan kegiatan berpikir yang bertujuan untuk menguraikan keseluruhan menjadi komponen-komponen terpisah. Hasil dari analisis ini memungkinkan kita untuk mengenali tanda-tanda yang melekat pada setiap komponen, mengidentifikasi hubungan antara komponen-komponen tersebut, serta memahami fungsi masing-masing komponen dalam konteks keseluruhan yang terintegrasi. Dengan demikian, analisis membantu kita memahami lebih dalam tentang struktur dan makna di balik suatu entitas atau konsep.

2.1.2. PPDB

Proses Penerimaan Peserta Didik Baru (PPDB) merupakan tahapan yang terdapat dalam lembaga pendidikan, seperti sekolah, yang memiliki tujuan untuk mengidentifikasi dan memilih calon siswa yang memenuhi kriteria yang telah ditetapkan oleh lembaga tersebut. PPDB umumnya melibatkan beberapa langkah, termasuk proses pendaftaran, tes seleksi, dan pengumuman hasil penerimaan siswa baru. Seiring dengan meningkatnya jumlah calon siswa baru, proses pengolahan informasi terkait PPDB, yang mencakup tahap penerimaan, pengolahan data, dan pengumuman hasil, menjadi semakin kompleks dan memakan waktu.

Menurut (Al-Khowarizmi, 2020), PPDB merupakan kegiatan rutin sekolah pada tiap tahunnya.untuk mendapatkan calon peserta didik baru diperlukan media promosi yang tepat agar dapat di terima oleh masyarakat banyak. Namun untuk melakukan promosi pada sekolah harus mampu bersaing dengan sekolah-sekolah lainnya yang mana persainggan sangat sengit pada media online. Sosial media dan website termasuk dalam upaya bersaing untuk mendapat calon perseta didik baru.

Sedangkan menurut (Ramdhani & Susetyo, 2020), PPDB merupakan suatu kegiatan atau proses pertama dalam sebuah kegiatan bagi lembaga sekolah, dimana PPDB tersebut melalui seleksi yang telah ditentukan oleh pihak sekolah kepada calon peserta didik baru atau siswa. PPDB dalam sebuah lembaga pendidikan merupakan hal yang sangat penting, karena dengan adanya proses PPDB yang dikelola secara profesional akan memberi keuntungan sekolah dalam bidang pendaftaran yang nantinya akan menjadi peserta didik pada sekolah tersebut. sehingga calon peserta didik yang masuk menjadi peserta didik baru secara otomatis operasional sekolah akan memberikan keuntungan dan proses belajar mengajar yang akan dilaksanakan akan berjalan dengan lancar, karena pembelajaran merupakan satu kesatuan antara peserta didik dan tenaga pendidik.

Penerimaan Peserta Didik Baru (PPDB) memang menjadi agenda rutin setiap tahun bagi institusi pendidikan untuk menerima siswa baru di lingkungannya. Namun, sering kali lembaga-lembaga ini menghadapi tantangan dalam mengelola aspek administrasi terkait siswa baru. Beberapa masalah yang muncul dalam hal administrasi meliputi kesulitan dalam penginputan data siswa baru dan ketidakrapihan dalam penyimpanan data, yang mengakibatkan kesulitan dalam pencarian informasi.

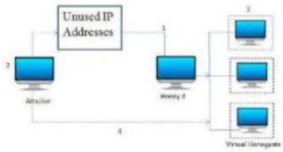
Tujuan dari proses penerimaan peserta didik baru adalah untuk memperlancar dan menyederhanakan proses pendaftaran siswa baru, pengumpulan data, serta penempatan siswa ke dalam kelas yang sesuai. Hal ini bertujuan agar semua proses dapat dijalankan dengan efisien, teratur, dan tepat waktu, dengan mematuhi persyaratan yang telah ditetapkan oleh sekolah. PPDB juga merupakan kewajiban rutin bagi pihak sekolah dan Dinas Pendidikan setiap tahun saat memasuki tahun ajaran baru. Dalam proses PPDB, seringkali terdapat tahapan seleksi administrasi dan akademis bagi calon siswa yang ingin melanjutkan ke jenjang pendidikan yang lebih tinggi. Hal ini dilakukan untuk memastikan bahwa siswa yang diterima memiliki kualifikasi yang sesuai dengan persyaratan yang telah ditetapkan.

2.1.3. Honeypot

Honeypot adalah sebuah teknologi keamanan yang digunakan dalam server web dengan tujuan untuk mengidentifikasi, menemukan celah keamanan, dan merekam aktivitas penyusupan dalam konteks teknologi informasi. Fungsinya sangat bervariasi, dan umumnya dapat dikelompokkan menjadi dua kategori utama: honeypot interaksi rendah (*low interaction honeypot*) dan honeypot berinteraksi tinggi (*high interaction honeypot*).

Low Interaction Honeypot dirancang untuk meniru infrastruktur jaringan pada server asli. Penyerang hanya dapat memeriksa dan terhubung ke satu atau beberapa port tertentu. Sebagai contoh, kita dapat membuat layanan palsu yang mendengarkan dan mencatat setiap koneksi yang datang ke suatu port tertentu. Honeypot dengan interaksi rendah ini memungkinkan adanya komunikasi satu arah, karena hanya mendengarkan dan mencatat koneksi tanpa memberikan

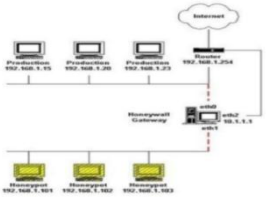
respons balik kepada koneksi tersebut. Hal ini akan mengurangi resiko karena tidak akan ada sistem yang akan diambil alih Arsitektur ini dapat dilihat pada gambar dibawah ini.



Gambar 2.1. *Arsitektur Low Interaction Honeypot* (Sumber: Anggeriana)

High Interaction Honeypot adalah jenis honeypot yang beroperasi dengan sistem operasi lengkap, memungkinkan interaksi langsung dengan peretas tanpa ada batasan yang menghambat interaksi tersebut. Dengan menghilangkan batasan-batasan ini, risiko yang dihadapi menjadi lebih tinggi karena peretas dapat memperoleh akses ke tingkat hak akses tertinggi (root). Pada saat yang sama, peluang untuk mengumpulkan informasi juga meningkat, termasuk pola serangan, perangkat lunak yang digunakan, motif peretas, dan lain sebagainya.

Pengoperasian high interaction honeypot memerlukan pemantauan yang konstan. Hal ini diperlukan karena jika honeypot tersebut berhasil diretas dan dimanfaatkan oleh penyerang, maka honeypot itu sendiri bisa menjadi ancaman bagi seluruh jaringan. Sebagai contoh, gambaran arsitektur high interaction honeypot dapat dilihat pada ilustrasi di bawah ini.



Gambar 2.2 *Arsitektur High Interaction Honeypot*
(Sumber: Anggeriana)

Perbandingan *Low Interaction Honeypot* dan *High Interaction Honeypot* Masing-masing kategori dari *honeypot* tersebut memiliki keunggulan, untuk *low interaction honeypot* yaitu, skala pembangunan dan skala pemeliharaan kategori sederhana, karena *low interaction honeypot* didesain hanya untuk mengumpulkan informasi penyerang dan menjadi target utama penyerang sehingga dampak resiko minimum dari sistem utama dapat dicapai. Sedangkan keunggulan dari *high interaction honeypot* yaitu, merekam dan mengumpulkan informasi lebih spesifik dari *low interaction honeypot*, behavior penyerang dan penelusuran jaringan *protocol* secara spesifik dari penyerang saat terjadinya insiden penyerangan atau penyusupan.

Tabel 2.1. Perbandingan Low Interaction dan High Interaction

Low Interaction Honeypot	***High Interaction Honeypot***
1. Mensimulasi sistem operasi dan servis.	1. Sistem Operasi dan servis sungguhan tanpa simulasi
2. Mudah diinstal dan *deploy*, konfigurasi software dapat anya sederhana.	2. Menangkap informasi lebih banyak.
3. Resiko minimal, simulasi mengontrol apa yang bisa dilakukan penyusup.	3. Bisa cukup kompleks.
4. Menangkap jumlah informasi terbatas.	4. Resiko tinggi, penyusup bisa berinteraksi dengan sistem operasi sungguhan.

2.1.4. *Internet*

Internet merupakan singkatan dari International Networking atau Interconnection Networking yang berarti sebuah atau seperangkat jaringan komputer yang menghubungkan jutaan komputer di seluruh dunia melalui jaringan komunikasi satelit global dan kabel telepon lokal sehingga setiap komputer ataupun media yang terkoneksi didalam jaringan dapat berkomunikasi atau bertukar data tanpa dibatasi jarak, waktu dan tempat. Di sisi lain internet merupakan sebuah ruang informasi dan komunikasi budaya yang menembus batas-batas negara denga tujuan mempercepat penyebaran, pertukaran ilmu dan

gagasan di kalangan ilmuwan dan cendekiawan di seluruh penjuru dunia (Al-Khowarizmi, hal 6, 2020).

2.1.5. *Website*

Website adalah suatu metode yang digunakan untuk menyajikan informasi di internet dengan memanfaatkan berbagai media seperti teks, gambar, suara, dan video. Interaktivitas juga menjadi ciri penting dari website, di mana pengguna dapat berinteraksi dengan konten melalui berbagai cara. Website memiliki keunggulan dalam kemampuannya untuk menghubungkan dokumen satu dengan yang lain melalui tautan (link) yang dapat diakses melalui perangkat lunak web browser.

Namun, perlu diingat bahwa website juga kerap menjadi sasaran serangan dalam lingkungan digital. Lebih dari 60% dari total serangan dalam dunia digital menargetkan aplikasi web.

2.1.6. *Aplikasi Web*

Aplikasi *web* merupakan program yang diterima melalui media dengan koneksi internet dan disimpan di *server* atau *cloud* yang dapat diakses melalui antarmuka *web browser*. Aplikasi web juga merupakan perangkat lunak komputer yang dibuat menggunakan bahasa pemrograman seperti HTML, JavaScript, Ruby, Python, PHP, Java, AJAX, dan bahasa pemrograman lainnya. Melalui aplikasi web, pengguna dapat berinteraksi dengan layanan atau konten yang disediakan melalui tampilan yang diakses melalui *web browser*.

2.1.7. *Server*

Server adalah sistem komputer yang dirancang untuk menyediakan layanan khusus, terutama dalam hal penyimpanan data. Data yang disimpan di dalam *server* mencakup berbagai jenis informasi dan dokumen yang kompleks. Layanan ini ditujukan untuk para klien (*client*) yang membutuhkan akses ke informasi yang disediakan oleh server. Fungsi utama server adalah memberikan layanan akses yang lebih cepat untuk mengirim atau menerima data serta informasi yang tersimpan di dalamnya.

Secara fisik, *server* biasanya berbentuk jaringan komputer yang memiliki ukuran besar dan dilengkapi dengan komponen-komponen pendukung seperti prosesor dan *RAM* dengan kapasitas besar. *Server* berperan penting dalam menjaga kestabilan layanan dan ketersediaan data untuk memenuhi kebutuhan klien yang berinteraksi dengannya.

2.1.8. *Web Server*

Suatu sistem komputer yang dikenal sebagai *web server* berfungsi secara khusus untuk merespons permintaan dalam protokol HTTP dan HTTPS. *Web server* mengambil kode yang diterima dari peramban, lalu mengirimkannya kembali dalam bentuk laman *web* yang dihasilkan. Proses ini melibatkan pengiriman laman *web* dalam bentuk dokumen HTML dan CSS yang nantinya akan diolah oleh peramban, menghasilkan halaman-halaman *web* yang menarik dan mudah dibaca oleh pengguna. Melalui penjelasan di atas, dapat disimpulkan bahwa *web server* memiliki peran sentral dalam mengirim berkas yang diminta oleh pengguna melalui peramban dengan menggunakan protokol khusus. Sehingga, pengguna memiliki kemampuan untuk mengakses berbagai konten

seperti teks, gambar, video, dan lainnya melalui peramban. Lebih dari sekadar mempublikasikan World Wide Web (WWW), *web server* saat ini juga memiliki kemampuan untuk mengelola perangkat keras lainnya melalui HTTP, seperti *printer*, kamera, dan *router web*. Tujuannya adalah untuk memudahkan pengelolaan tugas-tugas tertentu.

2.1.9. Apache

Apache adalah salah satu *server web* yang paling populer di dunia. *Server* ini dikembangkan oleh *Apache Software Foundation* dan tersedia secara gratis dan *open source*. Apache dapat diinstal pada berbagai sistem operasi, termasuk Linux, Windows, dan macOS. Apache dapat digunakan untuk meng-host *website* atau aplikasi *web*. Dalam hal ini, Apache bertanggung jawab untuk menerima permintaan dari *browser web* dan mengirimkan kembali halaman *web* yang diminta. *Apache* juga dapat dikonfigurasi untuk memproses permintaan dan menghasilkan respon yang sesuai, seperti menjalankan skrip CGI atau memproses permintaan PHP.

2.1.10. Database Mysql

MySQL merupakan sebuah perangkat manajemen basis data yang menggunakan perintah dasar *Structured Query Language* (SQL) yang cukup terkenal. *Database management system* (DBMS) MySQL multi pengguna dan multi alur ini sudah dipakai oleh lebih dari 6 juta pengguna di seluruh dunia. MySQL adalah DBMS yang *open source* dengan dua bentuk lisensi, yaitu perangkat lunak bebas dan perangkat lunak berpemilik yang penggunaannya terbatas. Jadi MySQL adalah *database server* yang gratis dengan lisensi GNU

General Public License (GPL) sehingga dapat Anda pakai untuk keperluan pribadi atau komersil tanpa harus membayar lisensi yang ada.

MySQL masuk ke dalam jenis RDBMS (*Relational Database Management System*). Maka dari itu, istilah istilah seperti baris, kolom, tabel, dipakai pada MySQL. Misalnya di dalam MySQL sebuah *database* terdapat satu atau beberapa tabel. SQL sendiri merupakan suatu bahasa yang dipakai di dalam pengambilan data pada relational *database* atau *database* yang terstruktur. Jadi MySQL adalah *database management system* yang menggunakan bahasa SQL sebagai bahasa penghubung antara perangkat lunak aplikasi dengan *database server*.

2.1.11. PHP

PHP (*Hypertext Preprocessor*) adalah bahasa pemrograman *server-side* yang digunakan untuk mengembangkan aplikasi web dinamis. PHP pertama kali dibuat pada tahun 1994 oleh Rasmus Lerdorf sebagai sekumpulan script untuk mengelola data pengunjung pada situs web pribadinya. Kemudian, PHP dikembangkan oleh tim di bawah naungan *The PHP Group* dan menjadi salah satu bahasa pemrograman yang paling populer di dunia.

PHP dapat dijalankan di hampir semua sistem operasi dan *platform* web, termasuk Windows, macOS, Linux, dan platform web populer seperti Apache dan Nginx. PHP juga kompatibel dengan berbagai macam database, seperti MySQL, PostgreSQL, dan Oracle. Dalam pengembangan web, PHP umumnya digunakan untuk membuat halaman web dinamis yang menampilkan data dari database, mengolah formulir, dan interaksi dengan pengguna. PHP dapat berintegrasi dengan HTML, CSS, dan JavaScript untuk membuat tampilan yang menarik dan

interaktif pada aplikasi web. PHP memiliki sintaks yang mirip dengan C dan Perl, serta mudah dipelajari oleh pemula. Selain itu, PHP memiliki ribuan library dan framework yang dapat digunakan untuk mempercepat pengembangan aplikasi web.

2.1.12. HTML

Hypertext Markup Language atau yang disingkat HTML merupakan sebuah bahasa markah standar untuk dokumen yang dirancang untuk ditampilkan di peramban internet (*web browser*). Ini dapat dibantu oleh teknologi seperti *Cascading Style Sheets* (CSS) dan bahasa scripting seperti JavaScript dan VBScript. Peramban internet menerima dokumen HTML dari *server web* atau dari penyimpanan lokal dan membuat dokumen menjadi halaman *web* multimedia. HTML menggambarkan struktur halaman *web* secara semantik dan isyarat awal yang disertakan untuk penampilan dokumen.

Dokumen HTML merupakan *file* yang diakhiri dengan ekstensi. html ataupun. htm. Ekstensi *file* ini dapat dilihat dengan mengunakan *web browser*. Browser tersebut membaca *file* HTML serta me- render kontennya sehingga user internet dapat melihat serta membacanya.

Tiap-tiap halaman HTML terdiri atas beberapa *tags* (atau disebut *elements*), yang mengacu pada *buildingblock* halaman *web*. *Tag* tersebut membuat hirarki yang menyusun konten sampai jadi bagian, paragraf, *heading*, serta *block* konten yang lain. Sebagian besar element HTML mempunyai tag pembuka serta penutup yang memakai *syntax* <tag></tag>.

2.1.13. Cascading Style Sheets

Cascading Style Sheet (CSS) merupakan aturan untuk mengatur beberapa komponen dalam sebuah *web* sehingga akan lebih terstruktur, cantik, dan seragam, akan tetapi CSS bukanlah termasuk kedalam sebuah bahasa pemograman. Sama halnya *styles* dalam aplikasi pengolahan kata seperti *MicrosoftWord* yang dapat mengatur beberapa *style*, misalnya *heading*, *subbab*, bodytext, *footer*, images, dan *style* lainnya untuk dapat digunakan bersama-sama dalam beberapa berkas. Pada umumnya CSS dipakai untuk memformat tampilan halaman *web* yang dibuat dengan bahasa HTML dan XHTML.

2.1.14. *Visual Studio Code*

Visual Studio Code merupakan suatu *text editor* yang sering digunakan oleh *programmer* khususnya seorang *developer*. Aplikasi ini menjadi sesuatu yang sangat penting bagi *developer* sebagai alat bantu dalam melakukan pemrograman. Banyak *developer* yang menggunakan aplikasi *Visual Studio Code* untuk mendukung proses pekerjaan mereka. Warna dari tulisan *syntax* yang sangat variasi dan interaktif tentu sangat menarik dan sangat membantu dalam membaca penulisan *syntax*, warna *syntax* yang bervariasi dan sangat menarik mampu membuat penggunanya cukup nyaman dalam menjalankan proses pemrograman. Selain itu, ada banyak fitur yang tersedia di *Visual Studio Code* yang memiliki banyak kegunaan.

2.1.15. Google Chrome

Google Chrome merupakan perangkat lunak peramban web lintas *platform* yang dikembangkan oleh perusahaan *Google*. Pertama kalinya dirilis pada tahun

2008 untuk sistem operasi *Microsoft Windows*, kemudian diporting ke sistem operasi berbasis Linux, macOS, iOS, dan Android yang menjadikannya sebagai peramban bawaan dalam sistem operasi. Peramban ini juga merupakan komponen utama *Chrome OS*, yang berfungsi sebagai *platform* untuk aplikasi web.

Adapun juga fitur-fitur unggulan yang dibawa oleh *Google Chrome* selain dari fitur standar yang ditemukan dikebanyakan aplikasi peramban ternama. Perambagn web ini mendukung diantaranya, Javascript, HTML 5, CSS 3, dan sejumlah fitur antara lain mode privasi, multi tab, berbagai pilihan tema dan ekstensi dan tambahan plugin pihak ketiga, pilihan bahasa, dan beberapa fitur unggulan lainnya.

2.1.16. *VirtualBox*

VirtualBox adalah sebuah program perangkat lunak virtualisasi yang memungkinkan pengguna untuk menjalankan sistem operasi dan aplikasi lain di atas sistem operasi yang sudah ada, tanpa perlu melakukan penginstalan langsung di atas *hardware* fisik. Dengan menggunakan teknologi virtualisasi, *VirtualBox* dapat menciptakan lingkungan virtual yang memungkinkan sistem operasi dan aplikasi lain untuk berjalan di dalamnya secara terisolasi dan independen dari sistem operasi dan aplikasi lain yang ada pada hardware fisik.

Secara ilmiah, *VirtualBox* menggunakan teknologi virtualisasi tipe 2, yang berarti bahwa ia berjalan di atas sistem operasi host dan memerlukan sebuah *hypervisor* untuk mengontrol akses ke *hardware* fisik. *VirtualBox* mengimplementasikan *hypervisor* ini sebagai sebuah driver perangkat lunak yang berjalan di dalam sistem operasi *host*, dan menggunakan teknologi seperti

dynamic recompilation untuk memungkinkan lingkungan virtual untuk berjalan dengan cepat dan efisien.

VirtualBox juga menyediakan fitur-fitur seperti *snapshotting*, yang memungkinkan pengguna untuk membuat salinan snapshot dari lingkungan *virtual* pada titik tertentu dalam waktu, serta fitur *shared folder* yang memungkinkan pengguna untuk berbagi file antara lingkungan virtual dan sistem operasi *host*.

2.1.17. HIHAT

High Interaction Honeypot Analysis Tool (HIHAT) adalah alat analisis keamanan yang digunakan untuk memeriksa dan mengumpulkan informasi tentang serangan pada *honeypot* yang berinteraksi secara tinggi. HIHAT bekerja dengan menggunakan teknik analisis forensik untuk menganalisis data yang dikumpulkan oleh *honeypot*. Alat ini memeriksa catatan *log*, memeriksa aktivitas jaringan, dan menganalisis *malware* yang ditemukan pada *honeypot*. HIHAT juga dapat membantu administrator keamanan dalam mengidentifikasi tindakan yang harus diambil untuk meningkatkan keamanan sistem, seperti menambahkan *filter* jaringan atau mengubah konfigurasi *firewall*.

HIHAT juga memiliki kemampuan untuk melakukan analisis forensik pada sistem yang telah diserang. Alat ini dapat membantu administrator keamanan dalam mengidentifikasi sumber serangan dan memperbaiki kerusakan pada sistem. HIHAT dapat membantu dalam membangun strategi keamanan yang lebih baik dan meningkatkan kemampuan organisasi dalam menghadapi serangan yang lebih kompleks dan canggih.

2.2. Penelitian Terdahulu

Table 2.2 Penelitian Terdahulu

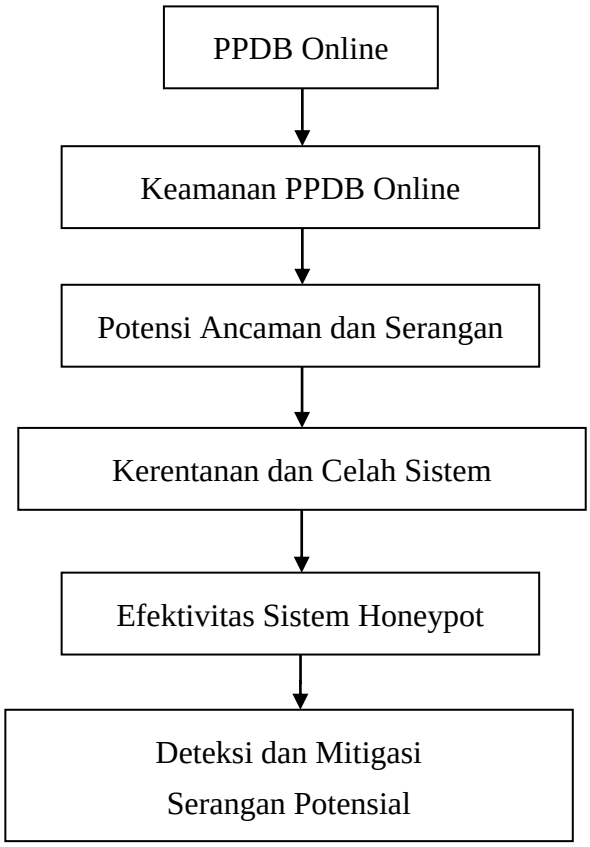
No	Judul Penelitian	Hasil Penelitian	Metode Penelitian
1.	"Implementasi Penerimaan Peserta Didik Baru (PPDB) Berbasis Web pada Sekolah Dasar Alam Semangat Bangsa dan Taman Kanak-Kanak Kartini Kecamatan Medan Johor", Al-Khowarizmi, 2020, Universitas Muhammadiyah Sumatera Utara	Implementasi Penerimaan Peserta Didik Baru (PPDB) Berbasis Web pada Sekolah Dasar Alam Semangat Bangsa dan Taman Kanak-Kanak Kartini Kecamatan Medan Johor. Perubahan yang cukup baik karena pendaftar lebih banyak menggunakan aplikasi PPDB berbasis web.	Metode penelitian ini menggunakan penelitian deskriptif kualitatif dengan teknik pengumpulan data yang digunakan adalah teknik observasi, wawancara dan dokumentasi.
2.	"Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) Dan Registrasi Online Berbasis Website Pada SMP Negeri 6 Palangka Raya", Dilla Ayu Dwipitaloka, 2020, Universitas Palangka Raya	Hasil dari pengujian blackbox pada sistem dapat diketahui bahwa fitur-fitur yang ada pada sistem informasi penerimaan peserta didik baru dan registrasi online dapat berfungsi seperti tujuan.	Metode penelitian ini menggunakan Studi Pendahuluan, Metodologi penelitian waterfall, dan Metode Pengembangan Sistem
3	"Efektivitas Penerimaan Peserta Didik Baru (PPDB) Melalui Sistem Penerimaan Peserta Didik Online", Asri Ulfah Wulan Sari, 2017, Universitas Negri Malang	Penerimaan berkas pendaftaran langsung di entry dan dimasukan ke dalam website dan kemudian mendapat print out formulir pendaftaran online. Kedua kejelasan prosedur tercantum dalam buku pedoman dan website dinas pendidikan. Keterbukaan juga telah dilaksanakan sehingga masyarakat dapat langsung melihat hasil dari pendaftaran. Keamanan serta keterbukaan berjalan dengan baik aman karena pelayanan berjalan dengan transparan tentang data peserta didik yang diterima. Ketiga sangat efisien dan ekonomis karena pendaftaran tanpa biaya/gratis. Keadilan berjalan dengan adil karena tidak ada perbedaan dalam menentukan penerimaan peserta didik baru. Ketepatan waktu dimulai dan berakhirnya penerimaan peserta didik	Metode penelitian ini menggunakan penelitian deskriptif kualitatif dengan teknik pengumpulan data yang digunakan adalah teknik observasi, wawancara dan dokumentasi.

		menggunakan sistem timer	
4.	"Pelaksanaan Pelayanan Penerimaan Peserta Didik Baru (PPDB) Pada Sekolah Dasar Al-Fath Cirendeu Tangerang Selatan", Wiwin Wianti, 2019, STKIP Situbondo	Prosedur pelayanan yang dinilai sederhana dan mudah dipahami oleh pendaftar; Waktu penyelesaian bergantung pada kecepatan dan ketepatan pendaftar dalam melakukan pembayaran; Semua biaya pelayanan terperinci dengan jelas dan dibayarkan sesuai dengan perincian; Sarana dan prasarana sudah tersedia dengan lengkap serta menunjang kegiatan sehingga menimbulkan rasa aman dan nyaman; Kompetensi petugas pemberi pelayanan dalam Penerimaan Peserta Didik Baru bersikap ramah, sopan, adil dan sesuai dengan bidang keahliannya masingmasing.	Metode penelitian ini menggunakan penelitian deskriptif kualitatif dengan teknik pengumpulan data yang digunakan adalah teknik observasi, wawancara dan dokumentasi.
5.	"Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) Berbasis WEB Di SMP Negri 1 Wanasari Brebes", Nur Ariesanto Ramdhan, 2019, Universitas Muhadi Setiabudi	Berdasarkan hasil penelitian dan pembahasan terhadap Sistem Informasi Penerimaan Peserta Didik Baru Berbasis Web di SMP Negeri 1 Wanasari Brebes, panitia PPDB dapat mengelola pelaksanaan program PPDB dengan baik seperti pendaftaran peserta, pendataan peserta, hasil seleksi peserta dan daftar ulang peserta dengan lebih efisien, baik dalam hal waktu, tempat, biaya, tenaga maupun kecurangan yang terjadi dalam pelaksanaan program penerimaan peserta didik baru.	Metode yang digunakan dalam penelitian ini adalah pengumpulan data, pengembangan sistem, analisis kebutuhan sistem, desain sistem, desain basis data, dan desain antarmuka
6.	"Penerimaan Peserta Didik Baru (PPDB) Pada SD Inpres Kalikodok Bintuni Berbasis Web", Marlinda Sanglise, 2022, Universitas Papua Manokwari	Sistem informasi penerimaan peserta didik baru berbasis web pada SD Inpres Kalikodok, panitia PPDB mengelola pelaksanaan program PPDB dengan baik seperti pendaftaran peserta, dan hasil seleksi peserta dengan lebih efisien, baik dalam	Metode penelitian yang dilakukan dalam penelitian ini adalah Studi Literatur, Analisis dan Perancan gan, Implementasi, Pengujian dan Dokumentasi

		ha l waktu, tempat, biaya, tenaga maupun kecurangan yang terjadi dalam pelaksanaan program penerimaan peserta didik baru.	
7.	"Perancangan Sistem Informasi Pendaftaran Peserta Didik Baru (PPDB) Berbasis Web Menggunakan Metode Rapid Apllication Development", Anton Yudahana, 2023, Universitas Ahmad Dahlan	Berdasarkan hasil penelitian disimpulkan bahwa desain sistem yang dibuat dapat mempermudah pengguna dalam menggunakan sistem tersebut, karena rancangan yang dibuat lebih menarik dan mudah dimengerti berbagai kalangan.	Metode penelitian ini adalah observasi, mengidentifikasi masalah, studi literature, wawancara, perancangan, analisis
8.	"Analisis Serangan Hackermenggunakan Honeypot High Interaction (HIHAT)", Wahyu Purnama Sari, 2018, Universitas Langlangbuana	Sistem yang digunakan pada analisis saat ini mencakup beberapa aspek dalamsoftware danjugahardware yang mumpuni dikarenakan kebutuhansistem yang sangat besar, aplikasi dapat berjalanapabila terdapat server yang dapat berjalandenganoptimal sehingga dapat mensupport softwareyangdigunakan. Berdasarkan banyaknya ancamandatayang diretas melalui aplikasi website yangtidakterintegrasi keamanannya maka dilakukananalisadengan memasang Honeypot High Interaction(HIHAT) di beberapa aplikasi yang sudah disebutkansebelumnya.	Metode penelitian yang digunakan adalah penelitian deskriptif, dimana peneliti memusatkan perhatian kepada serangan-serangan yang terjadi padaserver di perusahaan XYZ. Pengumpulan datauntukproses analisa dilakukan dengan cara observasi danwawancara untuk mendapatkan informasi yangakurat.
9.	"IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER", Lukito Prima Aidin, 2016, Universitas Telkom	Implementas i high interaction honeypot yang dipasang pada server yang berupa berhasil dilakukan dengan menggunakan High Interaction Analysis Tools sebagai high interaction honeypot untuk aplikasi web. Berdasarkan hasil pengujian, dapat disimpulkan bahwa honeypot high interaction HIHAT dapat mengemulas ikan dan mencatat serangan directiory buster	Metode penelitian ini menggunakan penelitian deskriptif.

		brute force, RFI, dan SQL Injection namun masih belum dapat mengemulasikan serangan DoS dengan sempurna. Dari hasil DoS, HIHAT pada honeupot mengalami delay saat mendapatkan request yang banyak secara bersamaan namun semua request tetap diproses tanpa adanya packet loss.	

2.3. Kerangka Berfikir Konseptual



Gambar 2.3. Kerangka Berfikir Konseptual

1. Keamanan PPDB Online: Pentingnya menjaga keamanan sistem PPDB Online. Hal ini mencakup perlindungan terhadap data sensitif, informasi

pribadi, dan menghindari potensi kerugian yang bisa ditimbulkan oleh kebocoran data atau serangan.

2. Potensi Ancaman dan Serangan: Tahap ini mencakup identifikasi potensi ancaman dan serangan yang mungkin dialami oleh PPDB Online. Beberapa contoh serangan yang dapat ditangani oleh honeypot termasuk serangan brute force, SQL injection, dan serangan mencurigakan lainnya.
3. Kerentanan dan Celah Sistem: Menjelaskan bahwa setiap sistem IT, termasuk PPDB Online, memiliki kerentanan dan celah yang bisa dimanfaatkan oleh penyerang. Implementasi metode honeypot bertujuan untuk menarik perhatian penyerang ke dalam lingkungan simulasi honeypot daripada sistem utama yang lebih sensitif.
4. Efektivitas Sistem Honeypot: Membahas tentang efektivitas dan kinerja sistem honeypot dalam mendeteksi, merekam, dan menghadapi serangan yang mengarah ke dalam lingkungan honeypot. Evaluasi ini penting untuk memastikan bahwa honeypot berfungsi sebagaimana mestinya.
5. Deteksi dan Mitigasi Serangan Potensial: Tahap ini menjelaskan bagaimana sistem honeypot dapat digunakan untuk mendeteksi dan menghadapi serangan potensial sebelum mereka mencapai bagian utama dari sistem PPDB Online. Dengan begitu, potensi kerusakan pada sistem utama dapat diminimalisasi atau dihindari.

2.4. Hipotesis

Hipotesis merupakan dugaan awal yang diajukan untuk diuji dalam penelitian atau eksperimen. Ini adalah pernyataan tentang hubungan atau efek antara variabel yang akan diuji dan dapat dibuktikan melalui pengumpulan data

dan analisis lebih lanjut. Maka dari itu hipotesis penelitian ini adalah sebagai berikut:

H1: PPDB mampu mengatasi permasalahan yang terjadi pada urusan administrasi diantaranya masalah pada penginputan data siswa baru dan tidak tertata menjadi data tersebut lebih mudah untuk ditemukan.

H2: PPDB yang dirancang dengan berbasis web yang dapat dibuka dimanapun serta memiliki proses yang cepat, sehingga proses PPDB dilakukan secara online agar tidak berkurangnya minat calon peserta didik baru untuk mendaftar di sekolah dasar SD Muhammadiyah 03 Sibolga.

H3: Metode *honeypot* yang merupakan salah satu cara dalam mengatasi resiko keamanan informasi sistem penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga, dengan menarik perhatian penyerang ke area yang telah dipersiapkan, yaitu dengan menyediakan *server* yang sama persis seperti server aslinya atau dapat disebut dengan *honeypot*, kemudian memasangkan program HIHAT pada *server* tersebut yang berfungsi untuk mengumpulkan semua informasi serangan yang masuk pada *honeypot*.

BAB 3

METODOLOGI PENELITIAN

3.1. Jenis Penelitian

Jenis Penelitian ini adalah penelitian deskriptif. Metode deskriptif adalah suatu metode yang digunakan untuk menganalisa data dengan cara mendeskripsikan atau menggambarkan data yang telah terkumpul sebagaimana adanya tanpa bermaksud membuat kesimpulan yang berlaku untuk umum atau generalisasi. Penelitian ini adalah bagaimana Analisis sistem informasi akuntansi penerimaan kas dalam peningkatan pendapatan pada SD Muhammadiyah 03 Sibolga, sehingga dapat dijelaskan bahwa jenis penelitian ini adalah penelitian kualitatif secara deskriptif yang mengambarkan keadaan yang diteliti dan memaparkan atau menyajikan apa adanya data yang diperoleh, kemudian membuat kesimpulan untuk memberikan alternatif pemecahannya.

3.2. Definisi Operasional

Definisi operasional adalah petunjuk bagaimana suatu variabel itu diukur, yang tujuannya untuk melihat sejauh mana pentingnya variabel yang digunakan dalam penelitian ini, dan juga untuk mempermudah pemahaman dan membahas penelitian ini mengenai Sistem Penerimaan Peserta Didik Baru (PPDB) dan Metode Penggunaan *Honeypot* Pada Keamanan *Server* dalam peningkatan pendapatan yang akan ditentukan dengan:

3.2.1. Sistem Informasi Penerimaan Peserta Didik Baru

PPDB adalah proses penerimaan peserta didik baru yang dilakukan melalui sebuah sistem yang dirancang untuk mengelola data input dari pendaftar yang kemudian dikirim ke sekolah pelaksana PPDB.

Alat Ukur adalah satuan terkecil objek penelitian yang diinginkan peneliti sebagai klasifikasi pengumpulan data serta memberikan gambaran sesuai dengan kenyataan ataupun fakta-fakta yang ada pada saat diadakan penelitian, adapun Alat Ukur yang digunakan adalah:

1. *Input* data dikumpulkan dan dimasukkan sebagai *input* ke dalam sistem, input data dilakukan oleh pendaftar atau calon siswa. Data-data yang di-*input* merupakan data diri yang nantinya dapat dilihat juga oleh admin sekolah.
2. *Proses* merupakan pengolahan data atau input untuk menghasilkan informasi baik secara manual atau terkomputerisasi. Pemrosesan data tersebut dilakukan pada tahap akhir, yaitu pada waktu yang telah ditentukan oleh sekolah yang dilakukan oleh admin sekolah kemudian akan menjadikan sebuah *output* informasi siswa yang lulus dihasilkan oleh sebuah sistem.
3. *Output* dari sebuah sistem informasi penerimaan peserta didik baru pada SD Muhammadiyah 03 Sibolga adalah berupa data calon siswa yang telah lulus pada tahap seleksi yang dilakukan oleh admin sekolah dengan menggunakan sistem ini. Selain data calon siswa yang telah lulus kemudian adapun juga data siswa tidak lulus pada tahap seleksi tersebut.

3.2.2. *Honeypot*

Honeypot merupakan teknologi keamanan *web server* yang bertujuan mengidentifikasi, mencari celah keamanan dan berkomprimasi aktif ketika terjadi aktifitas penyusupan keamanan teknologi informasi.

Metode *Honeypot* adalah teknik yang digunakan untuk mengamankan jaringan komputer atau sistem informasi dengan cara menarik perhatian penyerang atau hacker sehingga mereka tertarik untuk melakukan serangan ke dalam sistem yang disiapkan secara sengaja. Berikut ini adalah beberapa alasan mengapa menggunakan metode *Honeypot*:

1. Mendeteksi serangan: *Honeypot* berfungsi sebagai alat deteksi awal yang efektif. Dengan menarik perhatian penyerang, *Honeypot* dapat mendeteksi serangan sebelum mencapai sistem yang sebenarnya. Hal ini memungkinkan administrator sistem untuk mengambil langkah-langkah pencegahan sebelum kerusakan yang serius terjadi.
2. Mempelajari taktik penyerangan: Dengan menggunakan *Honeypot*, administrator sistem dapat mempelajari taktik dan metode yang digunakan oleh penyerang. Informasi ini sangat berharga untuk meningkatkan keamanan dan mencegah serangan serupa di masa depan.
3. Mengalihkan perhatian penyerang: Dengan memusatkan serangan pada Honeypot, sistem yang sebenarnya dapat menjadi lebih aman karena penyerang teralihkan dan sumber daya mereka terbuang. Dengan mengalihkan perhatian penyerang ke *Honeypot*, sistem asli dapat bekerja tanpa gangguan dan mengurangi risiko serangan yang merugikan.

4. Menganalisis dan memahami serangan: *Honeypot* menyediakan lingkungan yang terisolasi dan terkendali untuk mempelajari serangan yang dilakukan oleh penyerang. Ini memungkinkan penelitian yang mendalam tentang metode, alat, dan motif serangan yang dapat membantu meningkatkan keamanan sistem.
5. Menarik perhatian penyerang: Dalam lingkungan jaringan yang terus berkembang, penting untuk mengamankan sistem dengan menarik perhatian penyerang. *Honeypot* menawarkan target yang menarik bagi penyerang, mengalihkan perhatian mereka dari sistem yang sebenarnya. Dengan demikian, memungkinkan waktu yang lebih lama untuk mendeteksi dan mencegah serangan sebelum mereka mencapai target yang sebenarnya.

Namun, penting untuk diingat bahwa penggunaan *Honeypot* juga memiliki beberapa risiko. Jika tidak dikonfigurasi dengan baik, *Honeypot* dapat memberikan penyerang akses yang tidak sah ke sistem atau membiarkan mereka mengetahui informasi sensitif. Oleh karena itu, implementasi dan konfigurasi yang hati-hati sangat penting untuk meminimalkan risiko dan memastikan keberhasilan penggunaan metode *Honeypot*.

Selain metode honeypot, ada beberapa metode lainnya yang digunakan dalam mengamankan sebuah web server yaitu:

1. Firewall: Mencegah akses yang tidak sah ke jaringan.
2. IDS/IPS: Mendeteksi dan mencegah serangan.
3. Pemindaian Keamanan: Mengidentifikasi kerentanan sistem.

4. Enkripsi: Mengamankan data dengan mengubahnya menjadi bentuk yang tidak terbaca.
5. Keamanan kata sandi: Menggunakan kebijakan kata sandi yang kuat.
6. Sistem Operasi dan Perangkat Lunak yang Diperbarui: Memperbarui sistem dengan patch keamanan terbaru.
7. Segmentasi Jaringan: Memisahkan jaringan menjadi segmen untuk mengurangi dampak serangan.
8. Sertifikat SSL/TLS: Mengamankan koneksi web dan komunikasi.
9. Sistem Autentikasi dan Otorisasi yang Kuat: Menerapkan metode autentikasi yang kuat dan mengontrol akses pengguna.
10. Pelatihan Kesadaran Keamanan: Melatih karyawan tentang praktik keamanan dan ancaman yang ada.

Secara fungsional dari teknologi *honeypot* terdiri dalam banyak variasi dan umumnya terbadi dalam dua kategori yaitu *honeypot* interaksi rendah (*low interaction honeypot*) dan honeypot berinteraksi sensitif (*high interaction honeypot*). Adapun alat ukur yang digunakan adalah:

1. *Monitoring* atau merekam *web server* terhadap serangan-serangan hacker yang mencoba masuk seperti dengan melakuan *SQL Injection*, *XSS*, *Code Injection* dan percobaan untuk melakukan *Inclusion*.
2. Pemeliharaan diharapkan mampu mengoptiomalkan atau mengamankan *web server* terhadap serangan-serangan hacker, dengan melakukan pemantauan terhadap honeypot nantinya dapat diketahui log penyerangan terhadap web server. Kemudian dari sinilah dapat dilakukan pemeliharan server atau memperbaharui keamanan web server.

Adapun Cara Kerja Metode Honeypot Sebagai Berikut :

1. Ada dua server yaitu PPDB server asli juga ada server honeypot PPDB Honeypot, jadi kita menyediakam server lagi untuk honeypot nya bisa dibilang server PPDB tapi boongan, fungsinya untuk mengalabui hacker yang coba untuk melakukan penetrasi sql injection dan lainnya.

2. Nanti diserver honeypot itu ada log dari penyerangan yang telah dilakukan. Dari log log itu kita bisa analisa apakah sistem perlu dilakukan pembaharuandari segi keamanannya. Untuk memancing perhatian peretas, honeypot sengaja dibuat dengan tingkat keamanan yang rendah. Perlu dipahami jika honeypot bukanlah bentuk cyber security yang dapat mencegah serangan hacker secara langsung.

3.3. Lokasi dan Waktu Penelitian

1. Lokasi Penelitian

   Adapun penelitian ini dilakukan pada SD Muhammadiyah 03 Sibolga yang beralamat di Jl. Sisingamangaraja No. 97a, Pancuran Kerambil, Kec. Sibolga Sambas, Kota Sibolga Prov. Sumatera Utara.

2. Waktu penelitian

   Penelitian ini dilakukan selama 6 bulan, yang dimulai dari bulan Januari 2023 s/d Juni 2023

Tabel 3.1. Rencana jadwal penelitian/Jadwal penelitian

No	Aktifitas Penelitian	Januari 2023				Februari 2023				Maret 2023				April 2023				Mei 2023				Juni 2023			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Penelitian pendahuluan (prariset)																								
2	Penyusunan Proposal																								
3	Pembimbingan Proposal																								
4	Pengumpulan Data																								
5	Pengolahan dan analisis data																								
6	Penyusunan skripsi (laporan penelitian)																								
7	Pembimbingan skripsi																								
8	Seminar Hasil																								
9	Perbaikan Hasil Revisi																								
10	Sidang meja hijau																								
11	Penyempurnaan skripsi dan penulisan artikel jurnal																								

3.4. Metode Pengembangan Sistem

Metode pengembangan sistem diperlukan sebuah pendekatan atau metode pengembangan sistem yang sistematis dan terstruktur untuk mencapai tujuan penelitian dengan efisien dan efektif. Metode pengembangan sistem waterfall digunakan dalam penelitian PPDB Online di SD Muhammadiyah 03 Sibolga untuk memastikan adanya langkah-langkah yang terstruktur dan terurut. Setiap tahap harus diselesaikan sebelum melanjutkan ke tahap berikutnya, sehingga memastikan pengembangan sistem yang terencana dan terorganisir dengan baik. Berikut adalah beberapa tahapan yang dapat digunakan dalam metode pengembangan sistem tersebut:

1. Studi Pendahuluan, tahap pertama adalah melakukan studi pendahuluan untuk memahami secara menyeluruh mengenai PPDB Online SD

Muhammadiyah 03 Sibolga, termasuk arsitektur, infrastruktur, keamanan sistem yang sudah ada, dan potensi masalah keamanan yang mungkin timbul. Selain itu, juga perlu mempelajari konsep dan teknis implementasi metode honeypot yang akan digunakan.

2. Analisis Kebutuhan, pada tahap ini dilakukan analisis untuk menentukan kebutuhan dan tujuan implementasi metode honeypot pada PPDB Online. Hal ini melibatkan identifikasi potensi risiko keamanan yang ingin diatasi dengan penggunaan honeypot, serta kebutuhan fungsional dan non-fungsional dari sistem honeypot yang akan dikembangkan.
3. Desain Sistem, setelah kebutuhan dianalisis, tahap selanjutnya adalah merancang sistem honeypot yang sesuai. Ini melibatkan pemilihan jenis honeypot yang tepat, konfigurasi lingkungan simulasi, infrastruktur yang diperlukan, dan integrasi dengan sistem PPDB Online yang ada. Selain itu, aspek keamanan dan privasi juga harus diperhatikan selama perancangan ini.
4. Implementasi, Setelah desain sistem siap, langkah selanjutnya adalah mengimplementasikan sistem honeypot tersebut dalam lingkungan PPDB Online SD Muhammadiyah 03 Sibolga. Ini melibatkan penerapan konfigurasi honeypot, integrasi dengan sistem PPDB Online, dan pengujian untuk memastikan bahwa honeypot berfungsi sesuai harapan.
5. Uji Coba, sistem honeypot perlu diuji coba untuk mengevaluasi kinerjanya dalam mendeteksi dan menghadapi serangan potensial. Ini akan membantu untuk mengidentifikasi kekurangan dan melakukan perbaikan pada sistem honeypot jika diperlukan.

6. Integrasi dan Penerapan, jika hasil uji coba dan evaluasi sudah memuaskan, maka tahap selanjutnya adalah melakukan integrasi sistem honeypot ke dalam lingkungan produksi PPDB Online SD Muhammadiyah 03 Sibolga. Pastikan bahwa sistem honeypot berjalan dengan baik tanpa mengganggu kinerja sistem utama.
7. Monitoring dan Pemeliharaan, perlu dilakukan pemantauan secara berkala terhadap sistem honeypot untuk memastikan bahwa ia tetap berfungsi dengan baik dan efektif dalam menghadapi potensi serangan. Selain itu, lakukan pemeliharaan rutin untuk memastikan bahwa honeypot selalu mendapatkan pembaruan dan perlindungan terhadap ancaman baru.
8. Dokumentasi, penting untuk melakukan dokumentasi secara lengkap dan rapi. Hal ini akan membantu untuk memudahkan pemahaman dan mengatasi masalah di masa mendatang serta untuk memperluas penelitian lebih lanjut.

Dengan mengikuti tahapan-tahapan di atas, penelitian analisis dan implementasi metode honeypot pada PPDB Online SD Muhammadiyah 03 Sibolga dapat dilakukan dengan terstruktur dan menghasilkan sistem keamanan yang lebih efektif.

3.5. Teknik Pengambilan Sampel

Beberapa pendekatan yang digunakan oleh peneliti untuk mengumpulkan data dari sampel Honeypot HIHAT yang digunakan dalam penelitian ini. Berikut adalah penjelasan lebih rinci tentang metode pengumpulan data sampel pada penelitian ini:

1. Penempatan Honeypot HIHAT: Pertama-tama, peneliti menentukan lokasi dan konfigurasi penempatan Honeypot HIHAT di dalam lingkungan PPDB SD Muhammdiyah 03 Sibolga. Proses ini melibatkan pemilihan zona-zona yang berpotensi menjadi target serangan, seperti server basis data, server aplikasi, dan perangkat jaringan yang kritis. Setiap Honeypot HIHAT ditempatkan dengan konfigurasi yang mencerminkan potensi kerentanan sistem asli dan menarik perhatian penyerang.
2. Perekaman Data Aktivitas: Honeypot HIHAT yang telah ditempatkan di lingkungan PPDB akan merekam aktivitas yang terjadi di sekitarnya. Data yang direkam meliputi percobaan akses, percobaan login, permintaan data palsu, dan berbagai aktivitas yang mencurigakan. Pengumpulan data ini dilakukan secara pasif, dengan tujuan mendapatkan informasi tentang potensi serangan dan taktik penyerangan yang digunakan oleh para penyerang.
3. Analisis Log dan Kejadian: Data yang dikumpulkan dari Honeypot HIHAT akan dianalisis secara menyeluruh oleh peneliti. Log dan kejadian yang direkam oleh Honeypot akan diuraikan untuk mengidentifikasi pola serangan yang umum, metode yang digunakan oleh penyerang, serta upaya-upaya untuk mengeksploitasi sistem Honeypot. Analisis ini membantu peneliti dalam memahami ancaman keamanan yang mungkin dihadapi oleh sistem PPDB SD Muhammdiyah 03 Sibolga.
4. Validasi Data: Selama proses pengumpulan data, peneliti memastikan bahwa data yang direkam oleh Honeypot HIHAT akurat dan relevan untuk penelitian. Selain itu, langkah-langkah validasi dilakukan untuk

memastikan bahwa data yang dianalisis dapat diandalkan dan memberikan informasi yang benar-benar bermanfaat dalam mengidentifikasi potensi ancaman keamanan pada PPDB SD Muhammdiyah 03 Sibolga.

3.6. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan penulis dalam penelitian ini yaitu dengan menggunakan cara studi dokumentasi. Dokumentasi dengan mengumpulkan data pada log honeypot HiHAT.

3.7. Teknik Analisis Data

Teknik analisis data yang digunakan adalah dengan cara menguji keabsahan data kualitatif karena dengan keabsahan data merupakan salah satu awal kebenaran analisis data, penelitian ini sejalan dan seiring dengan proses penelitian yang sedang berlangsung yang dilakukan sejak awal pengambilan data yaitu sejak melakukan reduksi data, penyajian data dan penarikan kesimpulan atau verifikasi.

Analisis data yang dilakukan secara kualitatif dengan cara berulang-ulang dan berkesinambungan antara pengumpulan dan analisis data, baik selama pengumpulan data di lapangan maupun sesudah data.

Analisis data adalah kegiatan mengolah data yang telah dikumpulkan dari hasil penelitian. Adapun teknik analisis data deskriptif pada penelitian ini langkah- langkahnya sebagai berikut:

a. Menganalisis log file dari Honeypot, seperti log server web atau log SSH, untuk mengidentifikasi aktivitas yang mencurigakan, seperti permintaan HTTP yang tidak biasa atau percobaan login yang berulang.

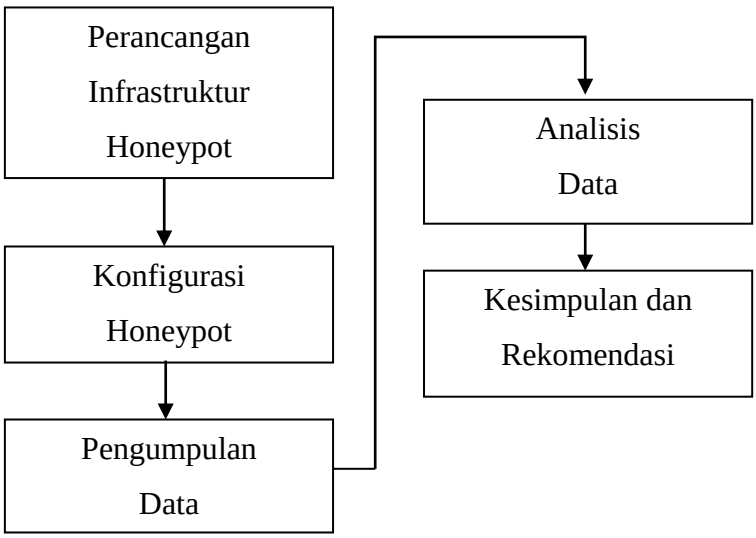
b. Menyoroti pola serangan yang sering muncul, seperti SQL injection, brute force attack, atau scanning.
c. Mencari pola serangan berulang dari alamat IP tertentu, menandakan adanya penyerang yang terus menerus mencoba mengeksploitasi Honeypot.
d. Mengetahui apakah penyerang berasal dari alamat IP yang sering terkait dengan aktivitas jahat atau bermasalah.
e. Melakukan analisis kesimpulan apakah metode *honeypot* dapat memperkuat keamanan pada *server* sistem informasi penerimaan peserta didik baru.

BAB 4

HASIL DAN PEMBAHASAN

4.1. Metode Honeypot

Metode Honeypot adalah salah satu pendekatan keamanan siber yang bertujuan untuk menarik dan memerangkap penyerang atau hacker yang mencoba untuk mendapatkan akses tidak sah ke sistem atau jaringan komputer. Penelitian ini bertujuan untuk mengimpelentasikan metode Honeypot pada sistem PPDB dalam mendeteksi dan merekam serangan siber, serta memahami perilaku penyerang yang mencoba mengeksploitasi sistem tersebut. Penelitian akan mencakup analisis taktik dan teknik yang digunakan penyerang, serta menilai tingkat keberhasilan Honeypot dalam mendeteksi dan merespons serangan. Berikut ini metode dalam mengimplementasikan honeypot pada sistem PPDB Online SD Muhammadiyah 03 Sibolga dapat dilihat bada gambar 4.1.



Gambar 4.1 Metode Honeypot

1. Perancangan Infrastruktur Honeypot, Infrastruktur Honeypot adalah sebuah sistem yang dirancang untuk menarik dan memantau serangan siber yang ditujukan ke dalam jaringan atau sistem tertentu. Tujuan utama dari Honeypot adalah untuk mengamati, mempelajari, dan memahami metode serangan yang digunakan, sehingga data yang didapatkan nantinya dapat dijadikan referensi dalam meningkatkan keamanan sistem secara keseluruhan.
2. Konfigurasi Honeypot, Peneliti akan mengimplementasikan honeypot pada sistem PPDB Online SD Muhammadiyah 03 Sibolga. Penerapan sesuai dengan petunjuk dari honeypot yang akan digunakan.
3. Pengumpulan Data, Metode ini melibatkan pemasangan mekanisme pemantauan dan logging pada Honeypot untuk merekam aktivitas penyerangan. Peneliti akan mengumpulkan data lalu lintas jaringan dan aktivitas mencurigakan yang mencoba mengeksploitasi Honeypot.
4. Analisis Data, Data yang dikumpulkan dari Honeypot akan dianalisis untuk mengidentifikasi jenis serangan yang terdeteksi, teknik yang digunakan penyerang, dan pola perilaku penyerang. Analisis ini penting untuk memahami taktik penyerangan dan efektivitas Honeypot dalam mendeteksi ancaman.
5. Kesimpulan dan Rekomendasi, Peneliti akan menyimpulkan hasil penelitian berdasarkan analisis data. Rekomendasi akan diberikan untuk meningkatkan keamanan siber berdasarkan temuan penelitian.

4.2. Perancangan dan Analisis Kebutuhan

Pada tahap perancangan, peneliti akan memaparkan langkah-langkah yang diambil untuk menganalisis dan mengimplementasikan metode honeypot dalam sistem Penerimaan Peserta Didik Baru (PPDB) Online di SD Muhammadiyah 03 Sibolga. Tujuan utama dari penelitian ini adalah untuk meningkatkan tingkat keamanan sistem PPDB Online serta melindungi sistem dari potensi serangan oleh pihak yang tidak bertanggung jawab.

Langkah pertama yang akan dilakukan oleh peneliti adalah melakukan analisis mendalam mengenai metode honeypot yang akan diterapkan. Memilih honeypot HiHAT menjadi pilihan yang relevan dalam penelitian ini karena honeypot HiHAT merupakan jenis honeypot yang efektif dalam menarik perhatian penyerang. Selain itu, honeypot HiHAT juga memiliki keunggulan dalam mendeteksi dan merekam aktivitas yang mencurigakan. Setiap interaksi yang terjadi pada honeypot ini akan terekam dengan baik, memberikan peneliti data yang berharga dalam menganalisis niat dan teknik serangan yang mungkin dilakukan oleh pihak yang tidak bertanggung jawab.

Memilih honeypot HiHAT dalam penelitian ini menjadi langkah yang tepat karena honeypot ini mampu menarik perhatian penyerang, merekam aktivitas mencurigakan, dan membantu meningkatkan keamanan sistem PPDB Online di SD Muhammadiyah 03 Sibolga.

Selanjutnya, peneliti akan memikirkan integrasi honeypot dengan sistem PPDB Online yang sudah ada. Hal ini akan melibatkan perencanaan agar penerapan honeypot tidak mengganggu fungsionalitas sistem utama. Selain itu, peneliti akan memastikan bahwa honeypot tersembunyi dengan baik sehingga

tidak mudah terdeteksi oleh penyerang. Peneliti juga akan membahas tentang analisis data yang dikumpulkan oleh honeypot. Data dan informasi yang diperoleh akan dianalisis guna meningkatkan keamanan sistem secara menyeluruh. Peneliti juga akan merancang tindakan respons terhadap serangan yang terdeteksi oleh honeypot, guna melindungi sistem PPDB Online dari potensi ancaman yang muncul.

Diharapkan bahwa hasil dari perancangan ini akan menjadi panduan bagi peneliti dalam mengimplementasikan metode honeypot dalam sistem PPDB Online SD Muhammadiyah 03 Sibolga. Implementasi honeypot yang tepat diharapkan dapat meningkatkan keamanan sistem secara signifikan, sehingga sistem PPDB Online dapat menghadapi berbagai potensi serangan siber dengan lebih efektif selama proses penerimaan peserta didik baru berlangsung.

Analisis kebutuhan merupakan suatu prosedur sebelum melakukan penelitian implementasi metode *honeypot* pada PPDB Online SD Muhammadiyah 03 Sibolga, peneliti akan menjabarkan kebutuhan perangkat keras maupun perangkat lunak yang akan digunakan untuk implementasi dan pengujian dalam penelitian ini. Dengan keterbatasan sumber daya, peneliti menggunakan cara alternatif dalam mengimplementasikan metode honeypot pada sistem PPDB Online SD Muhammadiyah 03 Sibolga, yaitu dengan cara virtualisasi, dalam hal ini peneliti menggunakan *software virtual machine* berupa Oracle VM VirtualBox. Berikut ini merupakan kebutuhan perangkat keras maupun perangkat lunak untuk mengimplementasikan metode *honeypot* pada sistem PPDB Online SD Muhammadiyah Sibolga :

Tabel 4.1. Kebutuhan Perangkat Keras / Perangkat Lunak

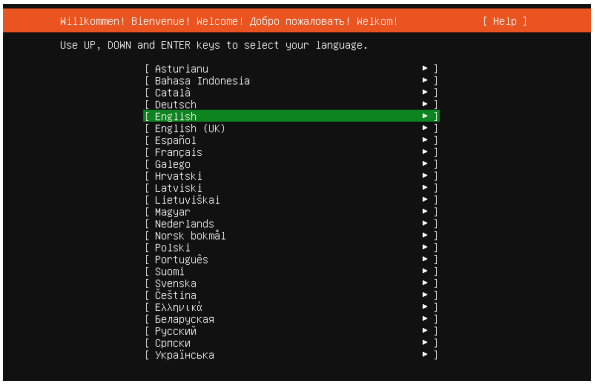
No	Perangkat Keras / Lunak	Spesifikasi	Jumlah
1	Web Server (Server PPDB)	Processor : CPU 1 Core RAM : 2 GB Penyimpanan : SSD 120 GB Sistem Operasi : Ubuntu Server 20.04	1
2	Web Server (Log Server)	Processor : CPU 1 Core RAM : 1 GB Penyimpanan : SSD 25 GB Sistem Operasi : Ubuntu Server 20.04	1
3	PC/Laptop (Client)	Processor : Intel Celeron RAM : 4 GB Penyimpanan : SSD 120 GB Sistem Operasi : Windows 11	1
4	Apache2	-	
5	PHP7.4	-	
6	MySql	-	
7	phpMyadmin	-	
8	Git (Github)	-	
9	HIHAT v1.1	PHP5.0, MySql	

4.3. Implementasi Dan Konfigurasi

Pada tahap implementasi dan konfirgurasi, peneliti akan melakukan proses instalasi server terlebih dahulu kemudian diikuti dengan konfigurasi-konfigurasi yang dibutuhkan di server PPDB yaitu apache2, php, mysql, phpmyadmin, git dan lainnya. Juga pada server Log yang dibutuhkan yaitu konfigurasi apache2, php, mysql, phpmyadmin dan lainnya. Setelah instalasi dan konfigurasi telah selesai dilakukan, selanjutnya adalah proses implementasi website PPDB Online pada server PPDB, diikuti dengan mengimplementasikan metode honeypot kedalam sistem ppdb online tersebut. Berikut ini peneliti akan menjelaskan secara rinci tahap-tahap instalasi ataupun konfigurasinya adalah sebagai berikut:

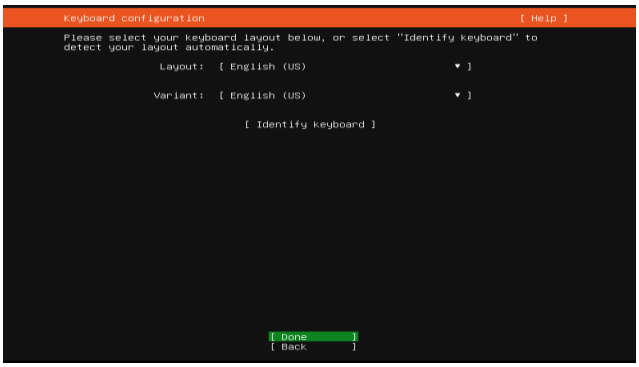
4.2.1. Instalasi Dan Konfigurasi Server PPDB

Untuk langkah awal adalah instalasi sistem operasi server PPDB menggunakan sistem operasi ubuntu server 20.04, sebelum melakukan proses instalasi sistem operasi hal yang pertama dilakukan adalah mempersiapkan media installernya. Jika proses sudah berjalan maka tampilan awal instalasi akan tampak seperti gambar dibawah ini.



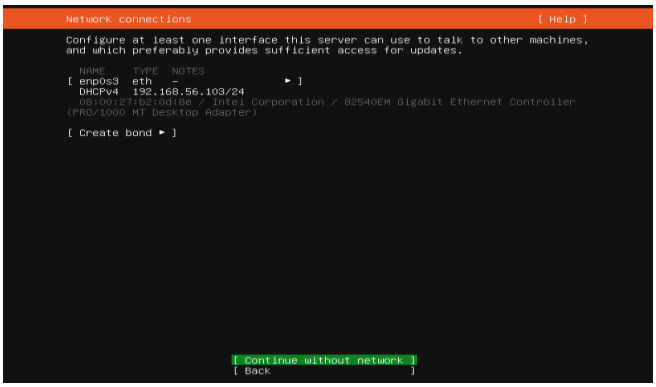
Gambar 4.2 Tampilan pemilihan bahasa pada proses instalasi sistem operasi server PPDB

Tampilan diatas merupakan pemilihan bahasa pada proses instalasi, pada opsi ini pilih dengan menggunakan tombol atas bawah untuk mengganti pilihan kemudian tekan tombol enter untuk memilih dan melanjutkan.



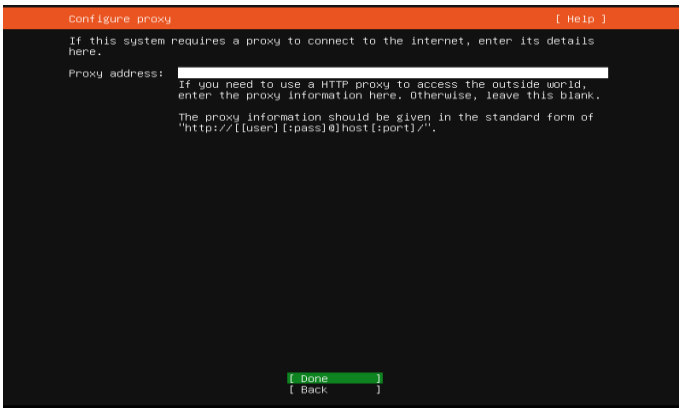
Gambar 4.3 Tampilan pemilihan keyboard

Pada pilihan keyboard peneliti lansung tekan enter saja untuk melanjutkan proses instalasi.



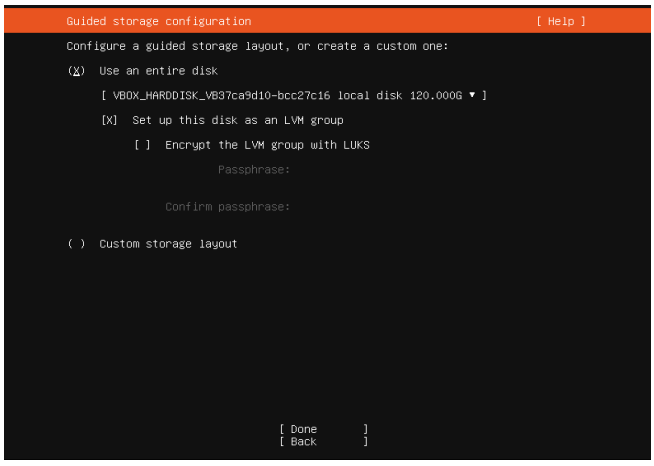
Gambar 4.4 Tampilan pilihan koneksi jaringan

Tampilan diatas merupakan pilihan koneksi jaringan yang tersedia pada server PPDB. Pilih koneksi jaringan dan tekan enter.



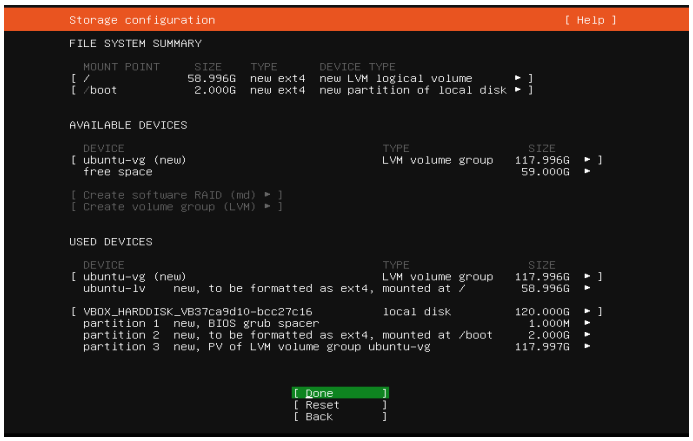
Gambar 4.5 Tampilan Proxy Address

Pada tahap ini peneliti kosongkan pada *field Proxy Address*, langsung saja tekan enter pada pilihan *Done*. Dan juga pada tampilan *mirror address* juga langsung saja tekan enter pada pilihan *Done*.



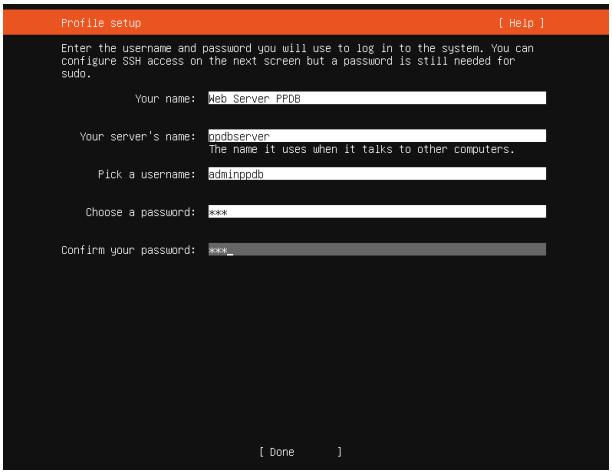
Gambar 4.6 Tampilan konfigurasi pemartisian pada penyimpanan

Disini peneliti pilih pada pilihan yang paling atas yaitu “Use an entire disk”, dimana nantinya sistem akan melakukan pemartisian secara otomatis. Jika ingin melakukan pemartisian secara custom dapat memilih pilihan “Custom storage layout”, selanjutnya pilih Done tekan tombol enter.



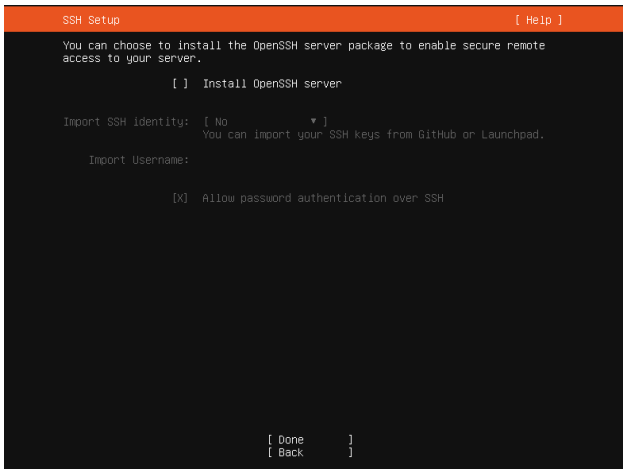
Gambar 4.7 Tampilan konfigurasi pemartisian
(Detail partisi yang akan dibuat)

Kemudian akan tampil detail partisi yang akan dibuat, dari gambar diatas tampak beberapa partisi yang akan dibuat yaitu partisi root (/) dengan volume 58.996Gb, /boot 2.00Gb. Jika dianalisa kembali pada partisi-partisi tersebut, masih ada ruang kosong yang tidak terpakai yaitu sebanyak 59.00Gb. Untuk itu peneliti menyarankan agar pemartisian dilakukan secara “Custom storage layout”, dengan ini dapat dimaksimalkan seluruh kapasitas hardisk ke partsisi root.



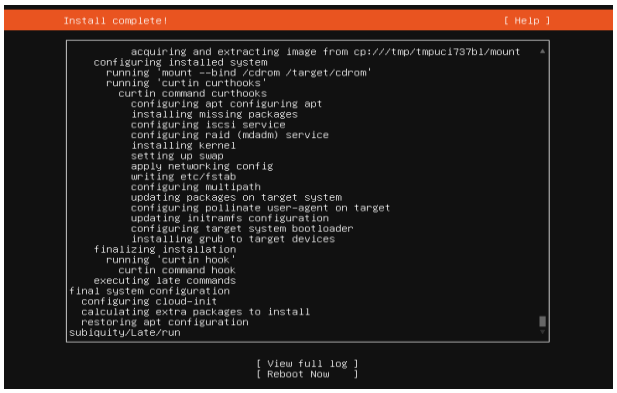
Gambar 4.8 Tampilan Profile Setup

Pada gambar diatas merupakan form pembuatan akun/profile untuk pengguna server. Buat akun dengan mengisi pada field-field tersebut.



Gambar 4.9 Tampilan Profile Setup

Pilih Install OpenSSH Server kemudian pilih Done untuk memasang OpenSSH Server. Selanjutnya tinggal menunggu proses instalasi selesai, dapat dilihat pada gambar dibawah ini.



Gambar 4.10 Proses instalasi berjalan

Jika proses instalasi telah selesai dilakukan, selanjutnya kita akan boot ulang atau restart mesin untuk masuk ke sistem yang telah diinstall tadi.

Gambar 4.11 Tampilan login awal pada server PPDB

Setelah restart maka tampilan awal yaitu login ke server, masukkan username dan password yang telah dibuat pada instalasi. Jika berhasil, maka tampilan server dapat dilihat seperti gambar dibawah ini.

Gambar 4.12 Tampilan ketika sudah masuk pada server PPDB

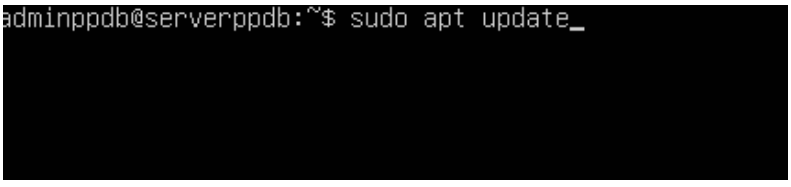
Pertama kali setelah proses instalasi selesai adalah melakukan konfirgurasi jaringan yaitu *ip address* dengan menjalankan perintah "sudo nano /etc/netplan/00-installer-config.yaml". Kemudian lakukan konfigurasi *ip adresss* menjadi seperti gambar dibawah ini.

Gambar 4.13 Konfigurasi IP Address

Jika sudah selesai tekan tombol "CTRL+O" kemudian tekan enter, kemudian tekan tombol "CTRL+X" lalu tekan enter. Selanjutnya jalankan perintah "sudo netplan apply" untuk mengaktifkan setingan *ip address* tersebut.

Untuk selanjutnya adalah langkah-langkah dalam instalasi dan konfigurasi Apache2, php, mysql, phpMyadmin, git dan lainnya. Yang pertama adalah instalasi dan konfigurasi Apache2. Apache2 adalah sebuah perangkat lunak *server web* yang bersifat *open-source* dan dapat dijalankan pada berbagai sistem operasi. Perangkat lunak ini berfungsi untuk melayani permintaan-permintaan dari klien melalui protokol HTTP (*Hypertext Transfer Protocol*) dan HTTPS (*Hypertext Transfer Protocol Secure*), serta memungkinkan pengguna untuk mengakses dan mengelola berbagai jenis konten *web* seperti halaman *web*, gambar, video, dan file lainnya.

Lanjut pada instalasi apache2, setelah selesai instalasi pada sistem operasi ubuntu *server* dan konfigurasi *ip address* sampai pada *server* telah terhubung dengan koneksi internet agar dapat melakukan instalasi dan konfigurasi. Sebelum melakukan instalasi apache2 terlebih dahulu melakukan perintah *update* atau memperbaharui *local package index* agar nantinya perintah-perintah untuk melakukan instalasi *pakage* yang dibutuhkan dapat diperbaharui. Caranya adalah dengan melakukan perintah "sudo apt update", kemudian tunggu sampai prosesnya selesai.

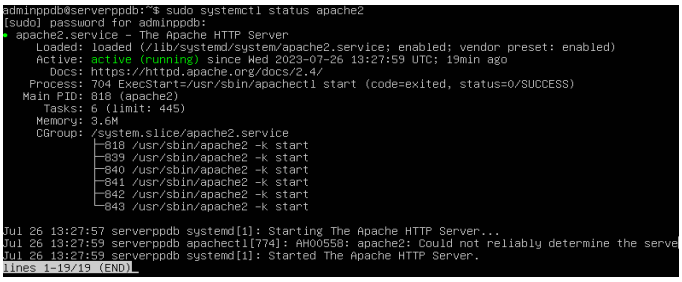


Gambar 4.14 Update Local Package Index

Setelah proses update selesai, selanjutnya dapat melakukan instalasi apache2 dengan menjalankan perintah "sudo apt install apache2". Jika ada pilihan

yes atau no pada konfirmasi instalasi, tekan tombol Y untuk setujui melanjutkan proses instalasi lalu tekan enter, kemudian tunggu hingga prosesnya selesai.

Jika proses instalasi telah selesai, langkah selanjutnya adalah menjalankan perintah “sudo ufw allow 'Apache'” agar firewall mengizinkan apache2 diakses oleh perangkat jaringan lain. Selanjutnya jalankan perintah “sudo systemctl status apache2”, untuk melihat apakah apache2 tersebut sudah running atau belum. Jika belum jalankan perintah “sudo systemctl enable apache2” kemudian jalankan juga perintah “sudo systemctl start apache2” untuk menjalankan apache2. Dan apabila apache2 telah berjalan maka akan tampak pada gambar dibawah ini.



Gambar 4.15 Apache2 berhasil berjalan

Setelah apache2 terpasang dan berjalan, selanjutnya adalah instalasi php7.4. Alasan peneliti menggunakan php7.4 adalah php versi tersebut dapat menjalankan source code PPDB Online yang akan diimplementasikan. Kembali ke proses instalasi php7.4 pertama kali menjalankan perintah “sudo apt -y install software-properties-common” dimana perintah ini untuk manajemen tambahan sumber perangkat lunak. Setelah prosesnya selesai kemudian jalankan perintah “sudo add-apt-repository ppa:ondrej/php” untuk menambahkan alamat repository php agar dapat menjalankan perintah instalasi php tersebut, kemudian jalankan perintah “sudo apt update” untuk memperbaharui repository pada apt. Selanjutnya barulah dapat menjalankan perintah instalasi php tersebut yaitu dengan perintah

“sudo apt -y install php7.4”, tunggu hingga proses instalasi tersebut selesai. Setelah proses instalasi tersebut selesai, lakukan pengecekkan instalasi dengan menjalankan perintah “php –v” maka akan tampil seperti gambar dibawah ini.

Gambar 4.16 Instalasi php7.4 telah berhasil

Selanjutnya adalah proses instalasi modul-modul yang secara umum dibutuhkan dalam menjalankan *source code* berbasis php, dengan menjalankan perintah “sudo apt install -y php7.4-cli php7.4-json php7.4-common php7.4-mysql php7.4-zip php7.4-gd php7.4-mbstring php7.4-curl php7.4-xml php7.4-bcmath”. Berikut ini merupakan penjelasan pada modul-modul tersebut:

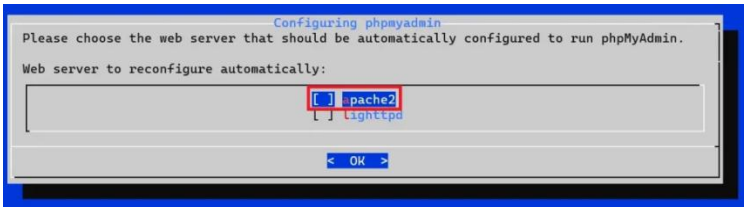
1. php7.4-cli - penerjemah perintah, berguna untuk menguji skrip PHP dari shell atau melakukan tugas skrip shell umum
2. php7.4-json - untuk bekerja dengan data JSON
3. php7.4-common - dokumentasi, contoh, dan modul umum untuk PHP
4. php7.4-mysql - untuk bekerja dengan database MySQL
5. php7.4-zip - untuk bekerja dengan file terkompresi
6. php7.4-gd - untuk bekerja dengan gambar
7. php7.4-mbstring - digunakan untuk mengelola string non-ASCII
8. php7.4-curl - memungkinkan Anda membuat permintaan HTTP di PHP
9. php7.4-xml - untuk bekerja dengan data XML
10. php7.4-bcmath - digunakan saat bekerja dengan pelampung presisi

Jalankan perintah “php -m” untuk melihat modul-modul yang sudah tersedia pada php.

Tahap selanjutnya adalah instalasi mysql-server, jalankan perintah “sudo apt install mysql-server”, konfirmasi pemasangan dan tunggu hingga prosesnya selesai. Jika proses instalasi selesai jalankan perintah “sudo systemctl start mysql.service” untuk menjalankan mysql-server.

Langkah selanjutnya adalah instalasi phpMyadmin. phpMyAdmin adalah sebuah aplikasi *web open-source* yang menyediakan antarmuka grafis untuk mengelola *database* MySQL. Dengan menggunakan phpMyAdmin, pengguna dapat dengan mudah melakukan tugas-tugas administrasi seperti membuat, menghapus, dan mengubah struktur tabel, serta mengelola isi dari tabel-tabel tersebut melalui *browser web* dengan sederhana dan efisien.

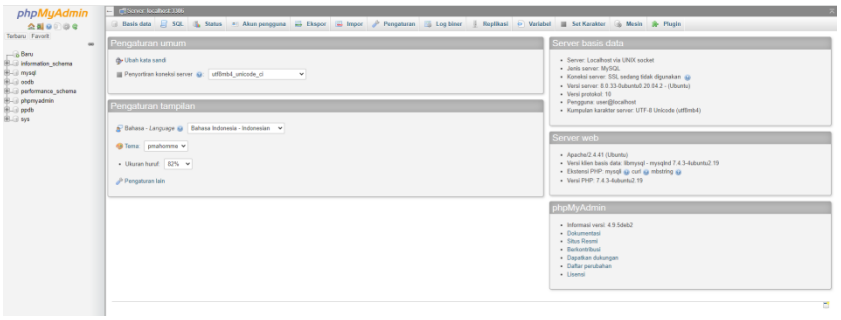
Untuk instalasi phpMyadmin jalankan perintah “sudo apt-get install phpmyadmin” tunggu hingga prosesnya selesai dan akan sampai pada tahap dimana ada pilihan web server yaitu apache2 dan lighhttpd, pilih apache2 denga menekan tombol space dan tekan tombol enter untuk melanjutkan.



Gambar 4.17 Pilihan Web Server pada instalasi phpMyadmin

Selanjutnya akan ditanya apakah ingin mengkonfigurasi database, disini pilih yes tekan enter, kemudian masukkan password untuk phpmyadmin lalu tekan enter, tunggu hingga proses instalasi tersebut sampai selesai. Jika proses instalasi telah selesai, masukkan “192.168.43.77/phpmyadmin” untuk mengakses

phpmyadmin dengan menggunakan web browser pada computer client. Pada tampilan awal phpmyadmin adalah tampilan halaman login, untuk masuk pada dashboard phpmyadmin login menggunakan akun root dan passwordnya adalah password yang telah diinputkan pada instalasi phpmyadmin tersebut.



Gambar 4.18 Tampilan dashboard phpMyadmin

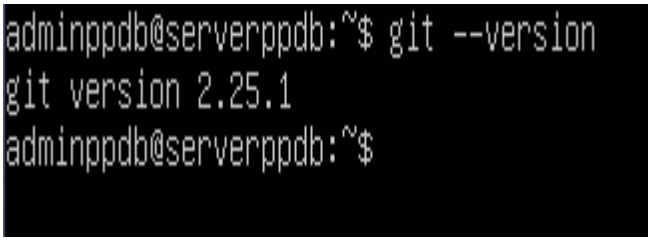
Selanjutnya adalah instalasi Git, Git adalah sebuah sistem kontrol versi distribusi terdistribusi yang digunakan untuk mengelola dan melacak perubahan pada kode sumber perangkat lunak atau proyek pengembangan perangkat lunak. Git lebih disukai daripada FTP karena merupakan sistem kontrol versi yang canggih dan terdistribusi.

Dibandingkan dengan FTP (File Transfer Protocol) yang hanya berfungsi sebagai protokol untuk mentransfer file, Git menawarkan kemampuan untuk melacak perubahan dalam kode sumber dan mengelola versi dari proyek perangkat lunak. Dengan Git, setiap perubahan yang dilakukan pada kode dapat dicatat secara terperinci, sehingga memudahkan para pengembang untuk mengidentifikasi dan mengatasi masalah yang muncul. Selain itu, Git memungkinkan bekerja secara kolaboratif dan mengelola cabang (branch) kode, sehingga memungkinkan tim pengembang untuk bekerja secara efisien dan aman pada fitur-fitur terpisah tanpa mengganggu kode utama.

FTP hanya menyediakan mekanisme transfer file, yang berarti sulit untuk melacak perubahan pada kode atau mengelola versi dari proyek. Ini membuat kolaborasi antara pengembang lebih rumit dan meningkatkan risiko terjadinya konflik file. Selain itu, FTP tidak menyediakan fitur-fitur yang memungkinkan pemulihan kode ke versi sebelumnya, yang dapat menghambat proses pengembangan dan memakan waktu jika terjadi kesalahan yang perlu diperbaiki.

Dengan demikian, Git memberikan fleksibilitas, keamanan, dan kemudahan dalam pengelolaan proyek perangkat lunak yang tidak dapat disaingi oleh FTP sebagai alat kontrol versi. Dari kesimpulan ini, peneliti memutuskan menggunakan Git sebagai transfer file serta manajemen perubahan source code secara rinci, sehingga jika sewaktu-waktu nantinya akan dilakukan pengembangan sistem PPDB Online SD Muhammadiyah 03 Sibolga lebih lanjut, dapat lebih mudah dalam proses deployment ke server tanpa harus secara manual melakukan replacement source code seperti yang dilakukan jika menggunakan FTP.

Kembali ke tahap instalasi Git, jalankan perintah “sudo apt install git”, kemudian tunggu hingga prosesnya selesai. Jika proses instalasi telah selesai jalankan perintah “git --version” untuk cek versi git yang telah terpasang.



Gambar 4.19 Versi Git yang terpasang

4.2.2. Instalasi Dan Konfigurasi Server Log

Pada dasarnya instalasi sistem operasi server log sama dengan instalasi server PPDB. Untuk lebih jelasnya, fungsi dari server log adalah hanya sebagai database server untuk data log dari honeypot HiHAT. Menurut panduan dari instalasi honeypot HiHAT (Alat Analisis Honeypot Interaksi Tinggi) yaitu pada halaman website resminya disebutkan bahwa.

"Logserver perlu disiapkan. Ingat, menurut arsitektur honeynet berbasis web, server log ini tidak boleh berupa honeypot atau terletak di dalam honeynet itu sendiri". Maka dari itu peneliti memutuskan untuk instalasi dan konfigurasi yang dibutuhkan pada server log adalah Apache2, php, mysql-server dan phpmyadmin.

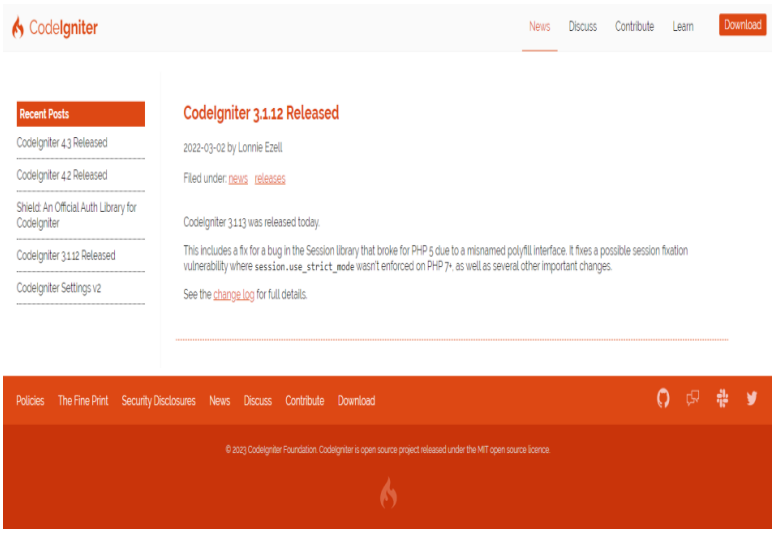
4.2.3. Implementasi Sistem Informasi PPDB Online SD Muhammadiyah 03 Sibolga

Untuk tahap implementasi Sistem Informasi PPDB Online SD Muhammadiah 03 Sibolga, beberapa hal yang dibutuhkan agar PPDB Online dapat berjalan yakni apache2, php dan mysql-server. Apache2 merupakan web server yang digunakan untuk menjalankan server web ppdb online, kemudian php berfungi sebagai perangkat lunak yang menjalankan bahasa pemrograman php karena sistem PPDB Online tersebut dibangun dengan bahasa pemrograman php, dan yang terakhir adalah mysq-server berfungsi sebagai penyimpanan data-data yang dipakai oleh sistem PPDB Online tersebut.

Pada proses konfigurasi atau implementasi sistem PPDB Online SD Muhammdiyah 03 Sibolga, beberapa hal yang dibutuhkan seperti text editor, Git, phpMyadmin. Text editor merupakan perangkat lunak yang digunakan untuk memperbaharui syntax atau melakukan sebuah perubahan pada source code sistem

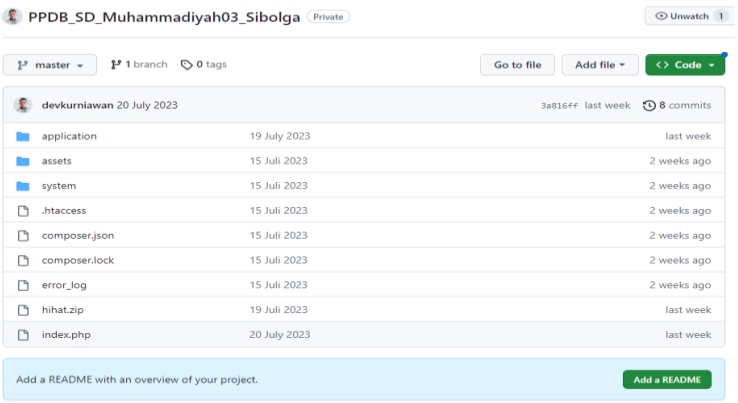
PPDB Online. Git merupakan program perangkat lunak yang digunakan untuk mendeploy sistem PPDB Online ke web server PPDB Online SD Muhammadiyah 03 Sibolga, dengan menggunakan Git proses deploy ke serve menjadi lebih mudah dan praktis tanpa harus secara manual mereplace file-file yang telah dirubah pada web server PPDB. Sistem PPDB Online yang akan diimplementasikan dibangun menggunakan bahasa pemrograman php, lebih tepatnya dibangun menggunakan framework php yaitu Codeigniter 3.

CodeIgniter adalah sebuah framework aplikasi web berbasis PHP yang bersifat open-source dan menerapkan pola desain Model-View-Controller (MVC). Tujuan utama dari CodeIgniter adalah untuk mempercepat proses pengembangan aplikasi web dengan menyediakan seperangkat fitur dan fungsi yang kuat serta mudah digunakan. Peneliti juga menganalisa bagaimana sistem yang telah dibangun menggunakan framework tersebut dapat berjalan dengan baik, maka dari itu peneliti menggunakan php7.4. Dimana Codeigniter 3 *compatible* atau dapat berjalan dengan baik pada php versi 7.x.



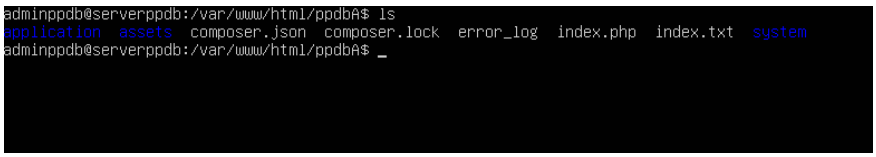
Gambar 4.20 Situs framework php Codeigniter

Tahap pertama untuk melakukan implementasi adalah melakukan push source code ke repository github. Berikut ini merupakan tampilan dimana source code tersebut telah terunggah pada repository github.



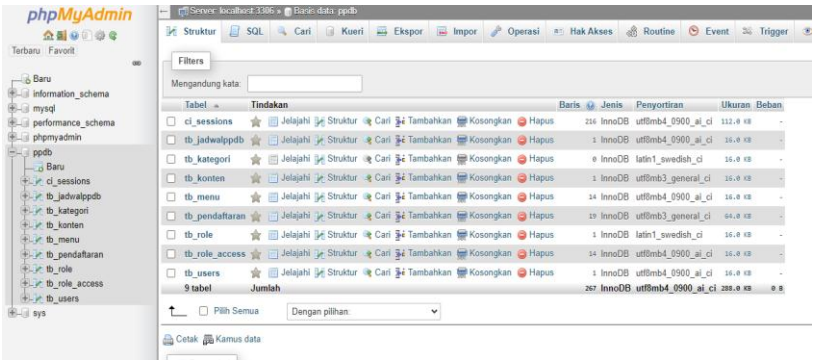
Gambar 4.21 Repository Source Code Sistem PPDB Onilne

Langkah selanjutnya pada sisi server PPDB, jalankan perintah “sudo su” terlebih dahulu untuk masuk ke mode super user. Selanjutnya jalankan perintah “cd /var/www/html/ppdbA” untuk masuk terlebih dahulu ke folder root sistem PPDB online tersebut, lalu jalankan perintah “git init” untuk menginisiasikan git kedalam folder tersebut, jalankan perintah “git remote set-url origin [alamat_repository]” untuk menetapkan alamat repository, kemudian jalankan perintah “git pull” kemudian akan diperintahkan masuk menggunakan akun github kemudian proses download akan berlangsung. Jika pull berhasil, cek directory pada root sistem PPDB dengan menjalankan perintah “ls -a”. Lalu seluruh source code akan tampil seperti gambar dibawah ini.



Gambar 4.22 Source code Sistem Informasi PPDB onilne pada web server

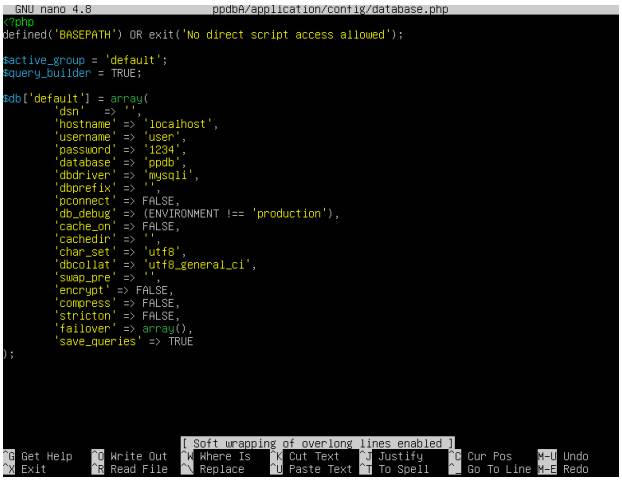
Langkah selanjutnya adalah konfigurasi database, untuk melakukan konfigurasi database langkah pertama adalah import file sql menggunakan phpmyadmin. Login terlebih dahulu ke phpmyadmin, kemudian pilih menu Basis Data (*Database*) kemudian pada bagian buat baru Basis Data, masukkan nama database yang akan dibuat kemudian klik tombol buat. Setelah berhasil membuat database, langkah selanjutnya ialah import file sql database PPDB yang sudah dibuat sebelumnya. Caranya yang pertama adalah klik terlebih dahulu database yang sudah berhasil dibuat tadi pada menu sidebar sebelah kiri, lalu klik menu import yang terletak pada menu bagian atas klik field file dan pilih file sql tersebut pada berkas computer lalu klik ok, kemudian klik kirim. Jika berhasil maka dapat dicek seluruh table yang berhasil diimportkan tadi seperti pada gambar dibawah ini.



Gambar 4.23 phpMyadmin Database
Sistem Informasi PPDB onilne

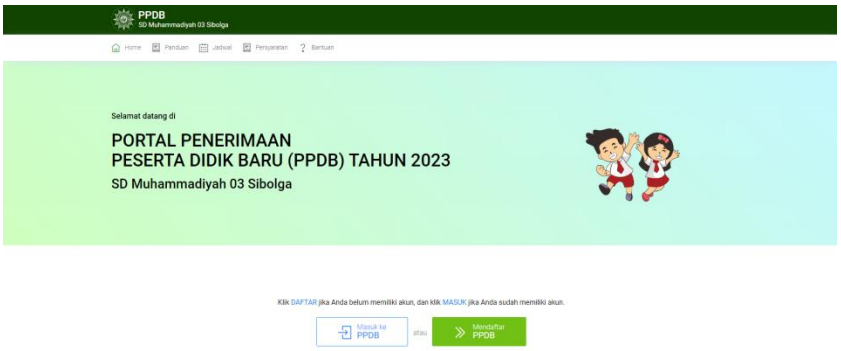
Untuk pembuatan database telah berhasil, kemudian langkah selanjutnya adalah konfigurasi *source code* database Sistem PPDB Onine SD Muhammadiya 03 Sibolga. Yang pertama adalah pada server web PPDB buka file database.php untuk diubah *source code* tersebut, jalankan perintah "sudo nano

/var/www/html/ppdabA/application/config/database.php", jika sudah selesai simpan perubahan dengan menekan tombol CTRL+O lalu tekan enter, lalu akan tampil *source code* dan diubah sesuai dengan gambar dibawah ini.



Gambar 4.24 Konfigurasi database pada source code PPDB

Kemudian pada client buka browser kemudian akses 192.168.43.77 (ip web server PPDB) lalu hasil nya akan tampil seperti gambar dibawah ini yang merupakan halaman utama Sistem Informasi PPDB Online 03 Sibolga, yang berarti konfirgurasi telah selesai dilakukan.



Gambar 4.25 Konfigurasi berhasil, halaman utama Sistem Informasi PPDB Online SD Muhammadiyah 03 Sibolga

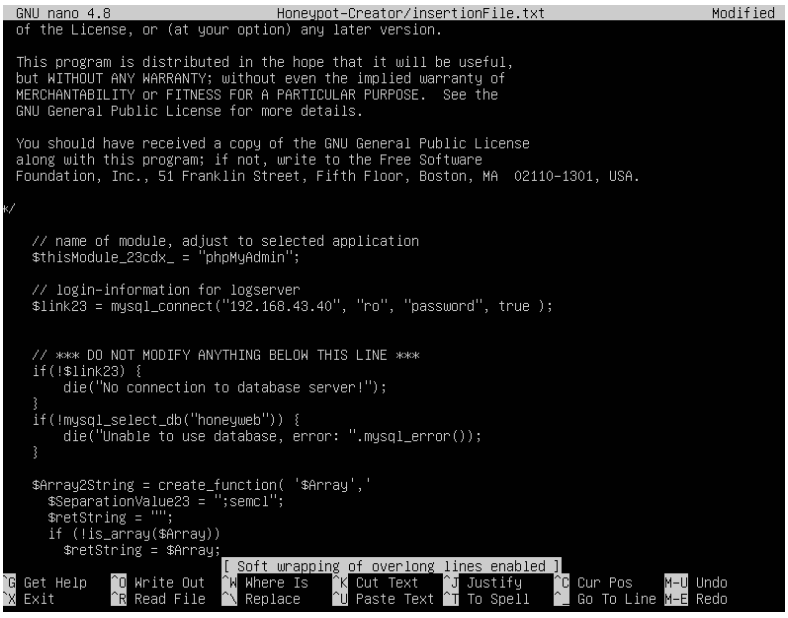
4.2.4. Implementasi Honeypot HiHAT Pada Sistem Informasi PPDB Online SD Muhammadiyah 03 Sibolga

Impelementasi honeypot HiHAT pada sistem informasi PPDB Online SD Muhammadiyah 03 Sibolga dimulai dari mengunduh *source code* honeypot HiHAT pada situs resminya yang dapat diakses pada link. Secara singkat tersedia juga panduan atau pedoman bagaimana cara melakukan instalasi honeypot HiHAT tersebut. Dari panduan tersebut, peneliti menyimpulkan kembali bahwa langkah pertama adalah menyiapkan logserver dengan memperhatikan arsitektur *honeynet* berbasis *web*. Penting untuk diingat bahwa *server log* ini tidak boleh berfungsi sebagai *honeypot* atau ditempatkan di dalam *honeynet* itu sendiri. Pastikan logserver telah dikonfigurasi dengan baik. Ini melibatkan penginstalan sistem minimalis hanya dengan perangkat lunak dan alat yang benar-benar diperlukan untuk menjalankan *honeypot*. Selain itu, nonaktifkan atau hapus semua layanan yang tidak diperlukan untuk menciptakan sistem yang minimalis. Agar sistem lebih aman, pastikan untuk mengunduh semua pembaruan yang tersedia, sehingga sistem tetap terkini baik saat instalasi maupun selama penggunaan.

Peneliti akan melakukan konfigurasi honeypot menggunakan pedoman dari situs resmi honeypot HiHAT adalah sebagai berikut.

1. Terlebih dahulu download source code pada situs resmi HiHAT.
2. Memilih aplikasi web berbasis PHP yang ingin dijadikan honeypot (modul) berbasis web dan simpan kode sumber aplikasi tersebut dalam sebuah direktori. Pastikan untuk memberikan izin tulis pada direktori untuk proses transformasi. Sebelumnya peneliti melakukan backup terlebih dahulu directory “ppdbA/” menjadi “ppdbB/”.

3. Konfigurasi nama modul Honeypot-Creator dengan cara membuka file "insertionFile.txt" dan mengganti isi variabel "$thisModule_23cdx_" dengan nama modul yang diinginkan. Ingatlah bahwa nama modul ini akan mengidentifikasi honeypot pada proses analisis selanjutnya, sehingga harus sesuai dengan nama file modul di alat analisis, disini peneliti menggunakan directory “ppdbB”, sebagai folder backup adalah directory “ppdbB”.
4. Tetapkan informasi login untuk database SQL di server log. Caranya, buka file "insertionFile.txt" dengan cara menjalankan perintah “nano /var/www/html/ppdbB” dan ubah alamat server, nama pengguna, dan kata sandi pada baris "$link23 = mysql_connect" di bagian awal file, kemudian simpan dengan menekan tombol CTRL+O. Hasil akhir konfigurasinya adalah seperti pada gambar dibawah ini.



Gambar 4.26 Konfigurasi insertionFile.txt

5. Instal Java Runtime Environment versi 1.4x atau yang lebih tinggi. Jalankan perintah “sudo apt install default-jre”, kemudian tunggu proses instalasi selesai. Selanjutnya jika instalasi selesai jalankan perintah “java -version” untuk melihat versi java yang sudah terinstall. Akan tampak seperti gambar dibawah ini.

Gambar 4.27 Konfigurasi insertionFile.txt

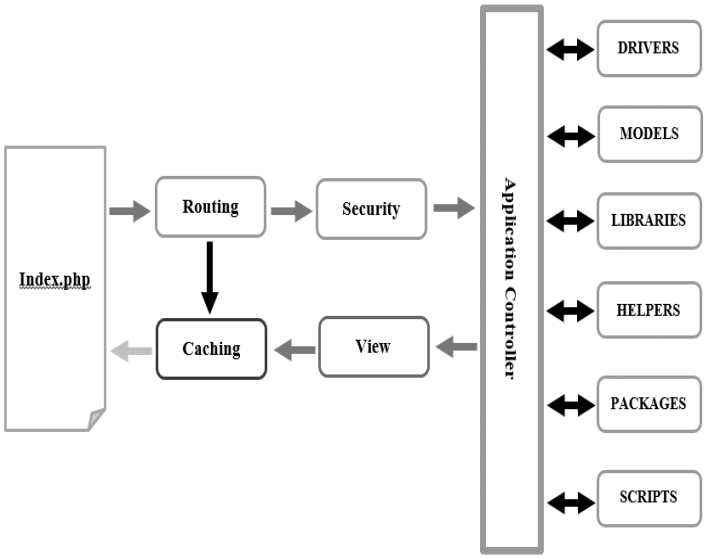
6. Jalankan Honeypot-Creator dengan mengetikkan perintah "java honeypot_creator XXX", dimana "XXX" adalah direktori tempat aplikasi web berbasis PHP berada. Disini menjalankan perintah "java honeypot_creator /var/www/html/ppdbB/". Pastikan juga izin tulis telah diizinkan pada direktori untuk proses transformasi.

Gambar 4.28 Proses Transformasi Selesai

Setelah peneliti melakukan analisa hasil dari implementasi honeypot HiHAT sesuai dengan pedoman dari situs web resminya, dan jika melihat kembali bahwa sistem informasi PPDB SD Muhammadiyah 03 Sibolga dibangun menggunakan bahasa pemrograman php yang sudah berbentuk framework lebih tepatnya Codeigniter 3, artinya apabila dilihat dari struktur file-file yang dibangun pada framework tersebut yang membentuk satu kesatuan, juga dengan konsep

pemrograman yang berbeda framework Codeigniter 3 dibangun dengan menggunakan konsep pemrograman OOP (Object Oriented Programming), dimana ini sangat berbeda dengan source code yang ada pada HiHAT yang masih menggunakan konsep pemrograman native. Adapun beberapa temuan kendala-kendala peneliti dalam melakukan implementasi HiHAT pada sistem informasi PPDB Online SD Muhammdiyah 03 Sibolga:

1. Versi php yang berbeda, dimana honeypot HiHAT masih menggunakan versi php yang lama yakni php versi kurang dari 5.0, sedangkan Codeigniter 3 sudah berjalan pada versi php5.6 – 7.4. Kendalanya adalah beberapa fungsi-fungsi php versi lama tersebut sudah dihapus pada pembaharuan versi php yang terbaru, dimana php versi 7.4 dipilih agar dapat menjalankan sistem PPDB Online yang menggunakan framework Codeigniter tersebut.
2. Konsep pemrograman yang berbeda, sistem PPDB menggunakan php framework dengan konsep pemrograman OOP (Object Oriented Programming) sedangkan HiHAT masih menggunakan native. Hal ini menjadi kendala dikarenakan proses implementasi tersebut menggunakan program berbasis java yang akan melakukan proses *generate* mengubah seluruh file php yang ada pada *directory* maupun sub-sub *directory*. Ini akan menjadikan *duplicate action* pada setiap requestnya. Hal ini akan menjadikan server tidak optimal dan menjadi lambat.



Gambar 4.29 Workflow Codeigniter 3

Dari gambar 4.26 dapat dilihat workflow dari codeigniter 3, pada setiap halaman yang akan diakses akan melalui file “index.php“ terlebih dahulu kemudian melewati tahap routing hingga sampai ke controller yang merupakan basis dari halaman-halaman yang dibuat. Ini berarti “index.php” tersebut merupakan file utama yang dapat diimplementasikan source code HiHAT tanpa harus melakukan generate ke seluruh file php yang dapat mengakibatkan *duplicate action* nantinya. Akhirnya peneliti menggunakan cara alternatif ini untuk implementasi honeypot HiHAT pada sistem PPDB Online SD Muhammdiyah 03 Sibolga.

Langkah pertama adalah menyalin “insertionFile.txt” ke file index.php pada directory root PPDB. Source pada “insertionFile.txt” merupakan source code yang nantinya akan degenerate dengan menjalankan program java yang akan mengeksekusi proses pengubahan source code php pada semua file-file php yang ada pada directory maupun sub directory pada aplikasi yang akan

diimplementasikan. Gambar dibawah ini merupakan sebagian dari source code HiHAT yang telah dicopy kedalam file “index.php”.

```php
// for each of these arrays:  read out last entry to avoid duplicates + add data if no duplicate
foreach ( $dbArrays AS $dbKeyArray => $dbValueArray ) {

    // $arrayContent_23cdx_[ $dbKeyArray ] = $Array2String( $dbValueArray );
    $arrayContent_23cdx_[ $dbKeyArray ] = cv_data( $dbValueArray );

}

$ip_23cdx_      =  isset( $_SERVER['REMOTE_ADDR'] ) ? $_SERVER['REMOTE_ADDR'] : "";
$browser_23cdx_ =  isset( $_SERVER['HTTP_USER_AGENT'] ) ? $_SERVER['HTTP_USER_AGENT'] : "";
$source_23cdx_  =  isset( $_SERVER['PHP_SELF'] ) ? $_SERVER['PHP_SELF'] : "";


$duplicateCounter_23cdx_ = 0;

// checks if same script has made same data-entry
$sql_23cdx_ = "SELECT Source, Value_Server, Value_Get, Value_Post, Value_Cookie, Module FROM main_logs
               WHERE
                     Value_Server = '".addslashes( htmlentities ( $arrayContent_23cdx_[ 0 ] , ENT_QUOTES )).
              "' AND Value_Get =    '".addslashes( htmlentities ( $arrayContent_23cdx_[ 1 ] , ENT_QUOTES )).
              "' AND Value_Post =   '".addslashes( htmlentities ( $arrayContent_23cdx_[ 2 ] , ENT_QUOTES )).
              "' AND Value_Cookie = '".addslashes( htmlentities ( $arrayContent_23cdx_[ 3 ] , ENT_QUOTES )).
              "' AND Module       = '".addslashes( htmlentities ( $thisModule_23cdx_ , ENT_QUOTES )).
              "' AND Source =       '".addslashes( htmlentities ( $source_23cdx_ , ENT_QUOTES)). "'";

$result_23cdx_ = $conn->query($sql_23cdx_);
while($row23 = mysqli_fetch_array($result_23cdx_)) {
    $duplicateCounter_23cdx_++;
}
```

Gambar 4.30 Source Code HiHAT Pada index.php

Dengan melakukan beberapa konfigurasi serta mengubah beberapa fungsi php versi lama menjadi fungsi php versi 7.4, fungsi-fungsi lama tersebut seperti mysql_connect(), mysql_select_db(), mysql_fetch_assoc(), mysql_num_rows(), create_function() dan lain-lain. Beberapa fungsi tersebut sudah tidak dapat lagi berjalan pada php versi 7.4 yang digunakan pada *server* PPDB SD Muhammadiyah 03 Sibolga, dengan demikian harus dilakukan pembaharuan dengan menyesuaikan versi php yang dipakai.

Yang pertama adalah mengubah source code koneksi database, disini sebelumnya menggunakan fungsi mysql_connect() dan mysql_select_db(), kemudian diganti dengan new mysqli() yang merupakan modul mysql yang dapat berjalan pada php versi 7.4 yang dipakai saat ini. Hasil dari konfigurasi tersebut dapat dilihat pada gambar dibawah ini.

```php
$host       = "192.168.43.40";
$username   = "ro";
$password   = "password";
$dbname     = "honeyweb";

$conn = new mysqli($host, $username, $password, $dbname); // Create connection
if (!$conn) die("Connection failed: " . $conn->connect_error()); // Check connection
```

Gambar 4.31 Mengubah fungsi konfigurasi database

Kemudian fungsi create_function() yang sudah di hapus pada versi php 7.4, diganti dengan menggunakan deklarasi function. Code akan terlihat seperti gambar dibawah ini.

```php
function cv_data($Array){
  $SeparationValue23 = ";semcl";
  $retString = "";
  if (!is_array($Array))
    $retString = $Array;
  else
    foreach ($Array as $Key => $Value) {
      if(is_array($Value)) {
        //$retString .="MULTI";
        foreach ($Value as $Key2 => $Value2)
          if(is_array($Value2)) {
            //$retString .="MULTI2 ";
            foreach ($Value2 as $Key3 => $Value3)
              if(is_array($Value3)) {
                  //$retString .="MULTI3 ";
                  foreach ($Value3 as $Key4 => $Value4)
                      if(is_array($Value4))
                          $retString .= "NO5DimArraySUPPORT";
                      else
                          $retString .= $Key4. "=".$Value4. $SeparationValue23;
              }
              else
                  $retString .= $Key3. "=".$Value3. $SeparationValue23;
          }
          else
              $retString .= $Key2. "=" .$Value2. $SeparationValue23;
      }
      else
        $retString .= $Key."=".$Value. $SeparationValue23;
    }
  return $retString;
}
```

Gambar 4.32 Mengubah fungsi create_function()

Selanjutnya adalah fungsi mysql_query() dan mysql_fetch_array() diganti dengan $conn->query() dan mysqli_fetch_array(). Menjadi terlihat pada gambar dibawah ini.

```php
$result_23cdx_ = $conn->query($sql_23cdx_);
while($row23 = mysqli_fetch_array($result_23cdx_)) {
    $duplicateCounter_23cdx_++;
}
```

Gambar 4.33 Mengubah fungsi query

Begitu juga fungsi mysql_query() lainnya yang diubah menjadi $conn->query(). Berikut ini merupakan gambar hasil akhir keseluruhan perubahan syntax HiHAT pada file index.php.

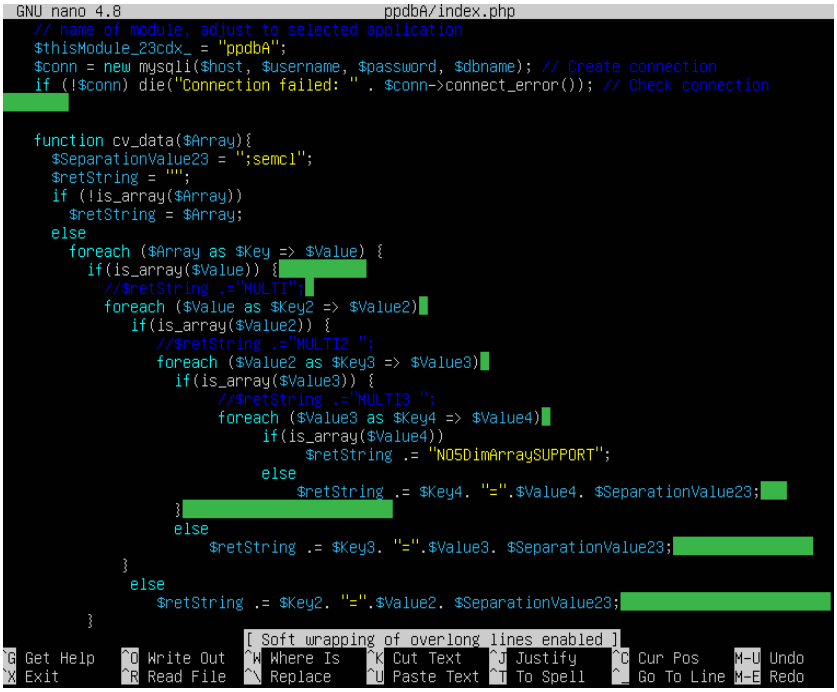
```php
<?php

/* This file is part of HIHAT v1.1
   ===============================
   Copyright (c) 2007 HIHAT-Project

  This program is free software; you can redistribute it and/or
  modify it under the terms of the GNU General Public License
  as published by the Free Software Foundation; either version 2
  of the License, or (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License
  along with this program; if not, write to the Free Software
  Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.

*/

    // name of module, adjust to selected application
    $thisModule_23cdx_ = "ppdbA";

    $host       = "192.168.43.40";
    $username   = "ro";
    $password   = "password";
    $dbname     = "honeyweb";

    $conn = new mysqli($host, $username, $password, $dbname); // Create connection
    if (!$conn) die("Connection failed: " . $conn->connect_error()); // Check connection


    function cv_data($Array){
      $SeparationValue23 = ";semcl";
      $retString = "";
      if (!is_array($Array))
        $retString = $Array;
      else
        foreach ($Array as $Key => $Value) {
          if(is_array($Value)) {
            //$retString .="MULTI";
            foreach ($Value as $Key2 => $Value2)
              if(is_array($Value2)) {
                  //$retString .="MULTI2 ";
                  foreach ($Value2 as $Key3 => $Value3)
                    if(is_array($Value3)) {
                        //$retString .="MULTI3 ";
                        foreach ($Value3 as $Key4 => $Value4)
                            if(is_array($Value4))
                                $retString .= "NO5DimArraySUPPORT";
                            else
                                $retString .= $Key4. "=".$Value4. $SeparationValue23;
                    }
                    else
                        $retString .= $Key3. "=".$Value3. $SeparationValue23;
              }
               else
                  $retString .= $Key2. "=".$Value2. $SeparationValue23;
          }
          else
            $retString .= $Key."=".$Value. $SeparationValue23;
        }
      return $retString;
    }

```

Gambar 4.34 Syntax HiHAT pada file index.php

```
68
69      // Select arrays to add to database
70      $dbArrays = array( $_SERVER, $_GET, $_POST, $_COOKIE );
71      $arrayContent_23cdx_[ 0 ] = "--"; // init array with nonsense
72
73      // read RAW post data
74      $rawData_23cdx_ = explode( "&", file_get_contents("php://input"));
75      $rawData2_23cdx_ = array();
76      foreach ( $rawData_23cdx_ AS $key_23cdx_ => $value_23cdx_ )  {      // put into form: key=value
77          $tempAr_23cdx_ = explode( "=", $rawData_23cdx_[$key_23cdx_], 2 );
78          if(count($tempAr_23cdx_) < 2) continue;
79          $rawData2_23cdx_[$tempAr_23cdx_[0]] = $tempAr_23cdx_[1];     // if identical keys exist: only last entry counts
80      }
81      foreach( $rawData2_23cdx_ AS $key2_23cdx_ => $value2_23cdx_)    // add to Post array if new stuff is found
82          if (!isset($_POST[$key2_23cdx_])) {
83              $_POST[ $key2_23cdx_ ] = $value2_23cdx_;
84          }
85
86      // for each of these arrays:  read out last entry to avoid duplicates + add data if no duplicate
87      foreach ( $dbArrays AS $dbKeyArray => $dbValueArray ) {
88
89          // $arrayContent_23cdx_[ $dbKeyArray ] = $Array2String( $dbValueArray );
90          $arrayContent_23cdx_[ $dbKeyArray ] = cv_data( $dbValueArray );
91
92      }
93
94      $ip_23cdx_      =  isset( $_SERVER['REMOTE_ADDR'] ) ? $_SERVER['REMOTE_ADDR'] : "";
95      $browser_23cdx_ =  isset( $_SERVER['HTTP_USER_AGENT'] ) ? $_SERVER['HTTP_USER_AGENT'] : "";
96      $source_23cdx_  =  isset( $_SERVER['PHP_SELF'] ) ? $_SERVER['PHP_SELF'] : "";
97
98
99      $duplicateCounter_23cdx_ = 0;
100
101     // checks if same script has made same data-entry
102     $sql_23cdx_ = "SELECT Source, Value_Server, Value_Get, Value_Post, Value_Cookie, Module FROM main_logs
103                    WHERE
104                         Value_Server = '".addslashes( htmlentities ( $arrayContent_23cdx_[ 0 ] , ENT_QUOTES )).
105                    "' AND Value_Get =     '".addslashes( htmlentities ( $arrayContent_23cdx_[ 1 ] , ENT_QUOTES )).
106                    "' AND Value_Post =    '".addslashes( htmlentities ( $arrayContent_23cdx_[ 2 ] , ENT_QUOTES )).
107                    "' AND Value_Cookie = '".addslashes( htmlentities ( $arrayContent_23cdx_[ 3 ] , ENT_QUOTES )).
108                    "' AND Module       = '".addslashes( htmlentities ( $thisModule_23cdx_ , ENT_QUOTES )).
109                    "' AND Source =       '".addslashes( htmlentities ( $source_23cdx_ , ENT_QUOTES)). "'";
110
111     $result_23cdx_ = $conn->query($sql_23cdx_);
112     while($row23 = mysqli_fetch_array($result_23cdx_)) {
113         $duplicateCounter_23cdx_++;
114     }
115
116     // add data of array to database
117     $sql_23cdx_ = "INSERT INTO main_logs ( attackerIP, attackerBrowser, Value_Server,
118                                            Value_Get, Value_Post,Value_Cookie, Source, Module ) VALUES
119                 ('".addslashes( htmlentities ( $ip_23cdx_, ENT_QUOTES))."',
120                 '".addslashes( htmlentities ( $browser_23cdx_, ENT_QUOTES)).'",
121                 '".addslashes( htmlentities ( $arrayContent_23cdx_[ 0 ], ENT_QUOTES)).'",
122                 '".addslashes( htmlentities ( $arrayContent_23cdx_[ 1 ], ENT_QUOTES)).'",
123                 '".addslashes( htmlentities ( $arrayContent_23cdx_[ 2 ], ENT_QUOTES)).'",
124                 '".addslashes( htmlentities ( $arrayContent_23cdx_[ 3 ], ENT_QUOTES)).'",
125                 '".addslashes( htmlentities ( $source_23cdx_, ENT_QUOTES)).'",
126                 '".addslashes( htmlentities ( $thisModule_23cdx_ , ENT_QUOTES )). "')";
127
128
129     if ( $duplicateCounter_23cdx_ == 0 & $arrayContent_23cdx_[ 0 ] != '' )     // don't add duplicates or empty fields
130         if ($conn->query($sql_23cdx_) !== TRUE)
131
132     $conn->close();
133
134      $value = "";
135      $key = "";
136      $max_23cdx_ = "";
137      $sql_23cdx_ = "";
138
139      $dbArrays = "";
140      $dbNameOfTargettable = "";
141  // */
142  ?>
143
144  <?php
145  /**
146   * CodeIgniter
147   *
148   * An open source application development framework for PHP
149   *
150   * This content is released under the MIT License (MIT)
151   *
152   * Copyright (c) 2014 - 2019, British Columbia Institute of Technology
153   *
154   * Permission is hereby granted, free of charge, to any person obtaining a copy
155   * of this software and associated documentation files (the "Software"), to deal
156   * in the Software without restriction, including without limitation the rights
157   * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
158   * copies of the Software, and to permit persons to whom the Software is
159   * furnished to do so, subject to the following conditions:
160   *
161   * The above copyright notice and this permission notice shall be included in
162   * all copies or substantial portions of the Software.
163   *
164   * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
165   * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
166   * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
167   * AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
168   * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
169   * OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
170   * THE SOFTWARE.
171   *
172   * @package CodeIgniter
173   * @author  EllisLab Dev Team
174   * @copyright   Copyright (c) 2008 - 2014, EllisLab, Inc. (https://ellislab.com/)
175   * @copyright   Copyright (c) 2014 - 2019, British Columbia Institute of Technology (https://bcit.ca/)
176   * @license https://opensource.org/licenses/MIT MIT License
177   * @link    https://codeigniter.com
178   * @since   Version 1.0.0
179   * @filesource
180   */
```

Gambar 4.35 Syntax HiHAT pada file index.php

Berikut ini hasil dari konfigurasi serta pembaharuan *source code*-nya setelah dideploy pada server PPDB Online.



Gambar 4.36 Implementasi dan Pembaharuan Source Code HiHAT

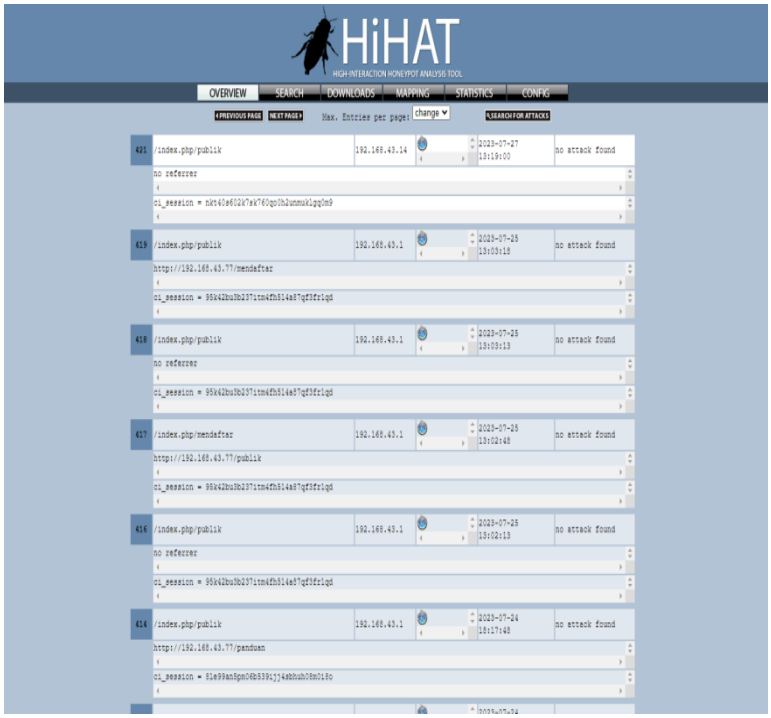
4.2.5. Implementasi Analisys Tool HiHAT

Langkah-langkah yang diperlukan untuk memasang alat analisis HIHAT adalah sebagai berikut:

1. Salin seluruh alat analisis HIHAT, termasuk subdirektori, ke server web.
2. Sesuaikan file "inc/constant.php" dengan pengaturan konfigurasi yang sesuai dengan kebutuhan. Pastikan untuk mendefinisikan pengaturan database SQL, username, dan password untuk mengakses data. Jika ingin menggunakan fungsi pemetaan geolokasi, konfigurasi basis data yang sesuai dan kunci untuk Google Maps juga harus diatur. Selain itu, dapat memilih opsi konfigurasi tambahan dalam file tersebut.

3. Untuk mengaktifkan pengunduhan otomatis alat berbahaya, pastikan "check_downloads.php" diakses secara berkala. Disarankan untuk membuat cronjob baru yang menjalankan perintah berikut setiap lima menit: "lynx -dump http://192.68.43.77/HiHAT/autodownloader/check_downloads.php?verobse=false".
4. Jika berencana menggunakan statistik grafis, periksa apakah perlu memperoleh lisensi untuk JpGraph. Mungkin juga perlu menginstal file tambahan dan GD Library v2.

Dengan mengikuti langkah-langkah di atas, alat analisis HIHAT akan terpasang dengan benar pada sistem server web dan siap digunakan untuk analisis dan pengawasan keamanan yang lebih baik. Dan ketika diakses pada http://192.168.43.77/HiHAT maka berikut ini tampilan Analisys Tool HIHAT:

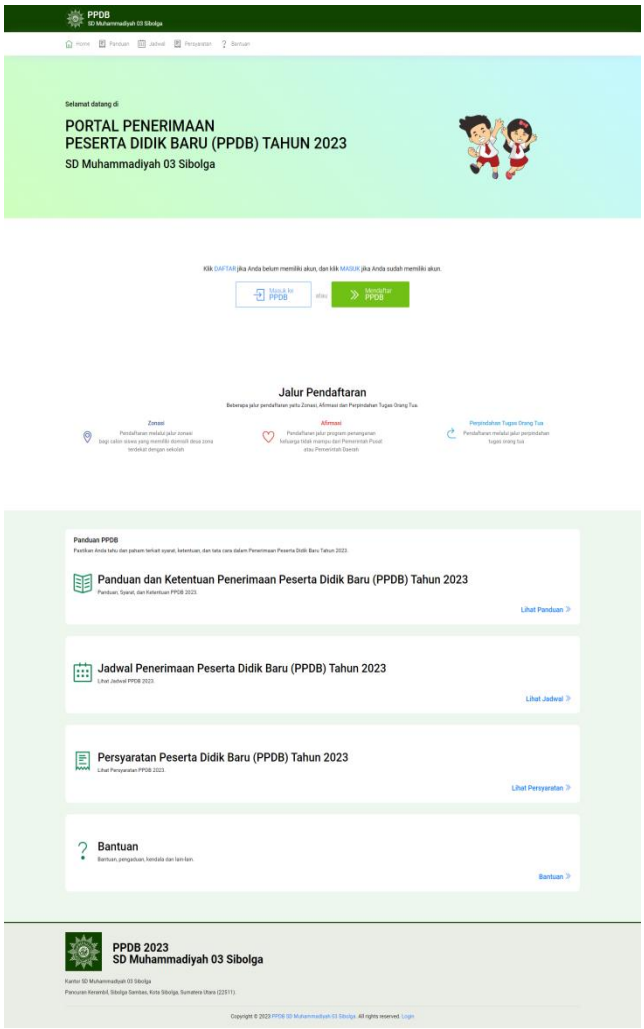


Gambar 4.37 Analisys Tool HIHAT

4.4. Analisis Antarmuka

4.3.1. Halaman Utama

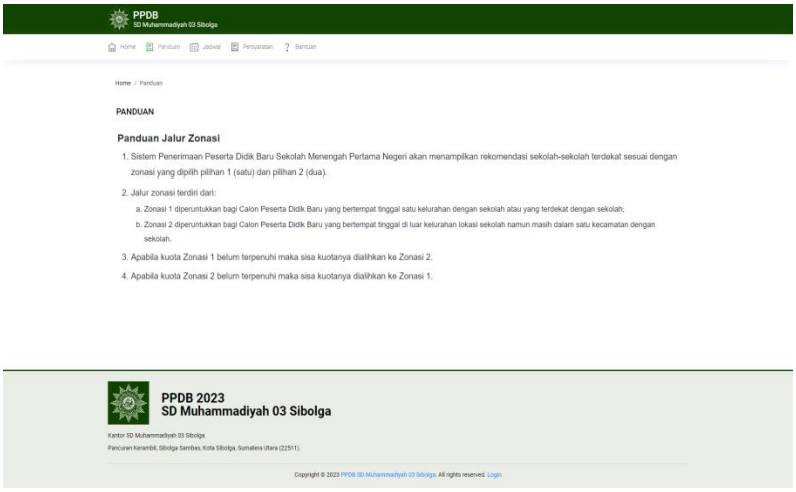
Halaman utama terdiri dari yang pertama adalah logo PPDB SD Muhammadiyah 03 Sibolga, kemudian menu navigasi berupa Home, Panduan, Jadwal, Persyaratan dan Bantuan, selanjutnya adalah banner, kemudian bagian dengan fitur pentingnya yaitu Pendaftaran/Masuk PPDB. Selanjutnya bagian info Jalur Pendaftaran dimana terdapat 3 jalur pendaftaran yaitu Zonasi, Afirmasi dan Perpindahan Tugas Orangtua/Wali. Dan beberapa bagian lainnya seperti Panduan, Jadwal, Persyaratan dan Bantuan.



Gambar 4.38 Halaman Utama Portal PPDB

4.3.2. Halaman Panduan

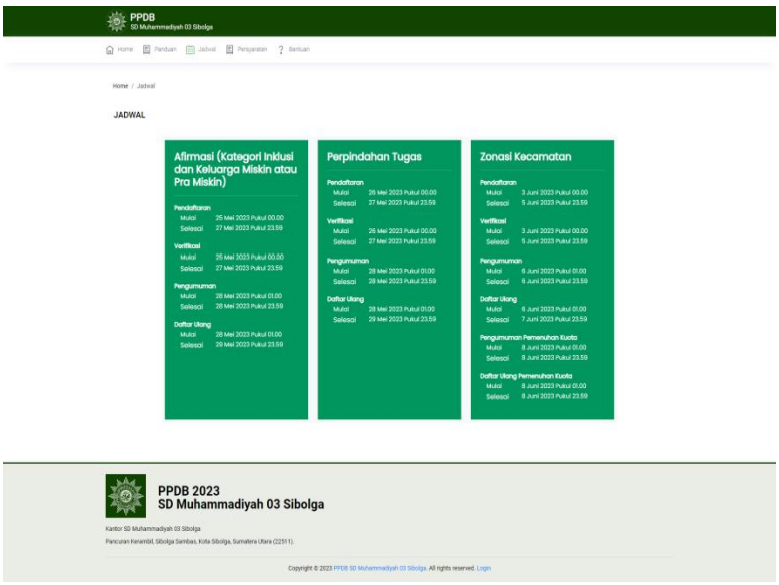
Halaman panduan merupakan halaman yang menampilkan panduan untuk pendaftaran PPDB.



Gambar 4.39 Halaman Panduan

4.3.3. Halaman Jadwal

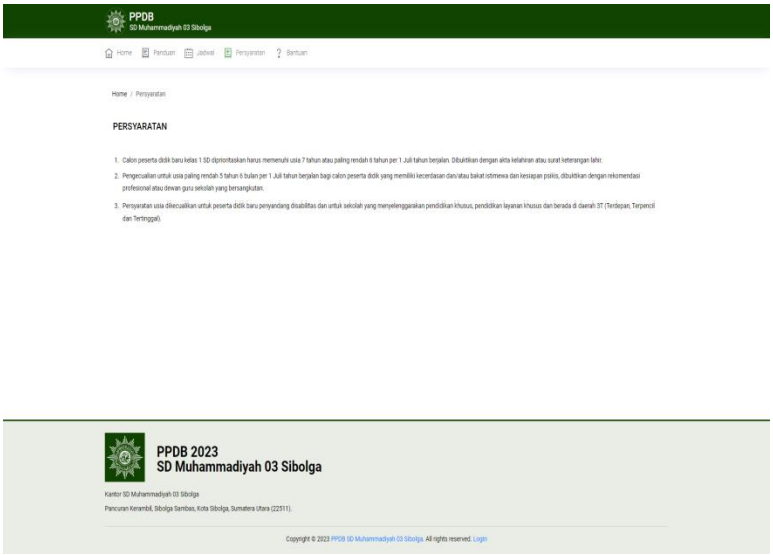
Halaman jadwal merupakan halaman yang menampilkan jadwal kapan pendaftaran PPDB akan dibuka.



Gambar 4.40 Halaman Jadwal

4.3.4. Halaman Persyaratan

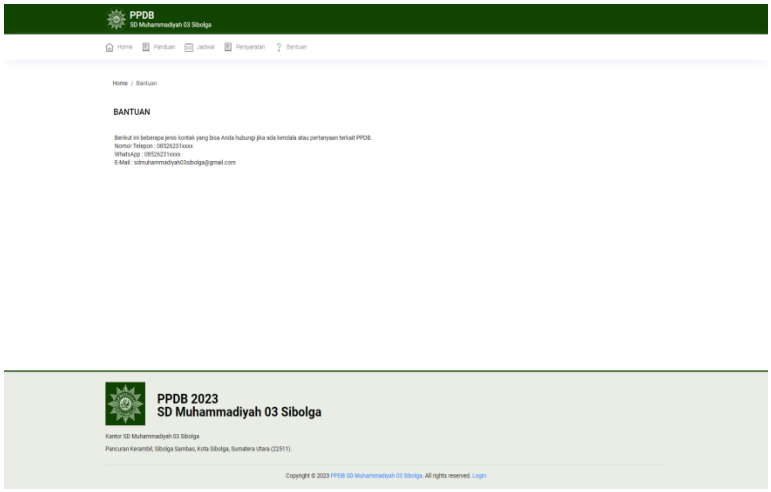
Halaman persyaratan merupakan halaman yang menampilkan persyaratan-persyaratan yang disiapkan untuk pendaftaran PPDB.



Gambar 4.41 Halaman Persyaratan

4.3.5. Halaman Bantuan

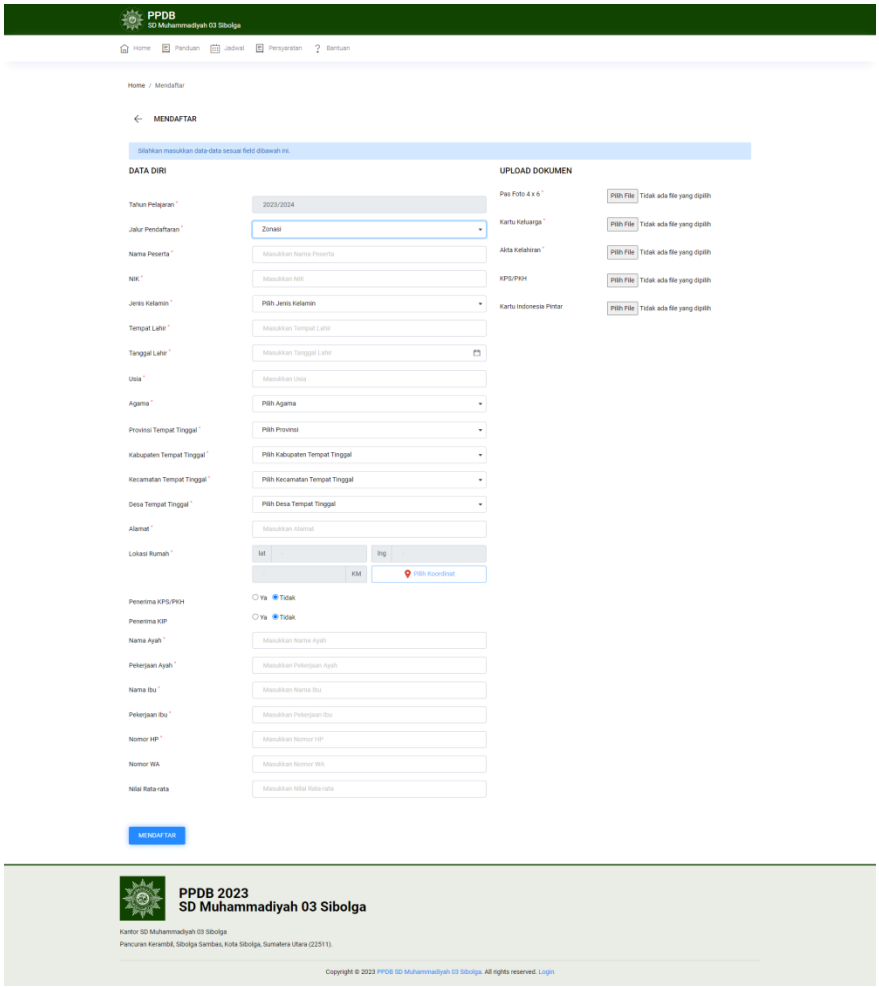
Halaman bantuan merupakan halaman yang menampilkan kontak person yang dapat dihubungi oleh calon siswa apa bila ada kendala dalam pendaftaran.



Gambar 4.42 Halaman Persyaratan

4.3.6. Halaman Mendaftar

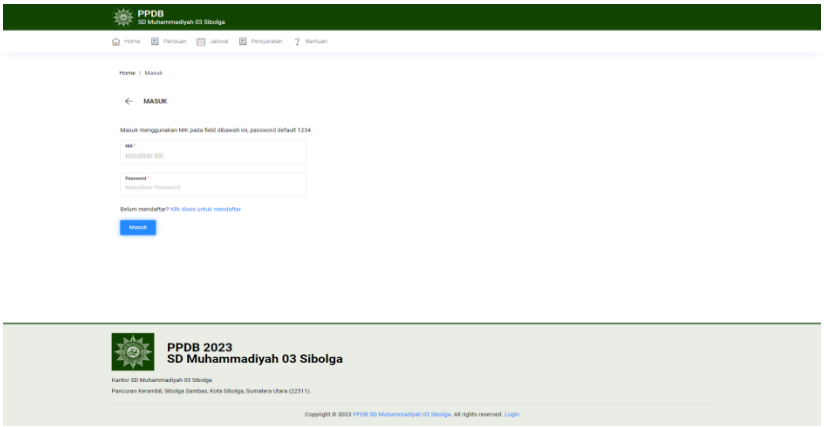
Halaman mendaftar merupakan halaman yang paling vital untuk diakses oleh calon pendaftar. Adapun data-data pada form yang akan diisi adalah pemilihan jalur pendaftaran, nama peserta, nik, jenis kelamin, tempat lahir, tanggal lahir, usia, agama, alamat, lokasi dengan menentukan titik kordinat tempat tinggal, penerima KPS / KPH, penerima KIP, nama ayah, pekerjaan ayah, nama ibu, pekerjaan ibu, nomor hp/wa serta upload berkas-berkas yang dibutuhkan seperti pas foto, kartu keluarga, akta kelahiran, kps/kph, kartu Indonesia pintar dan lainnya.



Gambar 4.43 Halaman Mendaftar

4.3.7. Halaman Masuk

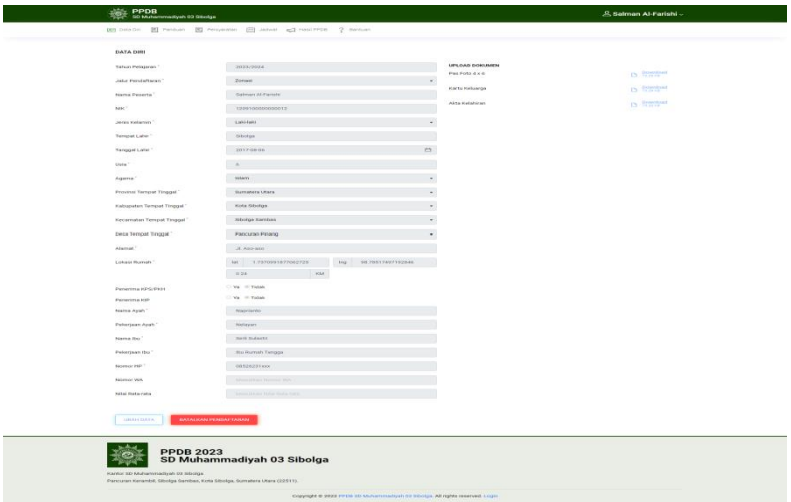
Halaman masuk bagi calon siswa yang telah berhasil melakukan pendaftaran, untuk login menggunakan nik dan passwordnya secara default adalah 1234.



Gambar 4.44 Halaman Masuk

4.3.8. Halaman Data Diri

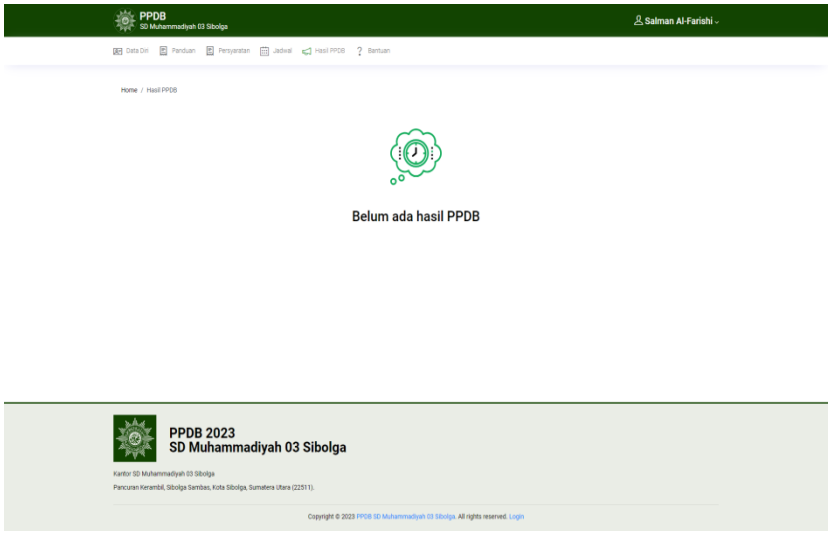
Saat berhasil masuk ke dalam sistem PPDB SD Muhammadiyah 03 Sibolga, maka akan tampil pada halaman berupa profil data diri, kemudian tombol ubah data diri dan tombol batalkan pendaftaran.



Gambar 4.45 Halaman Data Diri

4.3.9. Halaman Hasil PPDB

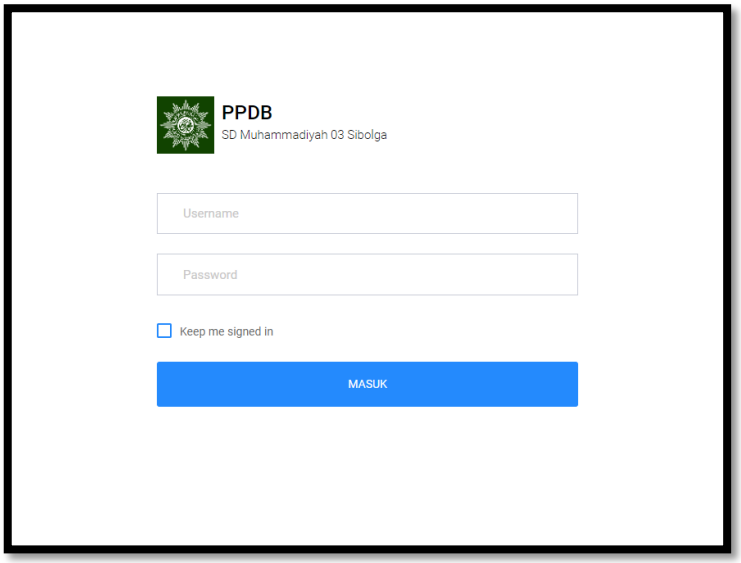
Halaman hasil PPDB merupakan halaman yang menampilkan status penerimaan calon siswa tersebut.



Gambar 4.46 Halaman Hasil PPDB

4.3.10. Halaman Masuk Admin

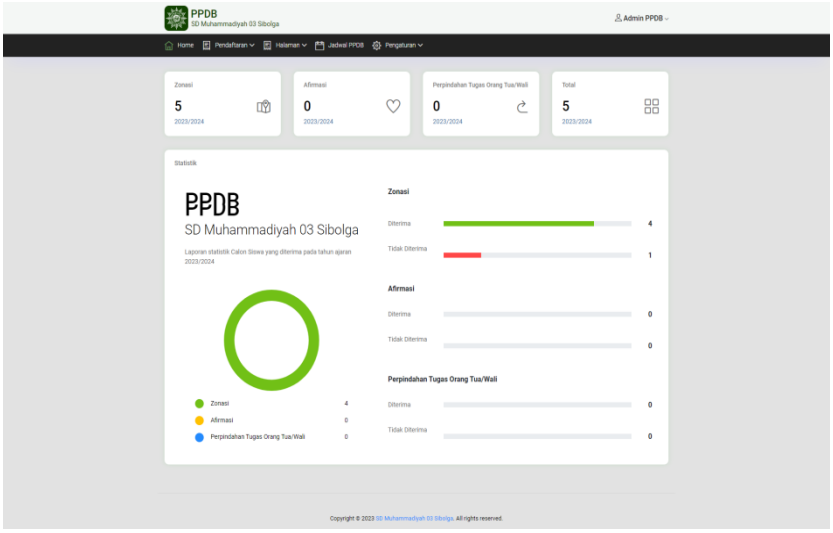
Halaman masuk untuk admin sekolah dalam memanajemen serta mengoperasikan sistem informasi PPDB Online SD Muhammadiyah 03 Sibolga.



Gambar 4.47 Halaman Login Admin PPDB

4.3.11.Halaman Dashboard Admin

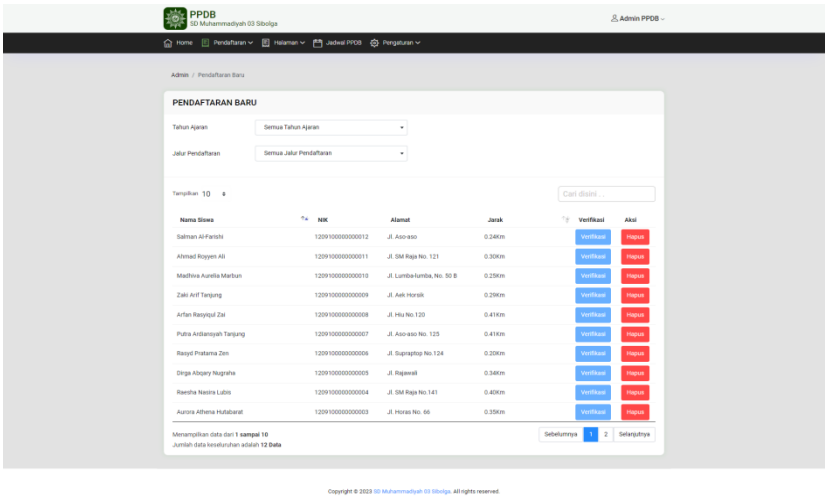
Halaman dashboard admin PPDB, terdapat beberapa statistik atau jumlah data penerimaan calon peserta didik.



Gambar 4.48 Halaman Dashboard Admin

4.3.12.Halaman Pendaftaran Baru

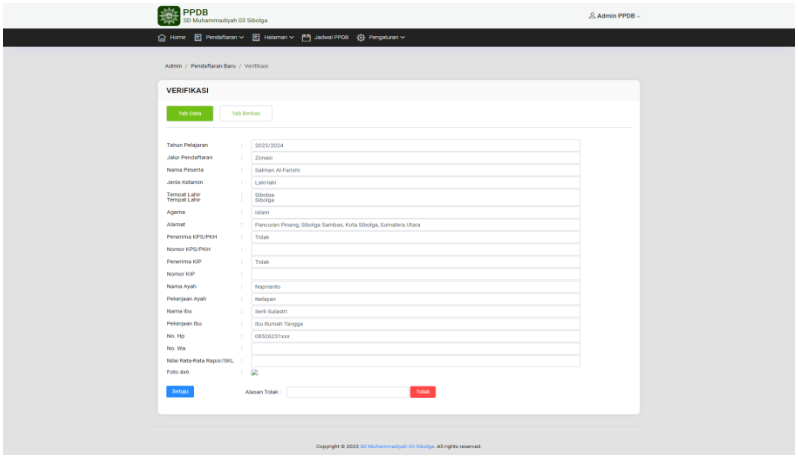
Halaman pendaftaran baru meruapakan halaman yang menampilkan data-data dari pendaftaran calon siswa, data ini masih bersifat baru dan perlu dilakukan verifikasi.



Gambar 4.49 Halaman Pendaftaran Baru

4.3.13.Halaman Verifikasi Pendaftaran Baru

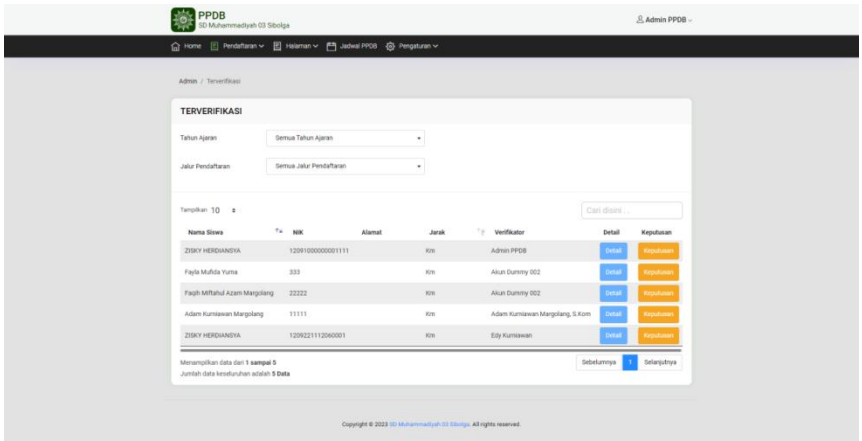
Halaman verifikasi data pendaftaran baru, pada halaman ini admin dapat melakukan verifikasi data, apakah inputan data sudah sesuai atau belum. Hal ini dilakukan untuk mencegah banyaknya data-data yang bersifat fiktif.



Gambar 4.50 Halaman Verifikasi Pendaftaran Baru

4.3.14.Halaman PendaftaranTerverifikasi

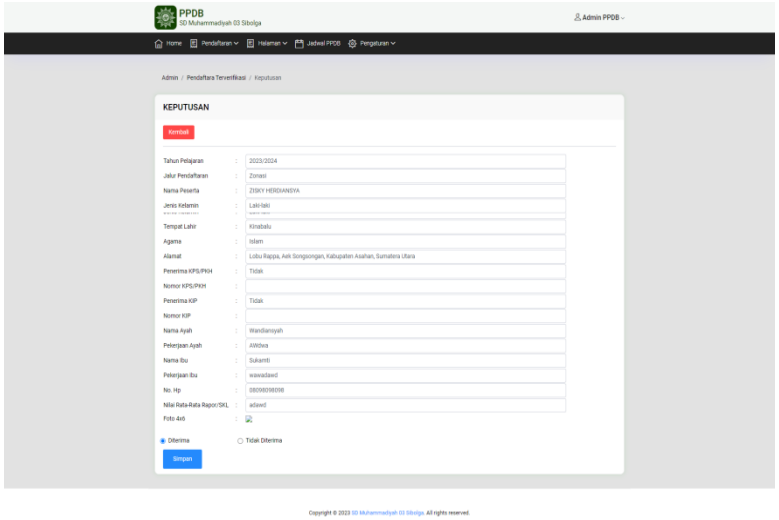
Merupakan halaman yang menampilkan data-data pendaftaran calon siswa yang sudah diverifikasi oleh admin PPDB, dan data ini nantinya yang akan dilakukan keputusan apakah calon siswa diterima atau tidak.



Gambar 4.51 Halaman Data Pendaftaran Terverifikasi

4.3.15.Halaman Keputusan

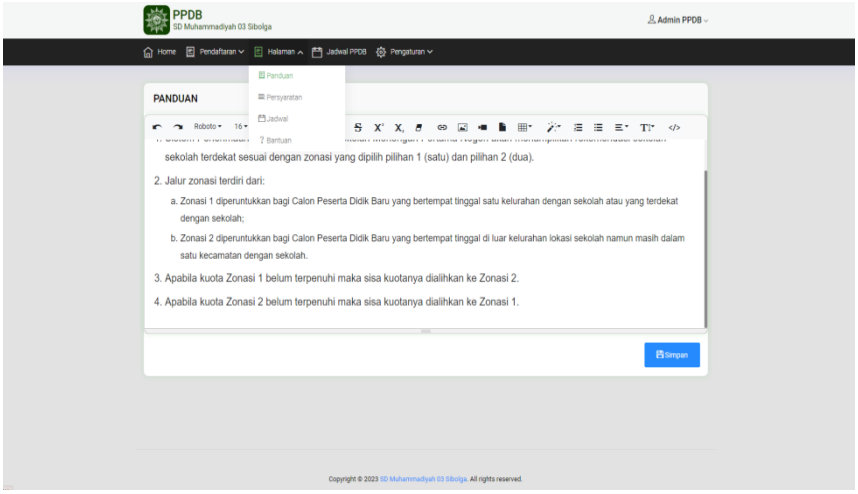
Merupakan halaman yang menampilkan data siswa untuk dilakukan keputusan apakah calon siswa diterima atau tidak.



Gambar 4.52 Halaman Keputusan

4.3.16. Halaman Pengaturan Konten Halaman

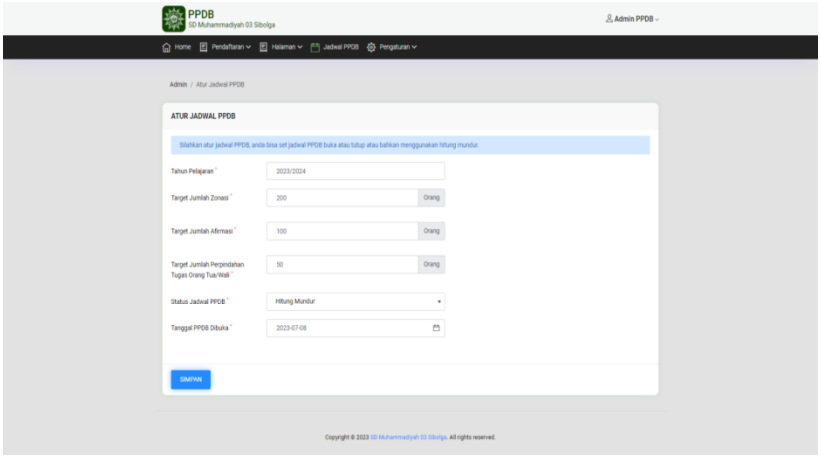
Halaman pengaturan konten halaman yaitu berupa pengaturan konten panduan, persyaratan, jadwal dan bantuan. Dengan pengaturan ini admin PPDB dapat melakukan pembaharuan informasi terkait PPDB Online.



Gambar 4.53 Halaman Pengaturan Konten Halaman

4.3.17.Halaman Pengaturan Jadwal PPDB

Digunakan oleh Admin PPDB untuk mengatur jadwal PPDB, admin dapat mengatur tahun pelajaran, jumlah target Zonasi, Afirmasi, Perpindahan Tugas Orangtua/Wali, kemudian status jadwal PPDB apakah buka, tutup ataupun countdown (hitung mundur) yang diikuti dengan mengatur tanggalnya.



Gambar 4.54 Halaman Pengaturan Jadwal PPDB

4.5. Deskripsi Data

4.4.1. Sumber Data

Peneliti mengidentifikasi berbagai sumber data yang digunakan dalam analisis keamanan jaringan. Sumber data meliputi log dari server web PPDB Online SD Muhammadiyah 03 Sibolga, termasuk log akses web dan log error, yang membantu pemelihara sistem dapat melihat aktivitas yang mencurigakan atau tidak dapat a pada situs web tersebut. Selain itu, peneliti juga menggunakan log dari firewall untuk memantau lalu lintas masuk dan keluar dari jaringan. Log aplikasi server tersebut juga menjadi sumber data penting karena membantu dalam melacak kegiatan pengguna dan potensi celah keamanan pada server web tersebut.

4.4.2. Jumlah Sampel

Jumlah sampel menjadi hal yang penting untuk ditentukan karena akan mempengaruhi validitas dan representativitas hasil penelitian. Berikut adalah penjelasan lebih rinci tentang bagaimana jumlah sampel ditentukan dalam penelitian ini:

1. Tujuan Penentuan Jumlah Sampel: Penelitian ini bertujuan untuk memahami taktik serangan siber yang mungkin terjadi selama proses PPDB, serta mengidentifikasi potensi ancaman dan celah keamanan yang ada. Dalam rangka mencapai tujuan tersebut, penentuan jumlah sampel honeypot harus memungkinkan peneliti untuk menarik kesimpulan yang valid tentang aktivitas penyerangan yang mencoba memanfaatkan sistem PPDB.
2. Pertimbangan Skala dan Kompleksitas Lingkungan PPDB: Dalam menentukan jumlah sampel, peneliti juga mempertimbangkan skala dan kompleksitas lingkungan PPDB di SD Muhammdiyah 03 Sibolga. Hal ini mencakup ukuran jaringan, jumlah pengguna, dan berbagai aplikasi dan sistem yang digunakan. Semakin kompleks lingkungan, semakin besar jumlah sampel honeypot yang mungkin dibutuhkan untuk mencakup berbagai jenis serangan potensial.
3. Validitas Statistik: Penting bagi peneliti untuk memastikan bahwa jumlah sampel yang dipilih cukup untuk memberikan hasil yang memiliki validitas statistik. Jumlah sampel yang terlalu kecil dapat menyebabkan hasil yang tidak representatif dan mengurangi daya generalisasi temuan. Oleh karena itu, peneliti melakukan perhitungan statistik untuk

memastikan bahwa jumlah sampel yang dipilih dapat memberikan hasil yang signifikan.

4. Keterbatasan Sumber Daya: Penentuan jumlah sampel juga harus mempertimbangkan keterbatasan sumber daya yang tersedia, seperti anggaran, waktu, dan perangkat keras. Peneliti harus memastikan bahwa jumlah sampel yang ditentukan dapat diimplementasikan dengan sumber daya yang ada tanpa mengorbankan kualitas dan keandalan penelitian.

4.2.6. Variabel Data

Dalam skripsi ini, penelitian berfokus pada implementasi honeypot pada sistem penerimaan peserta didik baru (PPDB) di SD Muhammdiyah 03 Sibolga. Pada judul ini akan menjelaskan tentang variabel-variabel yang menjadi fokus dalam mengumpulkan data dari sampel Honeypot yang digunakan dalam penelitian ini. Berikut adalah penjelasan lebih rinci tentang variabel-variabel data sampel pada penelitian ini:

1. Alamat IP *Honeypot*: Variabel ini mencakup alamat IP yang digunakan oleh masing-masing Honeypot yang ditempatkan di lingkungan PPDB SD Muhammdiyah 03 Sibolga. Alamat IP ini menjadi kunci dalam mengidentifikasi aktivitas atau serangan yang ditujukan langsung ke Honeypot.
2. Waktu Kejadian: Waktu kejadian mencatat waktu dan tanggal terjadinya aktivitas pada setiap *Honeypot HiHAT*. Informasi waktu ini akan membantu peneliti dalam menganalisis pola serangan dan mengidentifikasi periode waktu ketika serangan cenderung meningkat.

3. Jenis Serangan: Variabel ini mencatat jenis serangan atau aktivitas yang terdeteksi pada masing-masing *Honeypot HiHAT*. Misalnya, jenis serangan dapat mencakup percobaan *sql injection*, *DDoS*, eksploitasi kerentanan, atau jenis serangan lainnya yang berpotensi terjadi.
4. Protokol Jaringan: Informasi tentang protokol jaringan yang digunakan dalam serangan juga dicatat. Misalnya, apakah serangan dilakukan melalui protokol HTTP, FTP, SSH, atau protokol lainnya yang relevan.
5. Sumber IP Penyerang: Variabel ini mencatat alamat IP sumber dari penyerang yang melakukan aktivitas terhadap Honeypot HiHAT. Informasi ini dapat membantu peneliti dalam mengidentifikasi sumber serangan dan negara atau wilayah asal dari penyerang.
6. Hasil Serangan: Informasi tentang hasil dari serangan atau aktivitas penyerangan yang ditujukan ke Honeypot juga dicatat. Misalnya, apakah serangan berhasil atau gagal, ada informasi potensial yang dapat diambil oleh penyerang, atau memanfaatkan celah keamanan yang sudah diketahui.
7. Frekuensi Serangan: Variabel ini mencatat frekuensi terjadinya serangan pada masing-masing Honeypot. Informasi ini akan membantu peneliti dalam menilai seberapa sering serangan terjadi dan mengidentifikasi periode waktu dengan aktivitas serangan yang tinggi.

Dengan memperhatikan variabel-variabel data sampel ini, kiranya dapat menghasilkan informasi yang relevan tentang taktik serangan yang mungkin terjadi serta potensi ancaman keamanan yang perlu diperhatikan dalam menjaga keamanan sistem PPDB.

4.6. Analisis Data

4.5.1. Data Honeypot HiHAT

Ketika honeypot HiHAT diaktifkan pada sistem PPDB Online SD Muhammadiyah 03 Sibolga, ia akan berperan sebagai perangkap atau umpan bagi para penyerang siber yang berusaha mencari celah atau merusak sistem. Data yang dihasilkan oleh honeypot HiHAT dapat berupa log dan laporan mengenai aktivitas mencurigakan atau serangan yang terjadi. Contoh data yang dihasilkan oleh honeypot HiHAT pada sistem PPDB online:

1. Alamat IP Penyerang: Honeypot akan mencatat alamat IP dari mesin atau perangkat yang mencoba berinteraksi dengan sistem PPDB online secara tidak sah. Alamat IP ini akan membantu dalam mengidentifikasi asal atau lokasi dari serangan tersebut.
2. Metode Serangan: Honeypot akan mencatat metode serangan yang digunakan oleh penyerang. Misalnya, metode DDoS (Distributed Denial of Service), SQL Injection, Cross-Site Scripting (XSS), atau upaya login tidak sah.
3. Jenis Permintaan: Honeypot akan mencatat jenis permintaan yang dikirimkan oleh penyerang ke sistem PPDB online. Ini bisa berupa permintaan akses ke halaman tertentu, mencoba mencari celah pada formulir pendaftaran, atau mencoba mengakses basis data secara langsung.
4. Response dari Honeypot: Honeypot akan memberikan tanggapan palsu atau data simulasi yang terlihat seperti respon nyata dari sistem PPDB online. Data ini sebenarnya tidak memiliki dampak atau akses pada sistem asli, tetapi dapat menarik perhatian penyerang dan membuat mereka

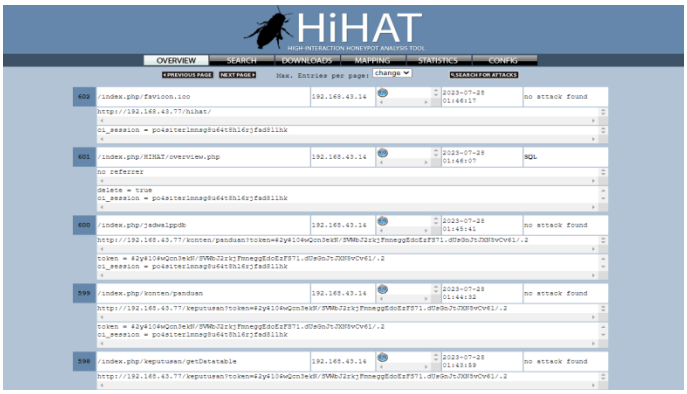
berpikir bahwa mereka telah berhasil meretas.

5. Waktu dan Durasi Serangan: Honeypot akan mencatat waktu mulai dan berakhirnya serangan serta lamanya serangan berlangsung. Informasi ini berguna untuk melacak pola serangan dan menilai tingkat risiko yang dihadapi oleh sistem.
6. Catatan Lain: Honeypot juga bisa mencatat informasi tambahan, seperti headers permintaan, jenis perangkat atau browser yang digunakan oleh penyerang, dan data lainnya yang relevan.

Dengan mengumpulkan data ini, honeypot HiHAT dapat membantu para administrator sistem untuk menganalisis serangan, mengidentifikasi potensi kerentanannya, dan mengambil langkah-langkah yang tepat untuk memperkuat keamanan sistem.

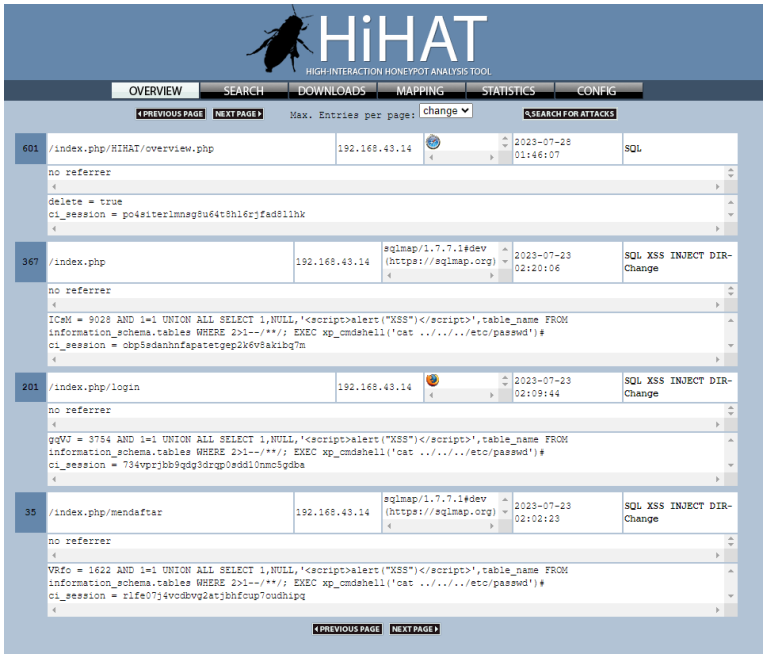
4.5.2. Analisis Serangan

Pada tahap awal, aplikasi Honeypot HiHAT menyediakan sebuah menu yang memberikan ringkasan tentang serangan-serangan yang terjadi. Menu Overview merupakan menu yang menampilkan data-data akses maupun serangan yang masuk.



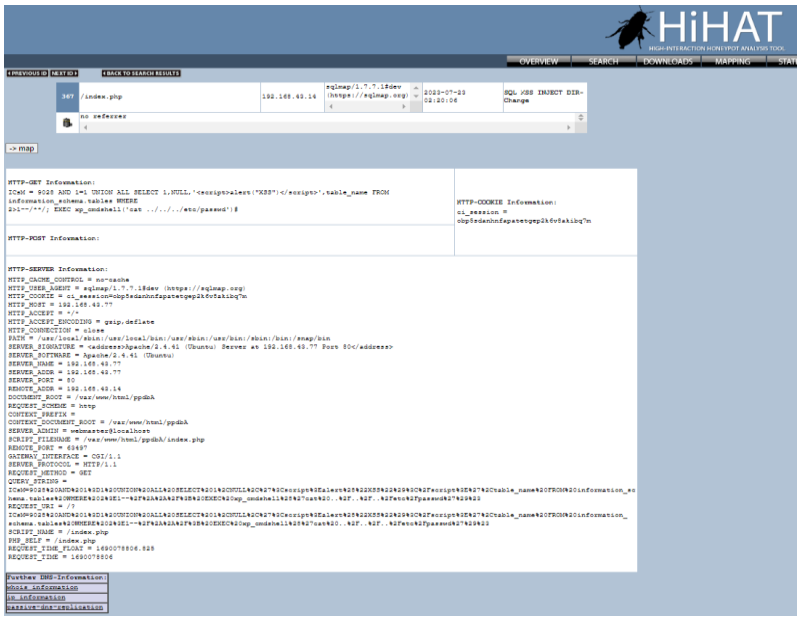
Gambar 4.55 Overview Pada HiHAT

Serangan-serangan yang masuk dapat dilihat secara keseluruhan dengan cara klik tombol “SEARCH FOR ATTACS”.



Gambar 4.56 Beberapa data serangan yang masuk

Pada menu details, akan tersedia lebih banyak informasi tentang serangan yang terdeteksi, seperti yang terlihat pada gambar dibawah.



Gambar 4.57 Detail informasi serangan yang masuk

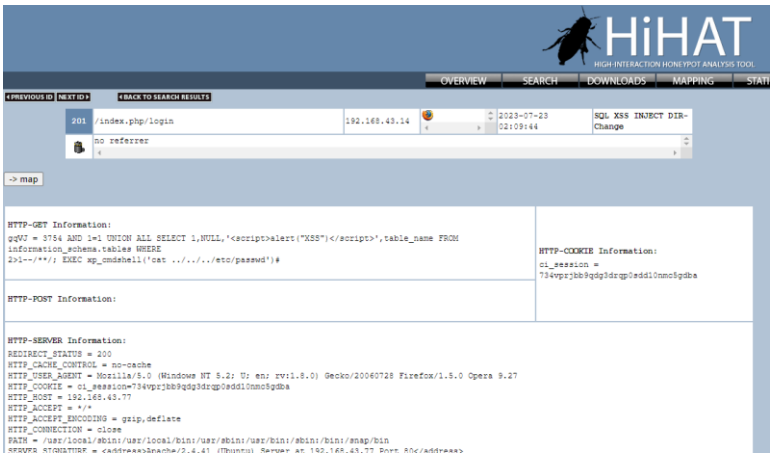
Berikut ini penjelasan beberapa bagian data informasi yang merupakan indikasi serangan terdapat keterangan:

1. Modul keuangan telah diserang
2. IP Address penyerang adalah 192.168.43.14
3. Aplikasi yang digunakan adalah sqlmap/1.7.7.1#dev (https://sqlmap.org)
4. Waktu terjadinya serangan adalah tanggal 2023-07-23 Pukul 02:02:23
5. Jenis serangan yang dilakukan adalah SQL XSS INJECT DIR-Change
6. URL atau alamat yang dijadikan target saatmenyerang adalah http://192.168.43.77/index.php/mendaftar atau form Mendaftar
7. Script serangan yang digunakan adalah VRfo = 1622 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#.

Dalam proses analisis ini, berbagai jenis serangan yang berhasil terdeteksi oleh Honeypot HiHAT dianalisis secara mendalam. Selama proses analisis ini, ditampilkan beberapa penyerangan-penyerangan yang dilakukan oleh penyerang. Berikut ini penjelasan beberapa serangan-serangan yang masuk pada honeypot HiHAT :

1. SQL Injection, merupakan jenis serangan keamanan pada aplikasi web yang memanfaatkan kelemahan dalam mekanisme input data pada aplikasi yang menggunakan SQL (*Structured Query Language*) untuk berinteraksi dengan database. Pada SQL *Injection*, penyerang memasukkan kode SQL berbahaya ke dalam bidang input aplikasi yang semestinya hanya menerima data biasa dari pengguna. Jika aplikasi tidak memvalidasi atau menyaring input dengan

benar, kode SQL berbahaya tersebut akan dieksekusi oleh database, memungkinkan penyerang untuk mendapatkan akses tidak sah ke data, mengubah data, atau bahkan menghapus data dari database. SQL Injection merupakan ancaman serius bagi aplikasi web yang tidak cukup aman dalam mengelola input dari pengguna.



Gambar 4.58 Serangan SQL Injection

Tabel 4.1 script yang terdeteksi digunakan dalam melakukan serangan SQL Injection.

Tabel 4.2. Serangan SQL Injection

Perintah	**Script**
SELECT	SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/
UNION	UNION ALL
EXEC	EXEC xp_cmdshell('cat ../../../etc/passwd')#

b. SELECT table_name: Perintah ini mencoba untuk mengambil nama tabel

dari database yang sesuai dengan kriteria yang akan didefinisikan nanti.

c. FROM information_schema.tables: Ini adalah bagian dari perintah yang menunjukkan bahwa kita akan mencari informasi tentang tabel. information_schema adalah suatu schema sistem khusus dalam database yang menyimpan metadata tentang struktur database seperti tabel, kolom, dan constraint.
d. WHERE 2 > 1: Bagian ini adalah klausul WHERE yang memberi kondisi untuk memfilter hasil. Kondisi 2 > 1 selalu benar, sehingga ini akan menghasilkan semua baris dalam tabel information_schema.tables tanpa ada filtering.
e. --/**/: Ini adalah komentar dalam SQL. Dalam contoh ini, komentar digunakan untuk mengakhiri perintah SQL asli sehingga sebaris perintah berbahaya selanjutnya tidak dieksekusi.
f. EXEC xp_cmdshell adalah perintah SQL yang digunakan untuk menjalankan perintah dari sistem operasi dalam lingkungan Microsoft SQL Server. xp_cmdshell adalah prosedur eksternal yang memungkinkan eksekusi perintah batch atau program yang ada di sistem operasi yang meng-host SQL Server. Secara umum penggunaan perintah xp_cmdshell memerlukan izin administratif (sysadmin) pada SQL Server, karena perintah ini memberikan akses ke perintah sistem operasi yang dapat menyebabkan potensi masalah keamanan jika digunakan secara tidak benar. Maka dari itu disarankan untuk tidak mengaktifkan atau menggunakan xp_cmdshell kecuali benar-benar diperlukan, dan pastikan untuk memberikan izin hanya kepada pengguna yang membutuhkan

akses tersebut.

2. XSS, Skrip SQL yang diberikan adalah contoh potensial serangan Cross-Site Scripting (XSS) yang dimaksudkan untuk dieksekusi pada database dengan tujuan menyisipkan serangan XSS ke dalam hasil kueri. Peneliti akan memberikan penjelasan tentang cara skrip tersebut dapat digunakan untuk serangan XSS. Pada kolom ketiga (Kolom 3) pada pernyataan SELECT, kita memiliki nilai yang diisi dengan kode skrip HTML yang berbahaya, yaitu: <script>alert("XSS")</script>. Skrip ini adalah contoh serangan XSS yang mencoba untuk menampilkan pesan peringatan pop-up dengan teks "XSS" ketika halaman yang mengandung kueri ini dimuat oleh browser. Apabila hasil kueri ini kemudian digunakan secara tidak aman dalam aplikasi web untuk menampilkan data di halaman web, maka skrip berbahaya dalam kolom ketiga akan diinterpretasikan dan dieksekusi oleh browser pengguna. Hasilnya, muncul pesan peringatan pop-up "XSS" yang dapat mengekspos pengguna pada risiko serangan lebih lanjut, seperti mencuri data login atau informasi sensitif lainnya.

```
1 | NULL | <script>alert("XSS")</script> | table1
2 | NULL | <script>alert("XSS")</script> | table2
3 | NULL | <script>alert("XSS")</script> | table3
```

Gambar 4.59 Contoh tampilan potensial pada halaman web tanpa perlindungan XSS

Penting untuk menghindari serangan XSS dengan memvalidasi, membersihkan, atau menghindari penggunaan data yang tidak dipercaya sebelum menampilkan konten di halaman web. Penggunaan metode escape/encoding yang tepat saat menampilkan data dapat membantu

mencegah interpretasi skrip berbahaya oleh browser dan melindungi pengguna dari serangan XSS.

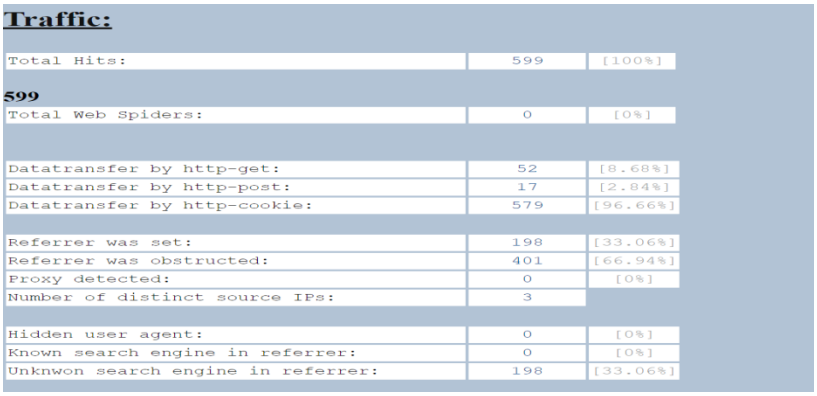
Berdasarkan analisis yang telah dilakukan terhadap serangan dan perilaku hacker menggunakan High Interaction Honeypot (HIHAT), dapat diambil beberapa kesimpulan sebagai berikut:

1. Melakukan pemeliharaan sistem aplikasi melalui perbaikan script dan pemasangan alat-alat pada server, seperti Honeypot, dapat membantu mendeteksi serangan yang dilakukan oleh hacker.
2. Implementasi aplikasi Honeypot dapat membantu memonitor dan merekam aktivitas web server dari serangan-serangan hacker, seperti upaya SQL Injection, XSS, Code Injection, dan percobaan Inclusion.

Dengan demikian, tindakan-tindakan tersebut dapat meningkatkan keamanan sistem aplikasi dan memberikan wawasan berharga tentang upaya serangan yang dilakukan oleh hacker.

4.5.3. Statistik Hit dan Serangan

Pada halaman statistic menampilkan beberapa data-data statistic jumlah seluruh serangan ataupun requrest yang pernah terjadi.



Traffic:

Total Hits:	599	[100%]

599

Total Web Spiders:	0	[0%]
Datatransfer by http-get:	52	[8.68%]
Datatransfer by http-post:	17	[2.84%]
Datatransfer by http-cookie:	579	[96.66%]
Referrer was set:	198	[33.06%]
Referrer was obstructed:	401	[66.94%]
Proxy detected:	0	[0%]
Number of distinct source IPs:	3	
Hidden user agent:	0	[0%]
Known search engine in referrer:	0	[0%]
Unknwon search engine in referrer:	198	[33.06%]

Gambar 4.60 Statistik Traffict yang masuk

Pada gambar 4.51 terdapat statistic URL/Link yang sering diakses, pada peringkat pertama terdapat url /index.php/publik yaitu sebanyak 31 Hits atau 5.18% yang merupakan halaman utama sistem PPDB Online tersebut. Diikuti dengan halaman /index.php/mendaftar yaitu sebanyak 20 Hits atau 3.34% yang merupakan halaman mendaftar bagi calon siswa, halaman ini merupakan halaman yang dapat dipastikan menjadi target dalam penyerangan, dalam hal ini penyerangan SQL Injection maupun serangan DDoS. Halaman yang juga memungkinkan menjadi target penyerangan adalah halaman /index.php/login yaitu sebanyak 9 Hits atau 1.51% dan juga halaman /index.php/auth/admin sebanyak 13 Hits atau 2.17%.

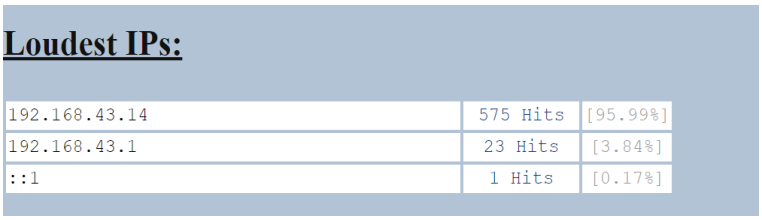
Most often accessed files:

/index.php/publik	31 Hits	[5.18%]
/index.php/mendaftar	20 Hits	[3.34%]
/index.php	19 Hits	[3.17%]
/index.php/favicon.ico	14 Hits	[2.34%]
/index.php/auth/admin	13 Hits	[2.17%]
/index.php/home	11 Hits	[1.84%]
/index.php/login	9 Hits	[1.5%]
/index.php/pendaftaran/verifikasi/26	9 Hits	[1.5%]
/index.php/ppdb/assets/vendors/datatables.net/jquery.dataTables.js	7 Hits	[1.17%]
/index.php/pendaftaran/getDatatable	6 Hits	[1%]
/index.php/konten/persyaratan	6 Hits	[1%]
/index.php/resources/pendaftaran/1689481280-3575.jpg	6 Hits	[1%]
/index.php/panduan	5 Hits	[0.83%]
/index.php/pendaftaran/baru	5 Hits	[0.83%]
/index.php/bantuan	5 Hits	[0.83%]

Gambar 4.61 Statistik URL/Link yang sering diakses

Terdapat statistic url/link yang sering diakses, url yang sering diakses adalah /index.php/publik yang merupakan halaman utama pada sistem PPDB yakni sebanyak 31 hits atau 5.18%. Lalu diikuti dengan /index.php/mendaftar sebanyak 20 hits atau 3.34% dan seterusnya.

Kemudian statistik jumlah akses ip pengguna/penyerang terlihat pada gambar 4.52, terdapat pada IP 192.168.43.14 sebanyak 574 Hits atau 95.99%, kemudian diikuti oleh 192.168.43.1 sebanyak 3.84% dan seterusnya. Dapat dilihat pada gambar dibawah ini.

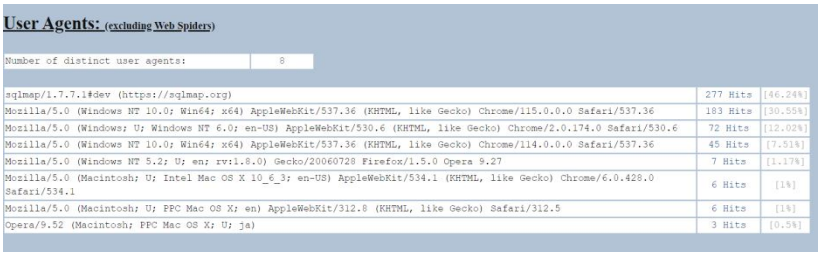


Loudest IPs:

192.168.43.14	575 Hits	[95.99%]
192.168.43.1	23 Hits	[3.84%]
::1	1 Hits	[0.17%]

Gambar 4.62 Statistik IP Pengguna/Penyerang

Ketika menggunakan Honeypot atau teknologi lain untuk mengamati aktivitas penyerang, secara umum akan menganalisis User Agents yang digunakan oleh penyerang saat mencoba berinteraksi dengan Honeypot. Analisis User Agents dapat memberikan wawasan tentang jenis perangkat lunak atau aplikasi yang digunakan oleh penyerang. Informasi ini dapat membantu dalam mengidentifikasi pola serangan dari berbagai jenis perangkat dan memahami preferensi atau kelemahan yang mungkin dimanfaatkan oleh penyerang. Statistik User Agents dapat dilihat pada gambar 4.53.



User Agents: (excluding Web Spiders)

Number of distinct user agents:	8

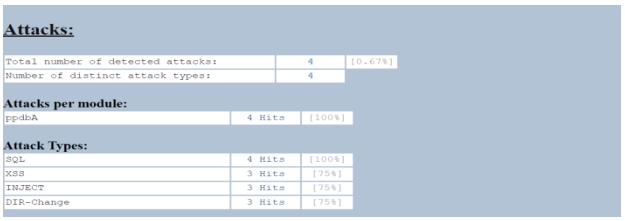
sqlmap/1.7.7.1#dev (https://sqlmap.org)	277 Hits	[46.24%]
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36	183 Hits	[30.55%]
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/530.6 (KHTML, like Gecko) Chrome/2.0.174.0 Safari/530.6	72 Hits	[12.02%]
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36	45 Hits	[7.51%]
Mozilla/5.0 (Windows NT 5.2; U; en; rv:1.8.0) Gecko/20060728 Firefox/1.5.0 Opera 9.27	7 Hits	[1.17%]
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/534.1 (KHTML, like Gecko) Chrome/6.0.428.0 Safari/534.1	6 Hits	[1%]
Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/312.8 (KHTML, like Gecko) Safari/312.5	6 Hits	[1%]
Opera/9.52 (Macintosh; PPC Mac OS X; U; ja)	3 Hits	[0.5%]

Gambar 4.63 Statistik User Agents

Statistik penyerangan yang terjadi, menampikan juga beberapa jenis penyerangan yang telah dilakukan. Berikut ini penjelasan dari data statistik jenis penyerangan yang dilakukan oleh penyerang.

Tabel 4.3. Statistik Jenis Penyerangan

Jenis Serangan	Hits	Presentasi Deteksi	Penjelasan
SQL Injection	4	100%	Honeypot berhasil mendeteksi 4 serangan SQL Injection dari total serangan yang terjadi, dengan tingkat deteksi 100%.
XSS	3	75%	Honeypot berhasil mendeteksi 3 serangan Cross-Site Scripting (XSS) dari total 4 serangan yang terjadi, dengan tingkat deteksi 75%.
INJECT	3	75%	Honeypot berhasil mendeteksi 3 serangan dengan jenis "INJECT" dari total 4 serangan yang terjadi, dengan tingkat deteksi 75%. Keterangan lebih lanjut tentang jenis serangan "INJECT" tidak diberikan dalam tabel ini.
DIR-Change	3	75%	Honeypot berhasil mendeteksi 3 serangan dengan jenis "DIR-Change" dari total 4 serangan yang terjadi, dengan tingkat deteksi 75%. Keterangan lebih lanjut tentang jenis serangan "DIR-Change" tidak diberikan dalam tabel ini.



Attacks:

Total number of detected attacks:	4	[0.67%]
Number of distinct attack types:	4	

Attacks per module:

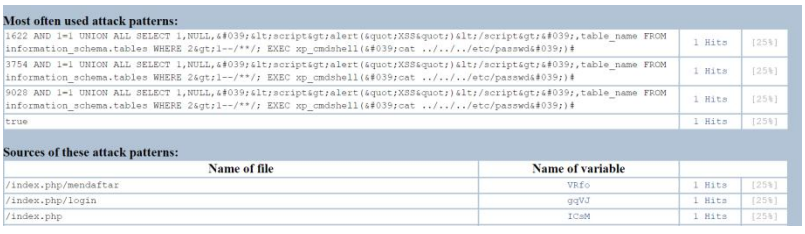
ppdbA	4 Hits	[100%]

Attack Types:

SQL	4 Hits	[100%]
XSS	3 Hits	[75%]
INJECT	3 Hits	[75%]
DIR-Change	3 Hits	[75%]

Gambar 4.64 Statistik Serangan

Statistik Pola Serangan yang menampilkan pola-pola penyerangan dapat dilihat pada gambar 4.55. Dari statistik ini kita dapat melihat bahwa penyerang melakukan pola penyerangannya menggunakan kode SQL pada halaman-halaman yang memang menjadi target oleh si penyerang seperti halaman mendaftar, login dan halaman utama.



Most often used attack patterns:

1622 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#	1 Hits	[25%]
3754 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#	1 Hits	[25%]
9028 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#	1 Hits	[25%]
true	1 Hits	[25%]

Sources of these attack patterns:

Name of file	Name of variable		
/index.php/mendaftar	VRfo	1 Hits	[25%]
/index.php/login	gqVJ	1 Hits	[25%]
/index.php	ICsM	1 Hits	[25%]

Gambar 4.65 Statistik Pola Serangan

BAB 5

KESIMPULAN DAN SARAN

6.1. Kesimpulan

Dalam PPDB Online SD Muhammadiyah 03 Sibolga telah memberikan kontribusi positif dalam membantu mengatasi permasalahan yang terjadi pada urusan administrasi, seperti penginputan data siswa baru yang tidak tertata dengan baik. Selain itu, implementasi PPDB berbasis web yang dapat diakses dari mana saja dan memiliki proses yang cepat juga berkontribusi dalam menarik minat calon peserta didik baru untuk mendaftar di SD Muhammadiyah 03 Sibolga. Kemudahan akses dan proses yang efisien memberikan kenyamanan bagi calon peserta didik dan orang tua dalam melakukan pendaftaran, sehingga meningkatkan kesempatan untuk lebih banyak calon peserta didik mendaftar di sekolah tersebut.

Berdasarkan penelitian yang telah dilakukan pada implementasi metode honeypot dalam PPDB Online SD Muhammadiyah 03 Sibolga, ditemukan beberapa hal penting terkait keamanan informasi sistem penerimaan peserta didik baru. Dua jenis serangan yang berhasil terdeteksi melalui metode honeypot adalah SQL Injection dan XSS (Cross-Site Scripting).

Hipotesis yang diajukan dalam penelitian menyatakan bahwa metode honeypot merupakan salah satu cara untuk mengatasi risiko keamanan informasi sistem penerimaan peserta didik baru pada SD Muhammadiyah 3 Sibolga.

Program HIHAT dipasangkan untuk mengumpulkan semua informasi serangan yang masuk pada honeypot.

Dari hasil penelitian, dapat disimpulkan bahwa implementasi metode honeypot telah membantu meningkatkan keamanan informasi pada sistem penerimaan peserta didik baru. Melalui pendekatan ini, pihak sekolah dapat mengidentifikasi dan mengantisipasi serangan yang dapat terjadi, seperti SQL Injection dan XSS. Selain itu, program HIHAT yang digunakan untuk mengumpulkan informasi serangan pada honeypot berperan penting dalam analisis dan tindakan lebih lanjut untuk meningkatkan keamanan sistem. Dengan begitu, metode honeypot menjadi alat efektif dalam menghadapi ancaman keamanan pada PPDB Online SD Muhammadiyah 03 Sibolga.

6.2. Saran

Adapaun saran-saran dari peneliti pada sistem yang telah dikembangkan maupun pengembangan selanjutnya pada penelitian ini adalah sebagai berikut :

1. Pastikan sistem memberikan pemberitahuan secara tepat waktu kepada calon peserta didik dan orang tua mengenai tahapan pendaftaran, jadwal tes, dan hasil seleksi. Berikan informasi yang jelas dan komprehensif mengenai persyaratan pendaftaran dan prosedur yang harus diikuti.
2. Pastikan sistem PPDB dioptimalkan untuk memberikan kinerja yang cepat dan responsif. Waktu pemuatan yang lama dan keterlambatan dalam proses pendaftaran dapat mengurangi minat calon peserta didik baru.
3. Penting untuk selalu memperbarui dan meningkatkan sistem keamanan, karena teknik serangan juga terus berkembang. Metode honeypot bisa

menjadi bagian dari strategi yang lebih komprehensif untuk mengamankan sistem informasi sekolah secara keseluruhan.

4. Terapkan lapisan keamanan yang kuat, termasuk enkripsi data sensitif, otentikasi ganda, dan sistem deteksi intrusi. Selain itu, lakukan uji penetrasi secara berkala untuk mengidentifikasi dan mengatasi potensi kerentanan sistem.

DAFTAR PUSTAKA

Al-Khowarizmi, Halim Maulana, Lutfi Basit (2020). Implementasi Penerimaan Peserta Didik Baru (PPDB) Berbasis Web pada Sekolah Dasar Alam Semangat Bangsa dan Taman Kanak-Kanak Kartini Kecamatan Medan Johor. Jurnal Pengabdian Barelang, 2 (3), 5-8.

Dilla Ayu Dwipitaloka, Enny Dwi Oktaviyani, Felicia Sylviana, Licantik (2020). Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) Dan Registrasi Online Berbasis Website Pada SMP Negeri 6 Palangka Raya. Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika, 14 (2), 119-128.

Asri Ulfah Wulan Sari, Ali Imron, Ahmad Yusuf Sobri (2020). Efektivitas Penerimaan Peserta Didik Baru (PPDB) Melalui Sistem Penerimaan Peserta Didik Online. Manajemen Pendidikan-Pascasarjana, 1-10.

Nur Ariesanto Ramdhan, Dimas Wahyudi (2019). Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) Berbasis WEB Di SMP Negri 1 Wanasari Brebes. Information Technology Journal (INTECH) of UMUS, 1 (1), 56-65.

Wiwin Wianti (2019). Pelaksanaan Pelayanan Penerimaan Peserta Didik Baru (PPDB) Pada Sekolah Dasar Al-Fath Cirendeu Tangerang Selatan. *Jurnal Pendidikan Dan Kewirausahaan*, 7 (1), 1-27

Marlinda Sanglise (2022). Penerimaan Peserta Didik Baru (PPDB) Pada SD Inpres Kalikodok Bintuni Berbasis Web. Jurnal Ilmiah Indonesia, 7 (9), 14581- 14592.

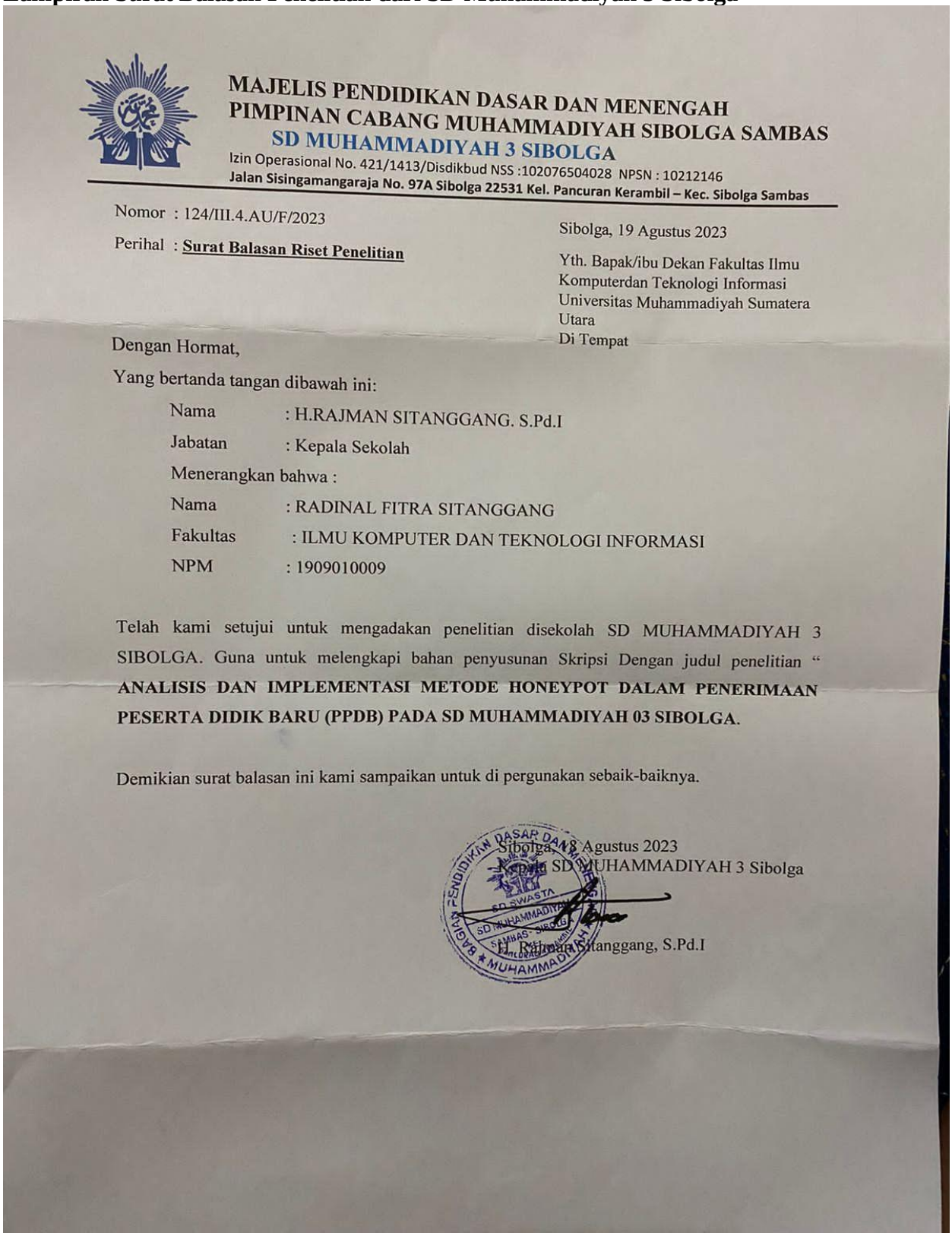
Anton Yudahana, Imam Riadi, Ade Elvina (2023). Perancangan Sistem Informasi Pendaftaran Peserta Didik Baru (PPDB) Berbasis Web Menggunakan Metode Rapid Apllication Development. Jurnal Teknologi dan Sistem Informasi Univrab, 8 (1), 47-58.

Wahyu Purnama Sari, I Nyoman Adhi Palguna Putra (2023). Analisis Serangan Hacker Menggunakan Honeypot High Interaction (HIHAT). Jurnal TIARSE, 14 (1), 13-18.

Lukito Prima Aidin, Surya Michrandi Nasution, Fairuz Azmi (2016). Implementasi High Interaction Honeypot Pada Server. e-Proceeding of Engineering, 3 (2), 2172- 2177.

Ramdhani, Susetyo (2017). Kwalitas Administrasi Sekolah Alam Semangat Bangsa. Jurnal Pengabdian Barelang. SI, FT. UN PGRI Kediri.

Lampiran Surat Balasan Penelitian dari SD Muhammadiyah 3 Sibolga



MAJELIS PENDIDIKAN DASAR DAN MENENGAH
PIMPINAN CABANG MUHAMMADIYAH SIBOLGA SAMBAS
SD MUHAMMADIYAH 3 SIBOLGA
Izin Operasional No. 421/1413/Disdikbud NSS :102076504028 NPSN : 10212146
Jalan Sisingamangaraja No. 97A Sibolga 22531 Kel. Pancuran Kerambil – Kec. Sibolga Sambas

Nomor : 124/III.4.AU/F/2023
Perihal : **Surat Balasan Riset Penelitian**

Sibolga, 19 Agustus 2023

Yth. Bapak/ibu Dekan Fakultas Ilmu Komputerdan Teknologi Informasi
Universitas Muhammadiyah Sumatera Utara
Di Tempat

Dengan Hormat,

Yang bertanda tangan dibawah ini:

Nama : H.RAJMAN SITANGGANG. S.Pd.I
Jabatan : Kepala Sekolah

Menerangkan bahwa :

Nama : RADINAL FITRA SITANGGANG
Fakultas : ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
NPM : 1909010009

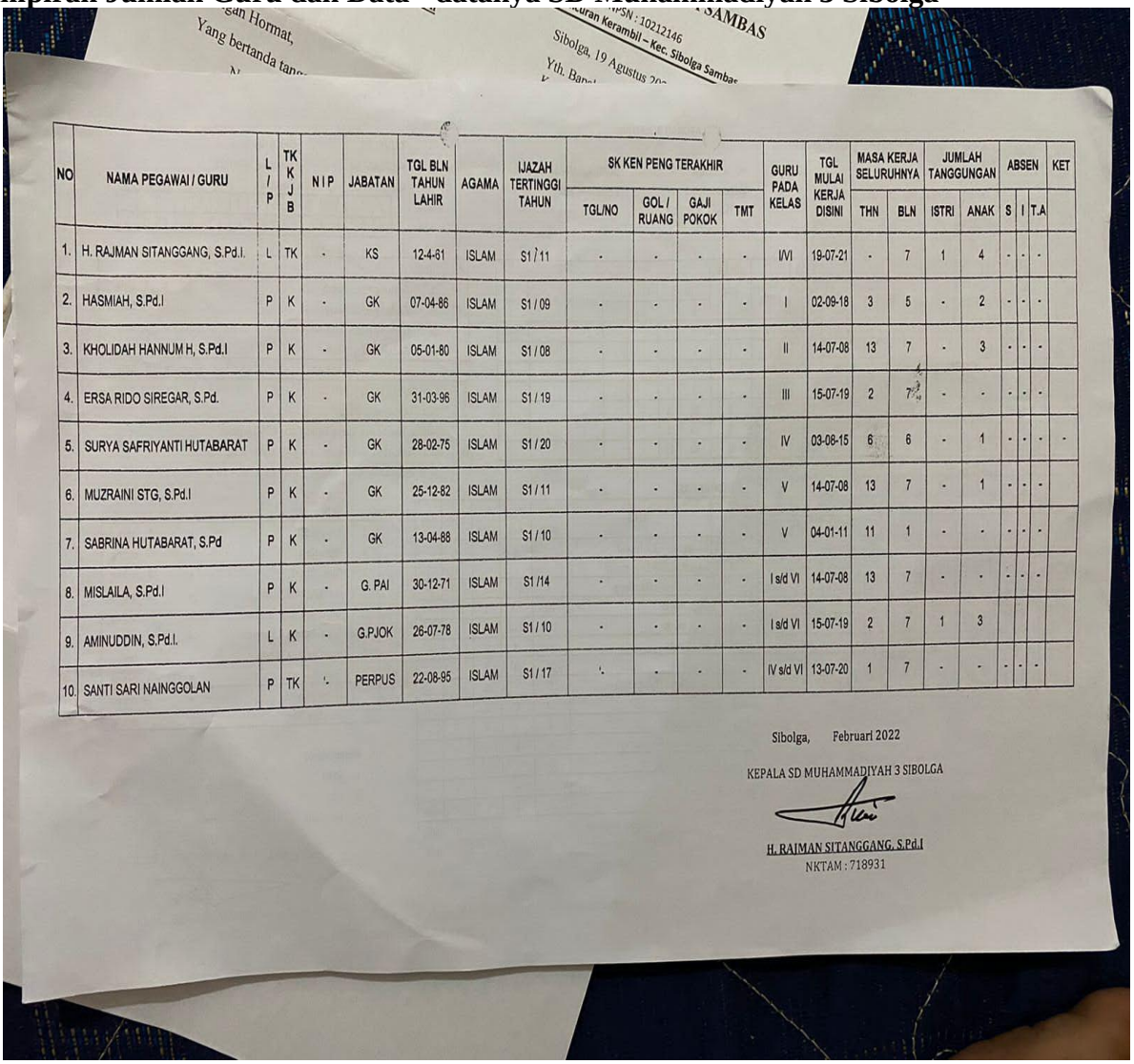
Telah kami setujui untuk mengadakan penelitian disekolah SD MUHAMMADIYAH 3 SIBOLGA. Guna untuk melengkapi bahan penyusunan Skripsi Dengan judul penelitian " **ANALISIS DAN IMPLEMENTASI METODE HONEYPOT DALAM PENERIMAAN PESERTA DIDIK BARU (PPDB) PADA SD MUHAMMADIYAH 03 SIBOLGA.**

Demikian surat balasan ini kami sampaikan untuk di pergunakan sebaik-baiknya.

Sibolga, 18 Agustus 2023
Kepala SD MUHAMMADIYAH 3 Sibolga

H. Rahman Sitanggang, S.Pd.I

Lampiran Jumlah Guru dan Data - datanya SD Muhammadiyah 3 Sibolga



Yang bertanda tan...gan Hormat,

...SAMBAS

...Kuran Kerambil – Kec. Sibolga Sambas

...NPSN : 10212146

Sibolga, 19 Agustus 20...

Yth. Ban...

NO	NAMA PEGAWAI / GURU	L / P	TK KJB	NIP	JABATAN	TGL BLN TAHUN LAHIR	AGAMA	IJAZAH TERTINGGI TAHUN	SK KEN PENG TERAKHIR				GURU PADA KELAS	TGL MULAI KERJA DISINI	MASA KERJA SELURUHNYA		JUMLAH TANGGUNGAN		ABSEN			KET
									TGL/NO	GOL / RUANG	GAJI POKOK	TMT			THN	BLN	ISTRI	ANAK	S	I	T.A	
1.	H. RAJMAN SITANGGANG, S.Pd.I.	L	TK	-	KS	12-4-61	ISLAM	S1 / 11	-	-	-	-	I/VI	19-07-21	-	7	1	4	-	-	-	
2.	HASMIAH, S.Pd.I	P	K	-	GK	07-04-86	ISLAM	S1 / 09	-	-	-	-	I	02-09-18	3	5	-	2	-	-	-	
3.	KHOLIDAH HANNUM H, S.Pd.I	P	K	-	GK	05-01-80	ISLAM	S1 / 08	-	-	-	-	II	14-07-08	13	7	-	3	-	-	-	
4.	ERSA RIDO SIREGAR, S.Pd.	P	K	-	GK	31-03-96	ISLAM	S1 / 19	-	-	-	-	III	15-07-19	2	7	-	-	-	-	-	
5.	SURYA SAFRIYANTI HUTABARAT	P	K	-	GK	28-02-75	ISLAM	S1 / 20	-	-	-	-	IV	03-08-15	6	6	-	1	-	-	-	-
6.	MUZRAINI STG, S.Pd.I	P	K	-	GK	25-12-82	ISLAM	S1 / 11	-	-	-	-	V	14-07-08	13	7	-	1	-	-	-	
7.	SABRINA HUTABARAT, S.Pd	P	K	-	GK	13-04-88	ISLAM	S1 / 10	-	-	-	-	V	04-01-11	11	1	-	-	-	-	-	
8.	MISLAILA, S.Pd.I	P	K	-	G. PAI	30-12-71	ISLAM	S1 /14	-	-	-	-	I s/d VI	14-07-08	13	7	-	-	-	-	-	
9.	AMINUDDIN, S.Pd.I.	L	K	-	G.PJOK	26-07-78	ISLAM	S1 / 10	-	-	-	-	I s/d VI	15-07-19	2	7	1	3				
10.	SANTI SARI NAINGGOLAN	P	TK	-	PERPUS	22-08-95	ISLAM	S1 / 17	-	-	-	-	IV s/d VI	13-07-20	1	7	-	-	-	-	-	

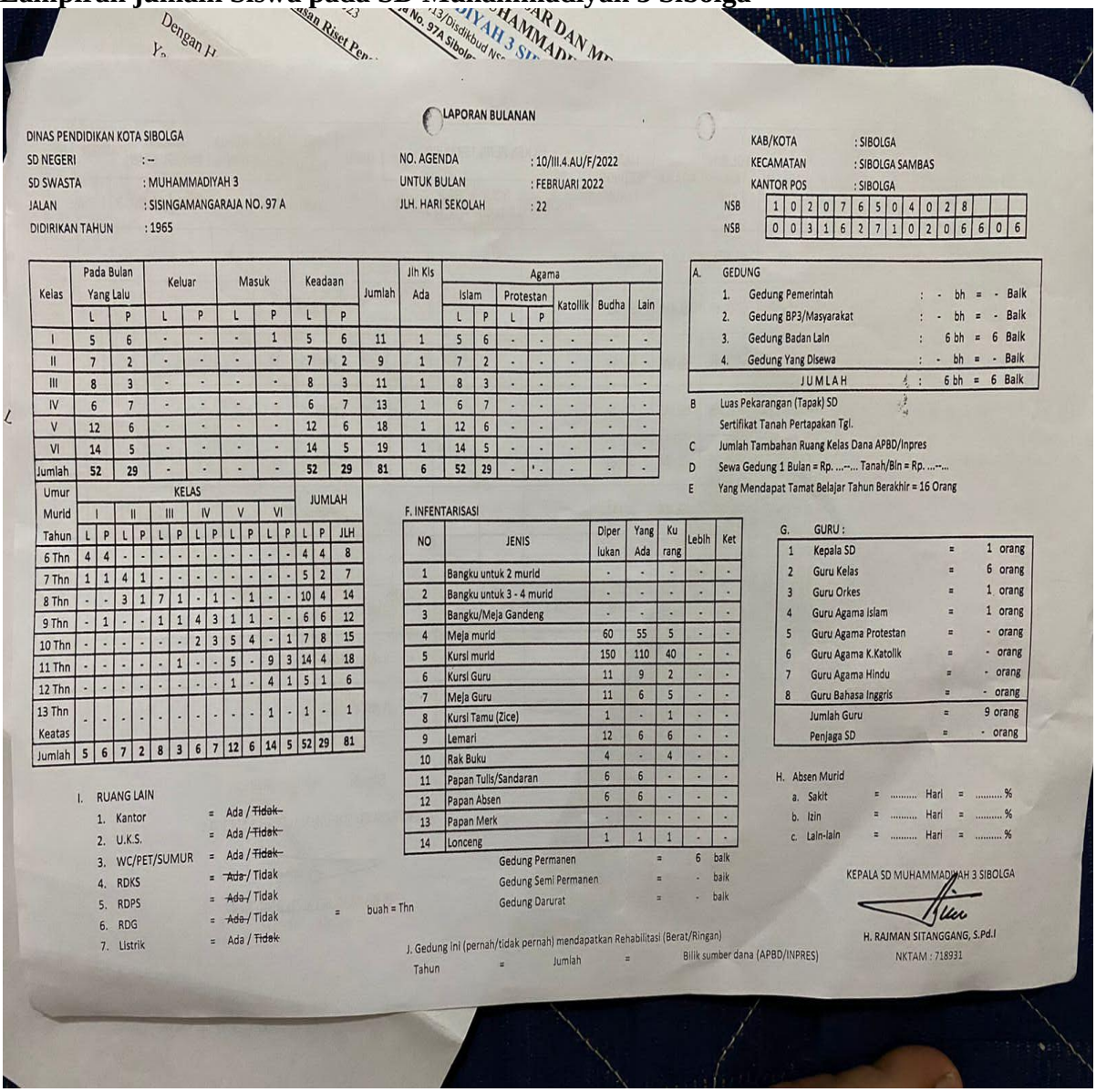
Sibolga, Februari 2022

KEPALA SD MUHAMMADIYAH 3 SIBOLGA

H. RAIMAN SITANGGANG, S.Pd.I

NKTAM : 718931

Lampiran jumalh Siswa pada SD Muhammadiyah 3 Sibolga



LAPORAN BULANAN

DINAS PENDIDIKAN KOTA SIBOLGA
SD NEGERI : --
SD SWASTA : MUHAMMADIYAH 3
JALAN : SISINGAMANGARAJA NO. 97 A
DIDIRIKAN TAHUN : 1965

NO. AGENDA : 10/III.4.AU/F/2022
UNTUK BULAN : FEBRUARI 2022
JLH. HARI SEKOLAH : 22

KAB/KOTA : SIBOLGA
KECAMATAN : SIBOLGA SAMBAS
KANTOR POS : SIBOLGA

NSB 1 0 2 0 7 6 5 0 4 0 2 8
NSB 0 0 3 1 6 2 7 1 0 2 0 6 6 0 6

Kelas	Pada Bulan Yang Lalu		Keluar		Masuk		Keadaan		Jumlah	Jlh Kls Ada	Agama						
											Islam		Protestan		Katollik	Budha	Lain
	L	P	L	P	L	P	L	P			L	P	L	P			
I	5	6	-	-	-	1	5	6	11	1	5	6	-	-	-	-	-
II	7	2	-	-	-	-	7	2	9	1	7	2	-	-	-	-	-
III	8	3	-	-	-	-	8	3	11	1	8	3	-	-	-	-	-
IV	6	7	-	-	-	-	6	7	13	1	6	7	-	-	-	-	-
V	12	6	-	-	-	-	12	6	18	1	12	6	-	-	-	-	-
VI	14	5	-	-	-	-	14	5	19	1	14	5	-	-	-	-	-
Jumlah	52	29	-	-	-	-	52	29	81	6	52	29	-	-	-	-	-

A. GEDUNG
1. Gedung Pemerintah : - bh = - Baik
2. Gedung BP3/Masyarakat : - bh = - Baik
3. Gedung Badan Lain : 6 bh = 6 Baik
4. Gedung Yang Disewa : - bh = - Baik
JUMLAH : 6 bh = 6 Baik

B Luas Pekarangan (Tapak) SD
Sertifikat Tanah Pertapakan Tgl.
C Jumlah Tambahan Ruang Kelas Dana APBD/Inpres
D Sewa Gedung 1 Bulan = Rp. ...--... Tanah/Bln = Rp. ...--...
E Yang Mendapat Tamat Belajar Tahun Berakhir = 16 Orang

Umur Murid	KELAS												JUMLAH		
	I		II		III		IV		V		VI				
Tahun	L	P	L	P	L	P	L	P	L	P	L	P	L	P	JLH
6 Thn	4	4	-	-	-	-	-	-	-	-	-	-	4	4	8
7 Thn	1	1	4	1	-	-	-	-	-	-	-	-	5	2	7
8 Thn	-	-	3	1	7	1	-	1	-	1	-	-	10	4	14
9 Thn	-	1	-	-	1	1	4	3	1	1	-	-	6	6	12
10 Thn	-	-	-	-	-	-	2	3	5	4	-	1	7	8	15
11 Thn	-	-	-	-	-	1	-	-	5	-	9	3	14	4	18
12 Thn	-	-	-	-	-	-	-	-	1	-	4	1	5	1	6
13 Thn Keatas	-	-	-	-	-	-	-	-	-	-	1	-	1	-	1
Jumlah	5	6	7	2	8	3	6	7	12	6	14	5	52	29	81

F. INFENTARISASI

NO	JENIS	Diperlukan	Yang Ada	Kurang	Lebih	Ket
1	Bangku untuk 2 murid	-	-	-	-	-
2	Bangku untuk 3 - 4 murid	-	-	-	-	-
3	Bangku/Meja Gandeng	-	-	-	-	-
4	Meja murid	60	55	5	-	-
5	Kursi murid	150	110	40	-	-
6	Kursi Guru	11	9	2	-	-
7	Meja Guru	11	6	5	-	-
8	Kursi Tamu (Zice)	1	-	1	-	-
9	Lemari	12	6	6	-	-
10	Rak Buku	4	-	4	-	-
11	Papan Tulis/Sandaran	6	6	-	-	-
12	Papan Absen	6	6	-	-	-
13	Papan Merk	-	-	-	-	-
14	Lonceng	1	1	1	-	-

G. GURU :

1	Kepala SD	=	1 orang
2	Guru Kelas	=	6 orang
3	Guru Orkes	=	1 orang
4	Guru Agama Islam	=	1 orang
5	Guru Agama Protestan	=	- orang
6	Guru Agama K.Katollik	=	- orang
7	Guru Agama Hindu	=	- orang
8	Guru Bahasa Inggris	=	- orang
	Jumlah Guru	=	9 orang
	Penjaga SD	=	- orang

I. RUANG LAIN
1. Kantor = Ada / ~~Tidak~~
2. U.K.S. = Ada / ~~Tidak~~
3. WC/PET/SUMUR = Ada / ~~Tidak~~
4. RDKS = ~~Ada~~ / Tidak
5. RDPS = ~~Ada~~ / Tidak
6. RDG = ~~Ada~~ / Tidak
7. Listrik = Ada / ~~Tidak~~

Gedung Permanen = 6 baik
Gedung Semi Permanen = - baik
Gedung Darurat = - baik

= buah = Thn

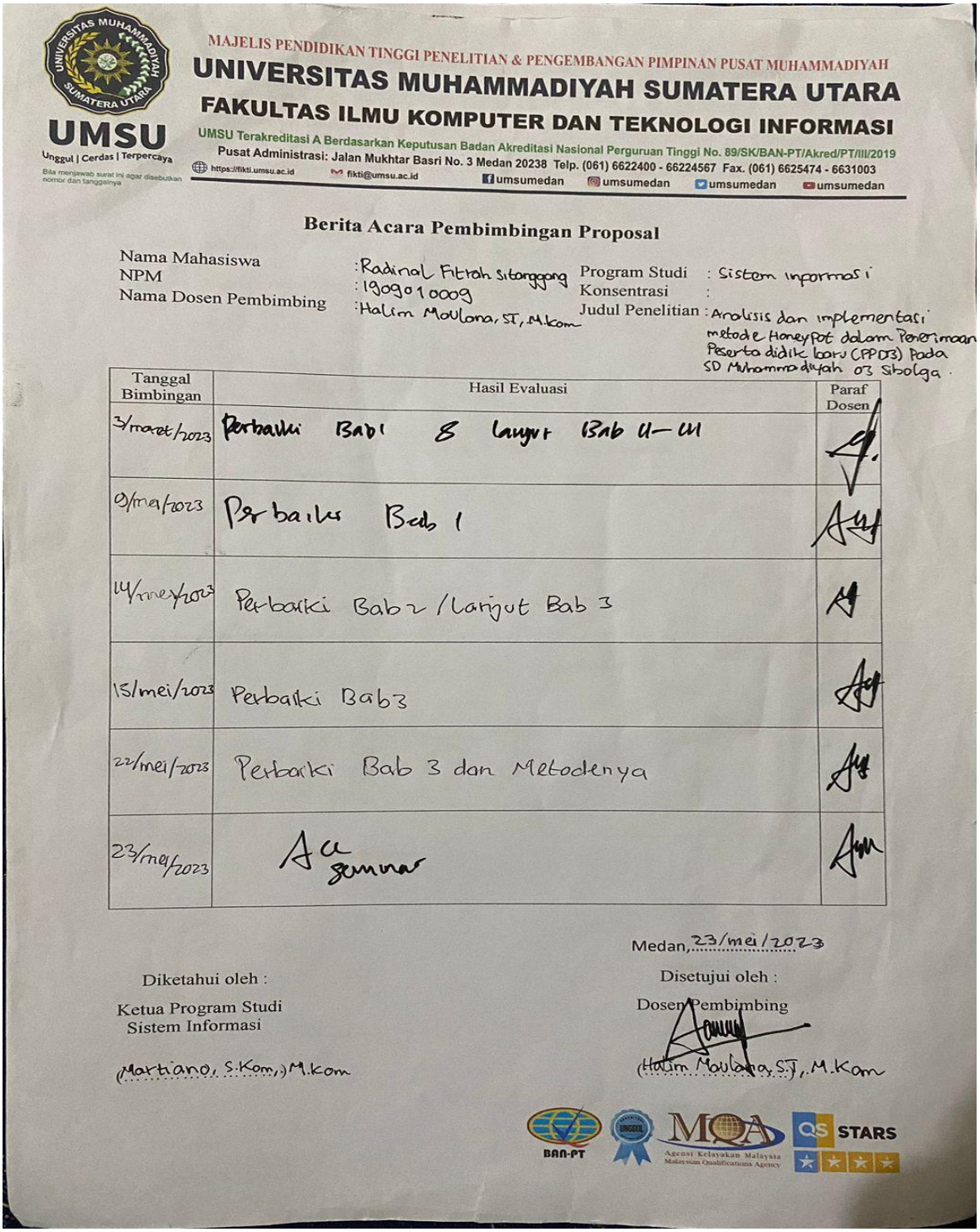
H. Absen Murid
a. Sakit = ... Hari = ...%
b. Izin = ... Hari = ...%
c. Lain-lain = ... Hari = ...%

KEPALA SD MUHAMMADIYAH 3 SIBOLGA

H. RAJMAN SITANGGANG, S.Pd.I
NKTAM : 718931

J. Gedung ini (pernah/tidak pernah) mendapatkan Rehabilitasi (Berat/Ringan)
Tahun = Jumlah = Bilik sumber dana (APBD/INPRES)

Lampiran 4. Berita Acara Bimbingan Proposal



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

UMSU
Unggul | Cerdas | Terpercaya
Bila menjawab surat ini agar disebutkan nomor dan tanggalnya

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Radinal Fitrah Sitanggang
NPM : 1909010009
Nama Dosen Pembimbing : Halim Maulana, ST, M.Kom
Program Studi : Sistem Informasi
Konsentrasi :
Judul Penelitian : Analisis dan implementasi metode Honeypot dalam Penerimaan Peserta didik baru (PPDB) pada SD Muhammadiyah 03 Sibolga.

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
3/maret/2023	Perbaiki Bab 1 & lanjut Bab II – III	
9/mei/2023	Perbaiki Bab 1	
14/mei/2023	Perbaiki Bab 2 / lanjut Bab 3	
15/mei/2023	Perbaiki Bab 3	
22/mei/2023	Perbaiki Bab 3 dan Metodenya	
23/mei/2023	Acc seminar	

Medan, 23/mei/2023

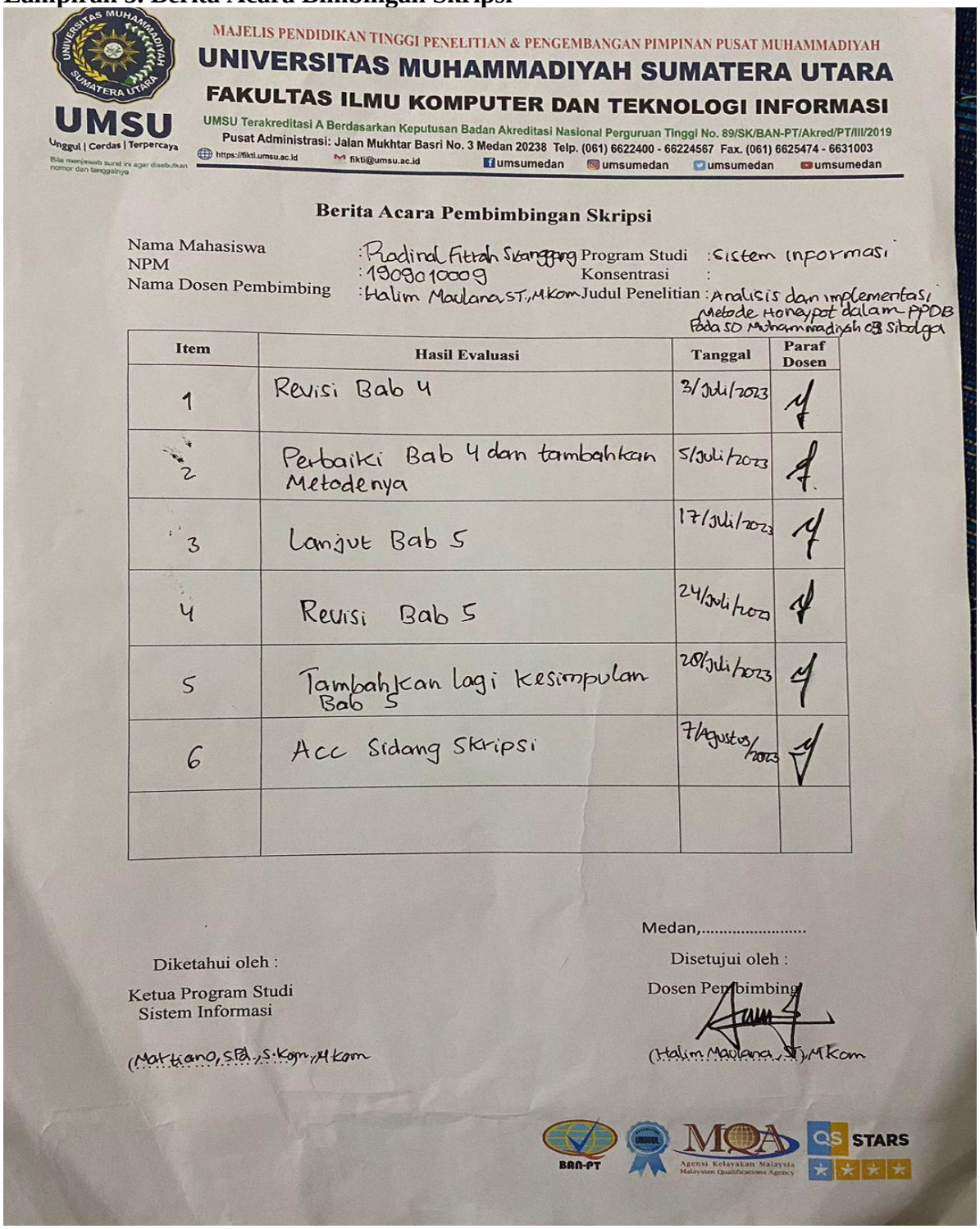
Diketahui oleh :
Ketua Program Studi
Sistem Informasi

(Martiano, S.Kom.,) M.Kom

Disetujui oleh :
Dosen Pembimbing

(Halim Maulana, S.T., M.Kom)

Lampiran 5. Berita Acara Bimbingan Skripsi



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

UMSU Unggul | Cerdas | Terpercaya

Bila menjawab surat ini agar disebutkan nomor dan tanggalnya

Berita Acara Pembimbingan Skripsi

Nama Mahasiswa : Rodinal Fitrah Siregar
NPM : 1909010009
Nama Dosen Pembimbing : Halim Maulana, ST., M.Kom
Program Studi : Sistem Informasi
Konsentrasi :
Judul Penelitian : Analisis dan Implementasi Metode Honeypot dalam PPDB Pada SD Muhammadiyah 08 Sibolga

Item	Hasil Evaluasi	Tanggal	Paraf Dosen
1	Revisi Bab 4	3/Juli/2023	
2	Perbaiki Bab 4 dan tambahkan Metodenya	5/Juli/2023	
3	Lanjut Bab 5	17/Juli/2023	
4	Revisi Bab 5	24/Juli/2023	
5	Tambahkan lagi kesimpulan Bab 5	28/Juli/2023	
6	Acc Sidang Skripsi	7/Agustus/2023	

Medan,.....

Diketahui oleh :
Ketua Program Studi
Sistem Informasi

(Maktuano, S.Pd., S.Kom., M.Kom)

Disetujui oleh :
Dosen Pembimbing

(Halim Maulana, ST., M.Kom)