UJI PENETRASI KEAMANAN SISTEM INFORMASI PADA *WEBSITE* MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

(Studi Kasus Dinas Komunikasi dan Informatika Kabupaten Mesuji)

(Skripsi)

Oleh :

AGHASTYA ICHSANUDIN ARIF
2115061105

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS LAMPUNG
2025

UJI PENETRASI KEAMANAN SISTEM INFORMASI PADA *WEBSITE* MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

(Studi Kasus Dinas Komunikasi dan Informatika Kabupaten Mesuji)

Oleh :

AGHASTYA ICHSANUDIN ARIF

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar SARJANA TEKNIK

Pada

Program Studi S1 Teknik Informatika

Fakultas Teknik

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

2025

ABSTRAK

UJI PENETRASI KEAMANAN SISTEM INFORMASI PADA *WEBSITE* MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

(Studi Kasus Dinas Komunikasi dan Informatika Kabupaten Mesuji)

Oleh

AGHASTYA ICHSANUDIN ARIF

Keamanan website pada layanan digital pemerintah memiliki peran penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi publik. Penelitian ini bertujuan mengidentifikasi serta mengevaluasi kerentanan pada domain dan subdomain website Dinas Komunikasi dan Informatika Kabupaten Mesuji dengan menggunakan Penetration Testing Execution Standard (PTES). Kerangka PTES memberikan prosedur pengujian yang terstruktur, meliputi tahap intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Beberapa alat seperti WhatWeb, Subfinder, Nmap, dan Xray digunakan untuk mengumpulkan informasi, melakukan enumerasi subdomain, memindai port terbuka, serta mendeteksi potensi celah keamanan. Hasil penelitian menunjukkan adanya sejumlah kerentanan dengan tingkat risiko beragam, termasuk konfigurasi server yang lemah, potensi SQL injection, penggunaan teknologi usang, serta paparan informasi sensitif. Pengujian eksploitasi memvalidasi bahwa beberapa kerentanan dapat dimanfaatkan untuk mengganggu keamanan sistem. Temuan ini menegaskan perlunya peningkatan praktik keamanan siber pada infrastruktur digital pemerintah. Rekomendasi mencakup penguatan konfigurasi server, pembaruan sistem berkala, penerapan mekanisme pertahanan berlapis, dan pelaksanaan uji penetrasi rutin untuk menjaga ketahanan sistem terhadap ancaman siber.

Kata kunci : uji penetrasi, analisis kerentanan, keamanan website, *SQL Injection*.

ABSTRACT

INFORMATION SYSTEM SECURITY PENETRATION TESTING ON WEBSITES USING THE PENETRATION TESTING EXECUTION STANDARD (PTES) METHOD

(Case Study of Dinas Komunikasi dan Informatika Kabupaten Mesuji)

By

AGHASTYA ICHSANUDIN ARIF

Website security in government digital services plays an important role in maintaining the confidentiality, integrity, and availability of public information. This study aims to identify and evaluate vulnerabilities in the domain and subdomain of the Mesuji Regency Communication and Information Agency website using the Penetration Testing Execution Standard (PTES). The PTES framework provides structured testing procedures, including intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting stages. Several tools such as WhatWeb, Subfinder, Nmap, and Xray were used to gather information, enumerate subdomains, scan open ports, and detect potential security gaps. The results of the study revealed a number of vulnerabilities with varying levels of risk, including weak server configuration, potential SQL injection, use of outdated technology, and exposure of sensitive information. Exploitation testing validated that some vulnerabilities could be exploited to compromise system security. These findings emphasize the need to improve cybersecurity practices in government digital infrastructure. Recommendations include strengthening server configurations, performing regular system updates, implementing layered defense mechanisms, and conducting routine penetration tests to maintain system resilience against cyber threats.

Keywords: penetration testing, vulnerability analysis, website security, SQL injection.

Judul Skripsi	:	Uji Penetrasi Keamanan Sistem Informasi Pada *Website* Menggunakan Metode *Penetration Testing Execution Standard* (Ptes) (Studi Kasus Dinas Komunikasi Dan Informatika Kabupaten Mesuji)
Nama Mahasiswa	:	Aghastya Ichsanudin Arif
Nomor Pokok Mahasiswa	:	2115061105
Program Studi	:	Teknik Informatika
Jurusan	:	Teknik Elektro
Fakultas	:	Teknik

MENYETUJUI

1. Komisi Pembimbing

Pembimbing Utama	Pembimbing Pendamping
Ir. Gigih Forda Nama, S.T., M.T.I., IPM	**Mahendra Pratama, S.T., M.Eng.**
NIP. 198307122008121003	NIP. 199112152019031013

2. Mengetahui

Ketua Jurusan Teknik Elektro	Ketua Program Studi Teknik Informatika
Herlinawati, S.T., M.T.	**Yessi Mulyani, S.T., M.T.**
NIP. 197103141999032001	NIP. 197312262000122001

MENGESAHKAN

1. Tim Penguji

   Ketua : **Ir. Gigih Forda Nama, S.T., M.T.I., IPM** .....

   Sekretaris : **Mahendra Pratama, S.T., M.Eng.** .....

   Penguji : **Dr. Ir. M. Komarudin, S.T., M.T.** .....

2. Dekan Fakultas Teknik

Dr. Ahmad Herison, S.T., M.T.
NIP. 196910302000031001

Tanggal Lulus Ujian Skripsi :**23 Desember 2025**

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi berjudul "Uji Penetrasi Keamanan Sistem Informasi Pada *Website* Menggunakan Metode *Penetration Testing Execution Standard* (PTES) (Studi Kasus Dinas Komunikasi dan Informatika Kabupaten Mesuji)" sepenuhnya merupakan hasil karya saya sendiri. Apabila di kemudian hari terbukti pernyataan ini tidak benar, saya siap menerima sanksi sesuai dengan ketentuan hukum yang berlaku.

Bandar Lampung, 28 Januari 2026

Penulis,

Aghastya Ichsanudin Arif

NPM. 2115061105

RIWAYAT HIDUP

Penulis dilahirkan di Bandar Lampung pada tanggal 24 Maret 2003 sebagai putra semata wayang, dari pasangan Bapak Ichsan Tito Subur, S.Kom., M.Si. dan Ibu Suci Amanah. Penulis menyelesaikan pendidikan formal di SDN 1 Beringin Raya pada tahun 2015, setelahnya melanjutkan ke SMPN 1 Bandar Lampung dan lulus pada tahun 2018, serta menamatkan pendidikan menengah atas di SMAN 9 Bandar Lampung pada tahun 2021. Pada tahun 2021, penulis diterima sebagai mahasiswa Program Studi Teknik Informatika Universitas Lampung melalui jalur seleksi SBMPTN. Selama masa perkuliahan, penulis aktif berpartisipasi dalam berbagai kegiatan, antara lain :

1. Menerima Beasiswa Polri Presisi 2023.
2. Mengikuti program VSGA *Junior Network Administrator Batch* 1
3. Mengikuti kegiatan Studi Independen Bersertifikat dari Kementerian Pendidikan dan Budaya di mitra Gama Multi Usaha Mandiri *cybersecurity* pada tahun 2023.
4. Mengikuti program FGA IT *Fundamental Batch* 3 *Digital Talent Scholarship* Komdigi.
5. Menjadi pengurus aktif departemen Pengembangan Keteknikan Himpunan Mahasiswa Teknik Elektro pada periode tahun 2022 – 2023.
6. Menjadi Staff Ahli Kajian dan Aksi Strategis BEM Fakultas Teknik Universitas Lampung pada periode 2023.

MOTTO

"*Lifelong Learning*"

(Penulis)

"Palu Gada, Apa Lu Mau Gua Ada"

(Ir. Gigih Forda Nama, S.T., M.T.I., IPM)

PERSEMBAHAN

Dengan segala kerendahan hati dan rasa syukur kepada Allah SWT atas segala nikmat, rahmat, dan karunia-Nya, skripsi ini saya persembahkan kepada kedua orang tua tercinta yang selalu mendoakan, mendukung, dan memberikan kasih sayang tanpa henti sepanjang hidup saya. Kepada keluarga yang senantiasa menjadi sumber semangat, dan kepada sahabat-sahabat seperjuangan yang selalu hadir dalam suka maupun duka.

SANWACANA

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, taufik, dan hidayah-Nya sehingga skripsi dengan judul "Pengembangan Tongkat Pintar Berbasis IoT Untuk Tunanetra Dengan Deteksi Objek Dan GPS" dapat diselesaikan. Dalam perjalanan penyusunan skripsi ini, penulis memperoleh begitu banyak dukungan, arahan, serta bantuan baik dalam bentuk moril maupun materil dari berbagai pihak. Oleh karena itu, dengan rasa hormat dan terima kasih yang tulus, penulis menyampaikan apresiasi yang sebesar-besarnya kepada :

1. Kedua orang tua tercinta beserta keluarga besar yang senantiasa memberikan doa, kasih sayang, dukungan, serta motivasi tiada henti kepada penulis;
2. Bapak Dr. Ahmad Herison, S.T., M.T., selaku Dekan Fakultas Teknik, Universitas Lampung;
3. Ibu Herlinawati, S.T., M.T., selaku Ketua Jurusan Teknik Elektro Universitas Lampung;
4. Ibu Yessi Mulyani, S.T., M.T., selaku Ketua Program Studi Teknik Informatika, Fakultas Teknik, Universitas Lampung, yang telah memberikan dukungan dan kesempatan serta arahan dalam menyelesaikan skripsi ini;
5. Bapak Ir. Gigih Forda Nama, S.T., M.T.I., IPM selaku Dosen Pembimbing Utama yang dengan sabar dan penuh perhatian telah memberikan bimbingan, saran, serta arahan selama proses penyusunan skripsi ini;
6. Bapak Mahendra Pratama, S.T., M.Eng. selaku Dosen Pembimbing Pendamping yang telah meluangkan waktunya untuk membimbing dan memberikan saran bagi penulis dalam menyelesaikan penulisan skripsi;
7. Bapak Dr. Ir. M. Komarudin, S.T., M.T. selaku Dosen Pembimbing Akademik sekaligus Dosen Penguji yang telah memberikan arahan akademik selama penulis menempuh pendidikan di program studi ini serta

memberikan saran dan kritik yang sangat berharga demi kesempurnaan dalam skripsi ini;

8. Seluruh Dosen Program Studi Teknik Informatika, yang telah memberikan ilmu dan pengetahuan selama masa perkuliahan;

Penulis berharap agar laporan ini dapat menjadi referensi bagi pengembangan keilmuan di bidang teknik informatika. Oleh karena itu, semoga penelitian ini bermanfaat bagi yang membacanya.

Bandar Lampung, 28 Januari 2026

Penulis,

Aghastya Ichsanudin Arif

NPM. 2115061105

DAFTAR ISI

ABSTRAK ..... **i**
PERSEMBAHAN ..... **viii**
SANWACANA ..... **ix**
DAFTAR ISI ..... **xi**
DAFTAR GAMBAR ..... **xiv**
DAFTAR TABEL ..... **xv**
I. PENDAHULUAN **2**
1.1 Latar Belakang 2
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 2
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 3
II. LANDASAN TEORI **5**
2.1 Penelitian Terdahulu 5
2.2 Website 16
2.3 Keamanan Sistem Informasi 17
2.4 *Penetration Testing Execution Standard* 18
2.4.1 *Pre-Engagement* 19
2.4.2 *Intelligence Gathering* 20
2.4.3 *Threat Modelling* 20
2.4.4 *Vulnerability Analysis* 20
2.4.5 *Exploitation* 20
2.4.6 *Post Exploitation* 20
2.4.7 *Reporting* 21
2.5 *Top 10 Vulnerabilities* 21
2.5.1 *Broken Access Control* 21
2.5.2 *Cryptographic Failures* 22
2.5.3 *Injection* 22
2.5.4 *Insecure Design* 22
2.5.5 *Security Misconfiguration* 22
2.5.6 *Vulnerable and Outdated Components* 22
2.5.7 *Identification and Authentication Failures* 22
2.5.8 *Software and Data Integrity Failures* 23
2.5.9 *Security Logging and Monitoring Failures* 23
2.5.10 *Server-Side Request Forgorey (SSRF)* 23
2.6 Parrot *Security* OS 24
2.7 Sqlmap 25
2.8 Xray 25
2.9 Subfinder 25
2.10 Whatweb 25

2.11 Nmap 26
2.12 Httpx 26
III. METODOLOGI PENELITIAN 27
3.1 Waktu dan Tempat Pelaksanaan 27
3.2 Alat dan Bahan Penelitian 28
3.2.1 Perangkat Lunak (*Software*) 28
3.2.2 Perangkat Keras (*Hardware*) 29
3.2.3 Objek Peneliian 29
3.3 Diagram Alir Penelitian 30
3.4 Diagram Arsitektur 32
IV. HASIL DAN PEMBAHASAN 34
4.1 *Pre-Engagement* 34
4.2 *Information Gathering* 35
4.2.1 Whatweb 35
4.2.2 Nmap 36
4.2.3 Subfinder 37
4.3 *Threat Modelling* 39
4.4 *Vulnerability Analysis* 42
4.4.1 Xray *Scanner* 42
4.5 *Exploitation* 47
4.5.1 Eksploitasi *Sql Injection* pada *Subdomain* https://web.mesujikab.go.id/ Parameter id 48
4.5.2 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter bentuk_peraturan 49
4.5.3 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter status 50
4.5.4 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter jenis_peraturan 51
4.5.5 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter judul 53
4.5.6 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter nomor_peraturan 54
4.6 *Post-Exloitation* 55
4.6.1 *Post-Expoiation* Pada *Subdomain* https://web.mesujikab.go.id/ ... 55
4.6.1.a *Subdomain* https://web.mesujikab.go.id/ Paramater id 56
4.6.2 *Post-Exploitation* Pada *Subdomain* https://jdih.mesujikab.go.id/ Parameter bentuk_peraturan 61
4.6.2.a *Subdomain* https://jdih.mesujikab.go.id/ Parameter bentuk_peraturan 61
4.6.2.b *Subdomain* https://jdih.mesujikab.go.id/ Parameter status 64
4.6.2.c *Subdomain* https://jdih.mesujikab.go.id/ Parameter jenis_peraturan 66
4.6.2.d *Subdomain* https://jdih.mesujikab.go.id/ Parameter judul .. 69
4.6.2.e *Subdomain* https://jdih.mesujikab.go.id/ Parameter nomor_peraturan 71
4.7 *Reporting* 73
V. KESIMPULAN DAN SARAN 76
5.1 Kesimpulan 76

5.2 Saran 77
DAFTAR PUSTAKA 78
LAMPIRAN 80

DAFTAR GAMBAR

2.4.1 *Pre-Engagement* 19
2.4.2 *Intelligence Gathering* 20
2.4.3 *Threat Modelling* 20
2.4.4 *Vulnerability Analysis* 20
2.4.5 *Exploitation* 20
2.4.6 *Post Exploitation* 20
2.4.7 *Reporting* 21
2.5.1 *Broken Access Control* 21
2.5.2 *Cryptographic Failures* 22
2.5.3 *Injection* 22
2.5.4 *Insecure Design* 22
2.5.5 *Security Misconfiguration* 22
2.5.6 *Vulnerable and Outdated Components* 22
2.5.7 *Identification and Authentication Failures* 22
2.5.8 *Software and Data Integrity Failures* 23
2.5.9 *Security Logging and Monitoring Failures* 23
2.5.10 *Server-Side Request Forgorey (SSRF)* 23
3.2.1 Perangkat Lunak (*Software*) 28
3.2.2 Perangkat Keras (*Hardware*) 29
4.2.1 Whatweb 35
4.2.2 Nmap 36
4.2.3 Subfinder 37
4.4.1 Xray *Scanner* 42
4.5.1 Eksploitasi *Sql Injection* pada *Subdomain* https://web.mesujikab.go.id/ Parameter id 48
4.5.2 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter bentuk_peraturan 49
4.5.3 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter status 50
4.5.4 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter jenis_peraturan 51
4.5.5 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter judul 53
4.5.6 Eksploitasi *Sql injection* pada *subdomain* https://jdih.mesujikab.go.id Parameter nomor_peraturan 54
4.6.1 *Post-Expoiation* Pada *Subdomain* https://web.mesujikab.go.id/ 55
4.6.2 *Post-Exploitation* Pada *Subdomain* https://jdih.mesujikab.go.id/ Parameter bentuk_peraturan 61

DAFTAR TABEL

Tabel 3.1 Waktu Penelitian 27
Tabel 3.2 Perangkat Lunak..... 28
Tabel 3.3 Perangkat Keras 29
Tabel 4.1 Hasil Pengujian *Tools* Whatweb https://web.mesujikab.go.id/..... 35
Tabel 4.2 Hasil Pengujian *Tools* Nmap https://web.mesujikab.go.id/ 37
Tabel 4.3 Hasil Pengujian *Filtering* Subdomain 200 *status code* 39
Tabel 4.4 Hasil Pengujian *Tools* Xray *Vulnerability Scanner* 43
Tabel 4.5 Hasil Eksploitasi *Sql Injection* Pada Parameter id 57
Tabel 4.6 Hasil Eksploitasi *Sql Injection* Pada Parameter bentuk_peraturan ... 62
Tabel 4.7 Hasil Eksploitasi *Sql Injection* Pada Parameter status 65
Tabel 4.8 Hasil Eksploitasi *Sql Injection* Pada Parameter jenis_peraturan..... 67
Tabel 4.9 Hasil Eksploitasi *Sql Injection* Pada Parameter judul 70
Tabel 4.10 Hasil Eksploitasi *Sql Injection* Pada Parameter nomor_peraturan.. 72
Tabel 4.11 Laporan Hasil Eksploitasi 75

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan digital seperti *website* berkembang seiring berjalannya tahun. *Website* menjadi sumber informasi yang besar dan penggunaannya sudah banyak diterapkan di berbagai bidang[1]. Keamanan merupakan salah aspek yang penting dalam perancangan sebuah aplikasi *website*. Namun, masih banyak pengembang *website* yang kurang peduli dalam meningkatkan keamanan aplikasi *website*, karena mungkin suatu website yang telah dibangun akan menjadi sebuah target kejahatan siber oleh peretas[2]. Aplikasi *website* berperan penting namun rentang terhadap serangan siber seperti Injeksi *SQL* dan *Cross-Site Scripting (XSS)*[3]. Serangan-serangan ini bisa merusak keamanan data dan privasi pengguna. Injeksi *SQL* melibatkan penyisipan *syntax SQL* berbahaya pada halaman aplikasi *website*[4]. Kerentanan *Cross-Site Scripting (XSS)* merupakan salah satu kerentanan paling sering ditemukan pada *website*[5]. Serangan *Cross-Site Scripting (XSS)* terjadi ketika peretas memasukkan kode *JavaScript* melalui *input* sisi klien. Serangan ini bertujuan untuk mendapatkan *cookie* dan token. *Cross-Site Scripting (XSS)* terjadi karena kerentanan keamanan dalam *HTML, flash, JavaScript, AJAX*[6].

Penetration testing adalah subkategori dari *ethical hacking* yaitu sebuah metode dan prosedur yang bertujuan untuk menguji dan melindungi keamanan informasi. Penetration testing merupakan aktivitas mengevaluasi sistem keamanan yang sudah dibuat dengan cara melakukan simulasi serangan menggunakan metode yang biasa digunakan oleh peretas. Kegiatan ini perlu mendapat persetujuan legal dari pemilik sistem tersebut. Seperti halnya sekarang sedang terjadi pembobolan maupun hacking pada perusahaan maupun website tertentu yang mengakibatkan kerugian pada pihak yang bersangkutan. Data tersebut dijual dan disalahgunakan oleh pihak tidak berwajib dan diperjualbelikan untuk kepentingan tersendiri[7].

Diskominfo Kabupaten Mesuji merupakan unit pelaksana pemerintahan di bidang komunikasi dan informatika dan memiliki tugas pokok yang mencakup pengelolaan informasi publik, pengembanan sistem pemerintahan berbasis elektronik (SPBE) untuk pelayangan yang lebih transparan dan efisien serta pengamanan informasi yang krusial untuk menjaga integritas data. Kemajuan teknologi bisa menjadi salah satu ancaman bagi sebuah keamanan sistem dan menjadikan Diskominfo Kabupaten Mesuji sebagai instansi pengamanan informasi untuk melindungi data dan sistem dari risiko kebocoran data akibat serangan siber atau upaya peretasan. Diskominfo Kabupaten Mesuji juga dituntut untuk memperkuat keamanan sistem, menerapkan protokol keamanan yang ketat, serta melakukan mitigasi risiko agar tidak adanya penyalahgunaan informasi sensitif ataupun data pribadi masyarakat jatuh ke tangan yang salah akibat kegiatan peretasan atau kejahatan siber. Oleh sebab itu Diskominfo Kabupaten Mesuji juga menjadi instansi yang bertanggung jawab terhadap berbagai risiko keamanan siber yang terus berkembang, guna memastikan seluruh aktivitas pemerintahan berjalan, terintegrasi dan terlindungi.

1.2 Rumusan Masalah

Adapun rumusan masalah yang dibahas pada penelitian ini, yaitu :

1. Bagaimana proses mengidentifikasi kerentanan pada *subdomain website* dikelola Diskominfo Kabupaten Mesuji?
2. Bagaimana proses membuktikan kerentanan yang berhasil diidentifikasi pada *subdomain website* dikelola Diskominfo Kabupaten Mesuji?
3. Apa dampak yang disebabkan oleh kerentanan yang terdapat pada *subdomain website*? Apakah dapat menyebabkan kebocoran data?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Menemukan celah kerentanan sistem informasi *website* yang dikelola Diskominfo Kabupaten Mesuji.
2. Melakukan uji penetrasi keamanan sistem informasi *website* yang dikelola Diskominfo Kabupaten Mesuji.

3. Mengetahui dampak yang disebabkan dari kerentanan yang berhasil di-identifikasi pada *subdomain* dikelola Diskominfo Kabupaten Mesuji.

1.4 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah sebagai berikut :

1. Pengujian dilakukan untuk menemukan kerentanan dengan cara mengumpulkan seluruh informasi pada *domain* dan *subdomain* yang dikelola Diskominfo Kabupaten Mesuji.
2. Pengujian dilakukan hanya sebatas membuktikan kerentanan dan tidak membahayakan sistem dan tidak mengambil data apapun dari sebuah kerentanan.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Guna mengetahui kerentanan *domain* dan *subdomain website*.
2. Guna mengetahui dampak kerentanan pada *domain* dan *subdomain website.*
3. Memberikan rekomendasi dan saran untuk menindak lanjuti temuan kerentanan.

1.6 Sistematika Penulisan

Sistematika penulisan akhir bertujuan guna memberikan gambaran secara sederhana terkait pembahasan yang ada dalam tugas akhir skiripsi serta untuk memudahkan dalam memahami isi yang disajikan dalam skripsi ini. Adapun sistematika yang digunakan oleh penulisan adalah sebagai berikut :

BAB I : PENDAHULUAN

BAB I merupakan pendahuluan yang berisikan tentang latar belakang, tujuan penelitian, rumusan masalah, batasan masalah, manfaat penelitian, sistematika penulisan.

BAB II : LANDASAN TEORI

BAB II berisi definisi dan pembahasan mengenai berbagai istilah yang relevan dalam pengerjaan skripsi. Definisi ini diambil dari berbagai sumber, seperti buku, jurnal, dan lainnya.

BAB III : METODOLOGI PENELITIAN

BAB III berisi tempat dan waktu penelitian, jadwal penelitian, perangkat lunak dan perangkat keras yang digunakan, dan objek penelitian.

BAB IV : HASIL DAN PEMBAHASAN

BAB IV menyajikan hasil dari penelitian yang telah dilakukan serta pengolahan data dari hasil penelitian.

BAB V : KESIMPULAN DAN SARAN

BAB V merupakan bagian yang memberikan kesimpulan dan saran berdasarkan penelitian.

DAFTAR PUSTAKA

LAMPIRAN

II. LANDASAN TEORI

2.1 Penelitian Terdahulu

2.1.1 Analisis Keamanan *Website* Pemerintah Desa Curug Menggunakan *(OWASP)*[8]

Keamanan siber telah menjadi isu krusial di era digital saat ini, terutama bagi situs-situs pemerintah yang sering menjadi target serangan. Menurut Badan Siber dan Sandi Negara (BSSN), situs pemerintah rentan diretas. Tujuan penelitian ini bertujuan untuk menganalisis keamanan website Pemerintah Desa Curug menggunakan Open Web Application Security Project (OWASP). Analisis dilakukan terhadap sepuluh kategori utama kerentanan keamanan aplikasi web yang terdaftar dalam OWASP Top 10 2021, termasuk Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, serta Server-side Request Forgery. Hasil dari pengujian yang dilakukan yaitu 4 dari 8 kerentanan tersebut termasuk ke dalam daftar OWASP Top 10 tahun 2021 yaitu pada kerentanan Injection dan Security Misconfiguration. Rekomendasi perbaikan diberikan berdasarkan temuan-temuan tersebut, yang diharapkan dapat membantu Pemerintah Desa Curug dalam memperkuat keamanan siber mereka[9].

2.1.2 Vulnerability Assessment untuk Analisis Tingkat Keamanan pada Sistem Informasi Repositori Karya Ilmiah Politeknik XYZ[10]

Penelitian ini berfokus pada penilaian kerentanan Informasi Repositori untuk meningkatkan keamanannya Metodologi yang digunakan termasuk mendefinisikan ruang lingkup mengumpulkan informasi publik seperti FQDN nama host dan detail IP serta memindai kerentanan menggunakan alat OWASP ZAP Pemindaian

tersebut mengidentifikasi 22 peringatan keamanan termasuk 1 peringatan berisiko tinggi yang membutuhkan perhatian segera 7 peringatan berisiko sedang 9 peringatan berisiko rendah dan 5 peringatan informasi dengan tingkat kepercayaan yang berbeda beda pada temuannya Penelitian ini memberikan dokumentasi kerentanan dan rekomendasi spesifik untuk perbaikan yang bertujuan untuk meningkatkan keamanan sistem repositori di Politeknik XYZ[10].

2.1.3 Analisis Keamanan Website E-Learning SMKN 1 Cibatu [4]

Gambar 2.1. referensi metode ptes

(Sumber Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard)

Penelitian ini menganalisis keamanan website e-learning SMKN 1 Cibatu menggunakan metode Penetration Testing Execution Standard (PTES), yang terdiri dari tujuh tahapan: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Pengujian menemukan beberapa celah keamanan, termasuk Web Server Transmits Cleartext Credentials, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF). Eksploitasi dilakukan menggunakan berbagai tools seperti Wireshark, OWASP ZAP, dan Nessus. Hasil pengujian menunjukkan bahwa metode PTES dapat membantu meningkatkan keamanan sistem informasi sekolah dengan memberikan rekomendasi perbaikan, seperti penerapan HTTPS, validasi input

untuk mencegah XSS, dan mekanisme anti-CSRF untuk mengurangi risiko serangan[4].

2.1.4 Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security[11]

Gambar 2.2 referensi metode ptes
(sumber Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security)

Penelitian ini menggarisbawahi peran penting audit keamanan web dan pengujian penetrasi dalam meningkatkan keamanan aplikasi web di tengah meningkatnya ancaman dunia maya Fokusnya adalah pada penggunaan alat seperti NMAP dan Burp Suite untuk mengidentifikasi kerentanan umum seperti SQL Injection dan Cross Site Scripting Temuan tersebut mengungkapkan bahwa metode ini efektif dalam menemukan dan mengatasi masalah keamanan dengan laporan penilaian yang memberikan panduan berharga bagi pengembang untuk memperbaiki

kerentanan Namun kelemahan yang teridentifikasi termasuk ketergantungan pada alat yang mungkin tidak mendeteksi semua jenis kerentanan dan keahlian teknis yang signifikan serta waktu yang dibutuhkan untuk pemindaian dan eksploitasi manual Penelitian ini menyarankan untuk meningkatkan algoritma dan teknik pemindaian serta menerapkan pemantauan berkelanjutan untuk mengidentifikasi kerentanan baru Dengan memajukan metode penilaian kerentanan otomatis dan mempertahankan praktik keamanan yang waspada organisasi dapat melindungi aplikasi web mereka dengan lebih baik[11].

2.1.5 *identify Vulnerabilities on the Ministry of Health's* Ayo Sehat *Website Through Penetration Testing*[12]

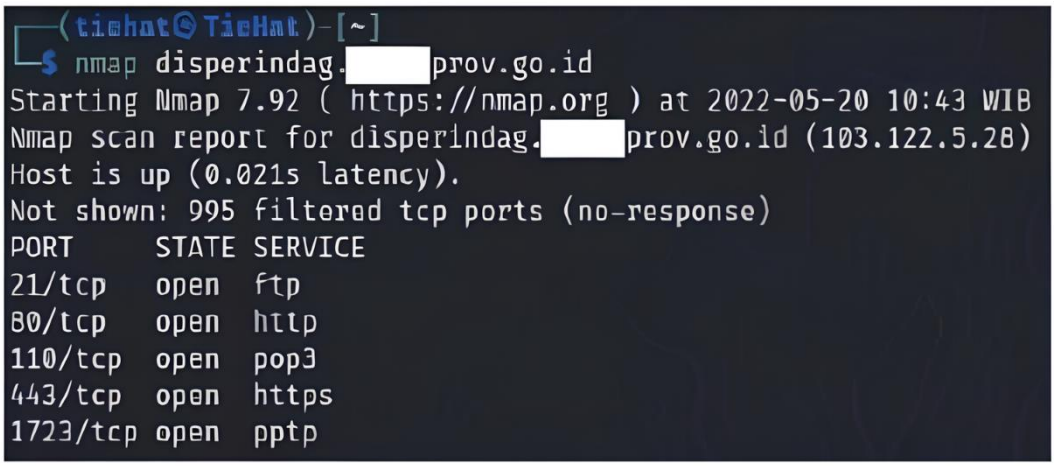
Penelitian ini mengevaluasi keamanan situs web Ayo Hidup Sehat Kementerian Kesehatan dengan fokus pada kerentanan seperti SQL Injection dan XSS Memanfaatkan alat seperti Nmap dan Subgraph Vega serta mengikuti metodologi ISSAF penelitian ini mengidentifikasi dan mengkategorikan kerentanan kedalam tingkat risiko tinggi sedang dan rendah Temuan utama termasuk beberapa kerentanan kritis terutama nomor jaminan sosial yang terekspos yang menimbulkan ancaman signifikan terhadap privasi pengguna Hasil penelitian menekankan perlunya mengatasi kerentanan berisiko tinggi ini untuk meningkatkan keamanan situs web dan melindungi informasi kesehatan yang sensitif memastikan kepercayaan pengguna dan integritas data[12].

2.1.6 Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organization[13]

Penelitian ini menunjukkan bahwa alat pengujian penetrasi otomatis efektif dan hemat biaya untuk organisasi kecil yang ingin meningkatkan keamanan siber mereka. Penelitian ini mengungkapkan bahwa alat ini, seperti OWASP ZAP, dapat secara efektif mengidentifikasi kerentanan dan menilai keamanan tanpa biaya tinggi yang terkait dengan mempekerjakan ahli eksternal. Pengujian menemukan beberapa port terbuka dan potensi kerentanan dalam infrastruktur jaringan dan aplikasi web, yang mengindikasikan area yang rentan dieksploitasi oleh penyerang. Meskipun organisasi kecil menyadari pentingnya keamanan siber, banyak yang

tidak memiliki sumber daya khusus untuk pengujian ekstensif dan lebih memilih solusi internal karena masalah biaya. Penelitian ini juga menyoroti variabilitas di antara alat, dengan beberapa alat menawarkan evaluasi risiko yang lebih komprehensif daripada yang lain. Secara keseluruhan, penelitian ini menegaskan bahwa pengujian penetrasi otomatis memberikan pendekatan praktis bagi bisnis kecil untuk meningkatkan postur keamanan mereka, sekaligus menyarankan perlunya eksplorasi lebih lanjut tentang kemampuan dan keterbatasan alat ini[13].

2.1.7 Security Vulnerability Analysis using (PTES): Case Study of Government's Website[14]



Gambar 2.3 referensi nmap

(Sumber *Security Vulnerability Analysis using Penetration TestingExecution Standard (PTES): Case Study of Government's Website*)

Jurnal ini menyajikan analisis komprehensif terhadap kerentanan keamanan pada situs web pemerintah menggunakan standar Penetration Testing Execution Standard (PTES). Penelitian ini mengidentifikasi berbagai celah keamanan, termasuk kerentanan pada sisi klien dan server, seperti SQL Injection, Cross-Site Scripting (XSS), dan miskonfigurasi keamanan. Dengan mengikuti tahapan PTES yang terstruktur, mulai dari pra-engagement hingga pelaporan pasca-pengujian, studi kasus ini menunjukkan bagaimana pengujian penetrasi dapat secara efektif mengungkap kelemahan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Temuan ini menggarisbawahi urgensi bagi instansi pemerintah untuk secara rutin melakukan pengujian keamanan guna menjaga integritas dan ketersediaan layanan digital mereka[14].

2.1.8 Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method[15]

Gambar 2.4 referensi whatweb

(Sumber *Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method*)

Jurnal ini bertujuan untuk menganalisis tingkat kerentanan pada sistem informasi akademik yang dikembangkan oleh Perusahaan XYZ, yang digunakan oleh 36 universitas negeri dan swasta. Penelitian ini menggunakan pendekatan deduktif untuk mengeksplorasi kerentanan berdasarkan insiden keamanan sistem di universitas, menggabungkan dua metode pengujian: Penetration Testing Execution Standard (PTES) dan Open Web Application Security Project (OWASP). Pengujian penetrasi mengikuti tujuh langkah PTES, sementara fokus ancaman diselaraskan dengan OWASP Top 10 tahun 2021. Hasil penelitian mengungkapkan delapan masalah keamanan kritis yang diukur menggunakan Common Vulnerability Scoring System (CVSS), termasuk dua kerentanan tingkat tinggi, lima tingkat menengah, dan satu tingkat rendah. Tiga kerentanan utama yang ditemukan adalah SQL Injection, kontrol akses yang rusak, dan enkripsi yang lemah[15].

2.1.9 Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes[16]

Pentingnya keamanan *website* sistem informasi Universitas Bina Darma semakin mendesak mengingat lonjakan pembelajaran daring berbasis web selama pandemi COVID-19. Penelitian ini secara spesifik bertujuan untuk menerapkan pengujian penetrasi pada situs elearning2.binadarma.ac.id menggunakan pendekatan Black Box yang dipandu oleh standar PTES (Penetration Testing Execution Standard). Melalui metode PTES yang mencakup tahapan pengumpulan informasi hingga pelaporan, ditemukan bahwa situs tersebut memiliki celah Cross-Site Scripting (XSS) yang berpotensi berbahaya jika tidak segera ditangani. Meskipun hasil keseluruhan menunjukkan *website* relatif aman, adanya kerentanan ini mengindikasikan bahwa situs masih dapat disusupi atau dimanipulasi oleh pihak tak bertanggung jawab. Oleh karena itu, rekomendasi kunci dari studi ini adalah perlunya pengecekan kerentanan secara rutin dan pengembangan implementasi PTES yang lebih mendalam pada elearning2.binadarma.ac.id guna memonitor dan mencegah serangan siber di masa mendatang[16].

2.1.10 Security Testing With (Ptes) Methods To Find Misconfigurations Vulnerabilities In Network Devices[17]

Studi ini menelisik secara mendalam keamanan jaringan Wi-Fi di lingkungan Universitas Pendidikan Ganesha, memanfaatkan kerangka kerja Penetration Testing Execution Standard (PTES). Tujuannya jelas: mengungkap serta menganalisis berbagai kerentanan yang timbul akibat miskonfigurasi dalam infrastruktur nirkabel kampus. Proses pengujian dilaksanakan melalui tahapan PTES yang komprehensif, mencakup interaksi pra-keterlibatan, pengumpulan intelijen, pemodelan ancaman, analisis kerentanan, eksploitasi, pasca-eksploitasi, dan pelaporan hasil. Temuan awal sudah menunjukkan adanya celah-celah krusial terkait dengan konfigurasi yang kurang tepat, misalnya penggunaan protokol yang rentan atau pengaturan yang tidak optimal. Analisis lebih lanjut menegaskan bahwa celah-celah ini berpotensi besar untuk dimanfaatkan oleh pihak tak bertanggung jawab, membuka pintu bagi pencurian data sensitif atau gangguan layanan. Oleh karena itu, riset ini tidak hanya mengidentifikasi masalah, tetapi juga menyertakan

rekomendasi konkret untuk perbaikan konfigurasi dan strategi mitigasi, guna memperkuat benteng keamanan Wi-Fi universitas. Harapannya, hasil ini dapat menjadi fondasi kokoh dalam merumuskan kebijakan keamanan yang lebih efektif dan melindungi infrastruktur jaringan di ranah akademis dengan lebih baik. Sebagai tindak lanjut, laporan ini memberikan serangkaian rekomendasi. Untuk mengantisipasi kerentanan yang telah teridentifikasi, implementasi langkah-langkah keamanan yang tepat harus segera dilakukan. Ini mencakup penggantian kata sandi *default*, pembaruan sistem keamanan secara berkala, penguatan enkripsi data, pemantauan aktif terhadap aktivitas mencurigakan, serta pengetatan kebijakan akses. Audit keamanan rutin juga menjadi keharusan demi memastikan sistem senantiasa terlindungi dari ancaman yang terus berkembang. Pada akhirnya, kerentanan yang ditemukan pada alamat-alamat IP tersebut harus diangkat sebagai prioritas tertinggi demi menjaga keamanan sistem dan data yang tersimpan di dalamnya. Dengan langkah-langkah yang sigap dan tepat, risiko dapat diminimalisir, sekaligus menjamin kelangsungan operasional dan menjaga kepercayaan *stakeholder* terhadap keamanan sistem informasi[17].

2.1.11 Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode (Ptes)[18]

Gambar 2.5 referensi sqlmap

(Sumber analisis pengujian keamanan website pengelolaan internet desa kragan menggunakan metode penetration testing execution standard (ptes))

Peningkatan drastis pengguna internet di era digital ini telah membuka ranah kehidupan baru, yang sayangnya juga membawa serta beragam ancaman siber. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan tren mengkhawatirkan, dengan hampir satu miliar serangan siber tercatat sepanjang tahun 2022—sebuah indikasi nyata bahwa tingkat keamanan siber di Indonesia masih memerlukan perhatian serius. Untuk mengukur dan memperbaiki kualitas proteksi pada situs pengelolaan internet Desa Kragan, tim peneliti memutuskan untuk menerapkan metode *penetration testing* berdasarkan standar PTES (Penetration Testing Execution Standard). Pengujian ini mengungkap empat belas celah keamanan yang bervariasi tingkat risikonya, dari rendah hingga tinggi. Beberapa di antaranya terbukti dapat dieksploitasi, termasuk Cloud Metadata Potentially Exposed, ketiadaan Anti-CSRF Tokens, Missing Anti-clickjacking Header, dan adanya *library* JavaScript yang rentan. Menariknya, meskipun upaya injeksi SQL tidak berhasil karena situs telah menggunakan SSL dan WAF yang cukup tangguh, temuan ini menegaskan bahwa satu lapisan keamanan saja tidaklah cukup. Banyak celah lain yang berhasil dimanfaatkan, menggarisbawahi bahwa ancaman dapat muncul dari berbagai sudut. Hasil uji penetrasi ini diharapkan menjadi landasan vital bagi rekomendasi perbaikan, memastikan situs Desa Kragan dapat beroperasi

dengan integritas data yang lebih baik di tengah lanskap ancaman siber yang terus berevolusi[18].

2.1.12 Information System Security Analysis to DetermineServer Security Vulnerability with (PTES) [19]

Penelitian ini menggarisbawahi pentingnya keamanan server sebagai bagian tak terpisahkan dari strategi perlindungan data dan pencegahan pencurian informasi. Terdapat kecenderungan bagi beberapa institusi, termasuk universitas, untuk merasa aman hanya dengan mengandalkan perangkat lunak dasar seperti antivirus atau firewall, mengabaikan perlunya pengamanan informasi yang lebih ketat.

Untuk mengatasi celah ini, studi pada server data karyawan di Universitas VWX ini menggunakan metode Penetration Testing Execution Standard (PTES). Melalui pengujian penetrasi, ditemukan sejumlah kerentanan signifikan, seperti serangan Cross-Site Tracing (CST), Sensitive Data Exposure, Password Guessing, DDoS Attack, dan aktivitas Sniffing yang membuka celah akses ke sistem server.

Berdasarkan hasil pengujian, terungkap bahwa kerentanan pada port 80 dan 53 memiliki potensi serangan tertinggi. Kerentanan Password Guessing dinilai memiliki tingkat kritis, sedangkan Cross-Site Tracing, Sensitive Data Exposure, dan DDoS Attack berada pada tingkat kerentanan sedang. Temuan ini menegaskan bahwa server Universitas VWX belum sepenuhnya memenuhi dua pilar utama keamanan informasi, yaitu Kerahasiaan (Confidentiality) dan Integritas (Integrity), yang menunjukkan perlunya perbaikan segera untuk memperkuat pertahanan siber mereka[19].

2.1.13 Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang[20]

Dalam konteks penggunaan teknologi yang semakin meluas, penelitian ini menyoroti permasalahan keamanan pada jaringan nirkabel di tempat umum seperti kafe. Dengan menggunakan kerangka kerja Penetration Testing Execution Standard (PTES), riset ini melakukan evaluasi keamanan secara menyeluruh melalui metode Vulnerability Assessment and Penetration Testing (VAPT).

Pengujian penetrasi dilakukan dengan mensimulasikan tiga jenis serangan utama: serangan akses tidak sah, serangan DoS (Denial of Service), dan *packet sniffing*. Hasilnya secara konsisten menunjukkan bahwa semua serangan berhasil menembus keamanan jaringan, menegaskan adanya celah yang dapat dieksploitasi.

Kesimpulan dari studi ini adalah bahwa jaringan Wi-Fi di kafe masih memiliki kerentanan signifikan. Hal ini tidak hanya membahayakan data pengguna yang rentan dicuri atau dimanipulasi, tetapi juga menunjukkan kurangnya kesadaran pemilik kafe akan pentingnya konfigurasi keamanan *access point* yang lebih ketat. Oleh karena itu, penelitian ini menekankan perlunya peningkatan keamanan Wi-Fi di kafe dan perlunya pengguna untuk lebih berhati-hati saat mengakses informasi sensitif[20].

2.2 Website

Website adalah kumpulan dari halaman web yang sudah dipublikasi di jaringan internet dan memiliki domain/URL (Uniform Resource Locator) yang dapat diakses semua pengguna internet dengan cara megetikan alamatnya. Hal ini dimungkinkan dengan adanya teknologi *World Wide Web* (WWW). halaman *website* biasanya berupa dokumen yang ditulis dalam format *Hype Text Language* (HTML), yang bisa diakses melalui *HTTP, HTTPS* adalah suatu protokol yang menyampaikan berbagai informasi dari *server website* untuk ditampilkan kepada para *user* melalui web *browser*[2].

Website adalah layanan internet yang menghubungkan dokumen lokal maupun jarak jauh. Tautan pada *website* memungkinkan pengguna untuk berpindah dari satu halaman ke halaman lain (*hypertext*), baik antar halaman yang disimpan di *server* pada aplikasi *browser*, seperti *Netscape Navigator* atau Internet *Explorer* yang digunakan untuk mengakses dan membaca halaman[21].

Website adalah kumpulan beberapa halaman web yang berisi teks, gambar, suara, dan jenis informasi lainnya. Ditampilkan sebagai *hypertext* dan dapat melalui perangkat lunak yang dikenal sebagai *browser*. Sebagian besar waktu, *HTML* digunakan untuk menulis informasi di halaman web. Grafik yang digunakan dalam bentuk format *JPG, GIF, PNG,* dan lainnya digunakan untuk menyajikan informasi

tambahan suara (WAV, AU, dan sebagainya), dan MIDI, *shockwave, Quicktime Movie,* 3D *World,* dan objek multimedia lainnya[22].

2.3 Keamanan Sistem Informasi

Keamanan Sistem Informasi adalah tentang mencegah penipuan atau paling tidak mendeteksi penipu dalam sistem berbasis informasi di mana informasi itu sendiri tidak memiliki bentuk fisik Keamanan Sistem Informasi berfokus pada perlindungan data dan informasi yang tidak memiliki nilai fisik namun secara strategis penting bagi organisasi Keamanan Sistem Informasi mencakup tiga dimensi utama yakni

- *Cognition* mengacu pada pengetahuan individu tentang keamanan sistem informasi.
- *Affection* berkaitan dengan sikap seseorang terhadap keamanan sistem informasi.
- *Behavior* berkaitan dengan tindakan yang dilakukan seseorang untuk mengamankan sistem informasi.

Dengan demikian, keamanan Sistem Informasi bertujuan untuk mengembangkan pengetahuan sikap dan perilaku yang tepat untuk melindungi data dan informasi penting. Di dalam keamanan sistem informasi terdapat aspek penting yaitu *CIA Confidentiality Integrity Availability* (CIA) adalah singkatan dari *Confidentiality Integrity* dan *Availability* yang merupakan bagian penting dari keamanan informasi dalam organisasi terutama untuk aplikasi web.

Gambar 2.6 Segitiga *CIA*

(Sumber https://www.nist.gov/image/cia-triad)

- *Confidentiality* Kerahasiaan berfokus pada menjaga kerahasiaan data dan mencegah akses yang tidak sah memastikan hanya pengguna yang berwenang yang dapat melihat informasi sensitif
- *Integrity* (Integritas) memastikan bahwa data tetap akurat dan dapat dipercaya, mencegah perubahan yang tidak sah dan menjaga konsistensi informasi Tujuannya yakni :
  1. Mencegah modifikasi yang tidak sah oleh pengguna.
  2. Mencegah akses yang tidak sah.
  3. Mempertahankan Konsistensi baik secara internal maupun eksternal.
- *Availability* Ketersediaan menjamin bahwa pengguna yang berwenang dapat mengakses data tanpa gangguan. Menggunakan cadangan dan alat keamanan untuk melindungi dari kehilangan data dan serangan *cyber*[3].

2.4 *Penetration Testing Execution Standard*

Gambar 2.7 *Penetration Testing Execution Standard*

(Sumber http://www.pentest-standard.org/index.php/Main_Page)

Penetration Testing Execution Standard (PTES) merupakan standar dalam mendokumentasikan proses pelaksanaan pengujian uji penetrasi. PTES menyediakan metodologi komprehensif yang mencakup aspek-aspek dalam uji penetrasi. PTES terdiri dari tujuh bagian utama yang mencakup seluruh proses uji penetrasi, PTES dengan versi 1.0 akan terus dikembangkan dan versi 2.0 yang akan datang menyediakan tingkatan intensitas yang lebih rinci untuk setiap elemen pengujian yang memungkinkan penyesuaian yang lebih baik dengan kebutuhan dan tingkat ancaman organisasi[4]. Terdapat tujuh tahapan dalam motede ini, yaitu sebagai berikut :

2.4.1 *Pre-Engagement*

Tahap ini merupakan langkah awal untuk melakukan uji penetrasi, aktivitas yang dilakukan pada tahap ini meliputi :

- Definisi Tujuan Klien

Tahap ini memahami dengan jelas tujuan klien melakukan uji penetrasi, dari mulai mengidentifikasi kerentanan.

- Ruang Lingkup Analisis

Untuk ruang lingkun pengujian, PTES memiliki beberapa lingkup yang dapat dilakukan pengujian sesuai dengan kebutuhan klien, diantaranya adalah :

a. *Network Penetration Test*
b. *Web Application Penetration Test*
c. *Wireless Network Penetration Test*
d. *Physical Penetration Test*
e. *Social Engineering*
f. *Questions for Business Unit managers*
g. *Questions for Systems Administrators*

- Aturan Keterlibatan (*Rules of Engangement*)

Pada tahap ini mendefinisikan metodologi yang akan digunakan, batasan pengujian, protokol komunikasi, waktu dan lokasi pengujian, penanganan bukti, izin pengujian dan pertimbangan hukum[23].

2.4.2 *Intelligence Gathering*

Tahap ini bertujuan untuk mengumpulkan informasi berharga mengenai lingkungan target, yang biasanya meliput langkah berikut :

- *Passive Data Collection*
- *Active Data Collection*
- *Open Source Intelligence*

2.4.3 *Threat Modelling*

Tahap ini berfokus pada identintifikasi potensi acaman. Pada tahap ini pemahanan tentang bagaimana pelaku kejahatan mungkin mencoba menyerang sistem atau aset berharga. Tahap ini memiliki tujuan untuk membuat skenario serangan dan hipotesis yang relevan[24].

2.4.4 *Vulnerability Analysis*

Tahap ini adalah proses menemukan celah keamanan dalam sistem dan proses target yang memungkinkan penyerang untuk menembus keamanan sistem. Celah keamanan sistem dapat ditemukan dalam penilaian aktif menggunakan *vulnerabilty scanner*[25].

2.4.5 *Exploitation*

Tahap ini bertujuan untuk menembus keamanan sistem target dengan memanfaatkan kerentanan yang telah diidentifikasi dan divalidasi melalui tahap *vulnerability Analysis* dengan *vulnerability scanner tools*[26].

2.4.6 *Post Exploitation*

Ketika mendapatkan akses atau mendapatkan informasi sensitif melalui tahap *exploitation*. Tahap ini mengidentifikasi hak akses atau informasi sensitif yang bertujuan untuk mengukur potensi pelangaran keamanan yang berhasil dan sebarapa jauh pelaku kejahatan dapat bergerak didalam sebuah sistem[27].

2.4.7 *Reporting*

Tahap terakhir adalah mendokumentasikan seluruh proses pengujian dalam format yang mudah dipahami oleh klien. Tahap ini harus mencakup temuan kerentanan, risiko yang terkait, dan rekomendasi untuk perbaikan[28].

2.5 *Top 10 Vulnerabilities*

Owasp top 10 merupakan dokumen standar yang diterbitkan oleh *Open Web Application Security Project* (OWASP) untuk menyoroti 10 kerentanan yang paling *critical* pada aplikasi *website.* Dokumen ini berfungsi untuk tolak ukur bagi pengembang dan profesional keamanan guna melakukan mitigasi pasca serangan. Dokumen ini secara rutin diperbarui dengan versi terkini 2021[29].

Terdapat tingkatan kerentanan atau *severity* yaitu *critical, high, medium, low*, dan *informational. Critical* merupakan kerentanan dengan dampak paling parah dikarenakan dapat menyebabkan akses penuh yang tidak sah ke sah atau data sensitif, pengambil alihan akun administrator atau seluruh sistem. *High* merupakan kerentanan yang memiliki potensi dampak serius dan dampak yang lebih terbatas karena dapat menyebabkan pencurian data sensitif, akses tidak sah atau data pengguna lain. *Medium* merupakan kerentanan yang dampaknya signifikan tetapi tidak terlalu merusak atau kerentanan serius tetapi sulit untuk dieksploitasi dan menyebabkan kebocoran data non-sensitif, gangguan fungsional aplikasi. *Low* kerentanan yang memiliki dampak yang sedikit pada sistem dan sulit dieksploitasi, kerentanan ini menyebabkan kebocoran data non-sensitif. *Informational* bukan termasuk kedalam kerentanan secara langsung, melainkan temuan yang menampilkan informasi yang dapat membantu pelaku kejahatan siber dalam serangan[29].

2.5.1 *Broken Access Control*

Kerentanan ini terjadi ketika adanya *miss-configuration control access*, yang diaman memungkinkan pengguna lain dapat mengakses data atau fungsi yang seharusnya tidak mereka miliki, sebagai contoh akses ke data pengguna lain, melakukan perubahan data orang lain, dan eskalasi akses[29].

2.5.2 *Cryptographic Failures*

Kerentanan ini berfokus pada gagalnya penggunaan *cryptograpy* yang benar, seperti enkripsi yang lemah atau bahkan tidak ada enskripsi yang dapat menyebabkan kebocoran data sensitif[29].

2.5.3 *Injection*

Kerenetanan ini meliputi berbagai jenis serangan injeksi seperti *SQL Injection*, *Command Injection,* dan *Cross-Site Scripting* (XSS). Serangan ini terjadi ketika tidak adanya validasi *input* pada perintah atau *query*, yang memungkinkan penyerang dapat menajalankan *script* berbahaya[29].

2.5.4 *Insecure Design*

Kerentanan ini terjadi ketika kurang atau tidak efektifnya kontrol keamanan yang dirancang sejak awal pengembangan perangkat lunak (*SDLC*). Kerentanan ini berarti keamanan dan perlindangan untuk menghadapi sebuah serangan siber tidak pernah atau tidak ada sejak perancangan aplikasi *website* yang menyebabkan kerentanan yang lebih mendalam dan struktural dan sulit untuk diperbaiki[29].

2.5.5 *Security Misconfiguration*

Kerentanan ini terjadi ketika pengaturan keamanan tidak dikonfigurasi dengan optimal atau ketika sebuah aplikasi diterapkan dengan pengaturan *default* yang belum tentu aman. Contohnya adalah fitur yang tidak diperlukan, tidak adanya *header* keamanan, dan akun *default* yang tidak diubah[29].

2.5.6 *Vulnerable and Outdated Components*

Kerentanan ini terjadi ketika perangkat lunak tidak dilakukan *update*, yang dimana pada versi yang usang terdapat kerentanan yang sudah diketahui oleh pelaku kejahatan siber melalui sebuah platform perangkat lunak tersebut mengapa dikeluarkan dengan versi terbaru[29].

2.5.7 *Identification and Authentication Failures*

Kerentanan ini ini berikaitan dengan autentikasi pengguna, dikarenakan penggunaan kata sandi yang lemah, proses pergantian kata sandi yang tidak aman, atau kurangnya *multi-factor authentication* (MFA), dimana pelaku kejahatan siber dapat melakukan *bruteforce* dan *credential stuffing* untuk melakukan *account take over* atau mengambil alih akun orang lain[29].

2.5.8 *Software and Data Integrity Failures*

Kerentanan ini terjadi ketika aplikasi atau sistem gagal perangkat lunak, pembaruan atau data yang diterima dan digunakan adalah asli, utuh dan belum dimanipulasi atau disispkan *virus*, *malware* dan sejenisnya, sehingga memungkinkan untuk menyisipkan kode berbahaya atau memodifikasi data tanpa terdeteksi[29].

2.5.9 *Security Logging and Monitoring Failures*

Kerentanan ini terjadi ketika sistem tidak mencatat *log* aktivitas penting secara menyeluruh, dan efektif untuk mendeteksi untuk merespon jika adanya pelaku kejahatan siber. Akibatnya pelaku kejahatan siber bisa tidak terdeteksi, dan dapat memperbesar dampak kerusakan bahkan memperlambat respons tims keamanan[29].

2.5.10 *Server-Side Request Forgorey (SSRF)*

SSRF merupakan kerentanan yang dimana pelaku kejahatan siber dapat memanipulasi server agar membuat *request HTTP* atau jaringan internal ataupun eksternal yang seharusnya tidak dapat diakses secara langsung oleh orang lain. Dengan kata lain pelaku kejahatan siber memanfaatkan server sebagai perantara untuk mengakses layanan atau data yang tidak bisa diakses oleh orang lain[29].

2.6 Parrot *Security* OS

Gambar 2.8 ParrotOS

(sumber https://parrotsec.org/blog/2025-01-31-parrot-6.3-release-notes)

Parrot *Security OS atau ParrotOS* merupakan distribusi *GNU/Linux Free* dan *Open Source* berbasis Debian Stable yang dirancang untuk memenuhi beragam kebutuhan *user*. Sistem operasi ini meminiliki 3 karakteristik *general purpose distribution*, *pentest distribution*, dan *secure distribution* yang dimana memungkinkan ParrotOS dapat berfungsi sebagai lingkungan kerja yang komprehensif bagi para profresional keamanan siber, peneliti, pengembang dan juga pengguna umum yang memprioritaskan privasi dan keamanan digital. ParrotOS dilengkapi dengan *tools open source* yang mencakup kebutuhan kemanan informasi, mulai dari pengujian pentrasi, *digital forensic*, analisis *malwar*. Selain fungsi keamanan ParrotOS tersedia untuk penggunaan sehari-hari dan *software development*. Fleksibelitas ini dapat dilihat melalui ketersediaan berbagai edisi yaitu termasuk Parrot *Security Edition,* Parrot *Home Edition*, Parrot *develop edition*[30].

2.7 Sqlmap

Sqlmap merupakan sebuah *tools open source* yang dirancang untuk melakukan uji penetrasi secara otomatis dalam mendeteksi dan eksploitasi celah keamanan *SQL Injection*. *Sqlmap* dapat melakukan ambil alih data dari sebuah database, dan akses ke sistem file dasar hingga eksekusi perintah pada sistem operasi melalui koneksi *out-of-band*[31].

2.8 Xray

Xray merupakan *tools* yang biasa digunakan untuk uji penetrasi dan dikembangkan oleh Chaitin. *Tools* ini dirancang dapat memindai terhadap kerentanan pada sebuah aplikasi *website* dan dapat menampilkan *proof-of-concept* (PoC) jika ditemukan kerentanan pada saat pemindaian selesai. Selain dapat melakukan *single single tools* ini juga dapat melakukan pemindaian secara menyeluruh, ketika melakukan pemindaian pada *domain* maka *subdomain* juga otomatis akan dilakukan pemindaian[32].

2.9 Subfinder

Subfinder merupakan *tool open-source* yang dikembangkan oleh ProjectDiscovery, dirancang untuk melalukan *enumeration subdomain* secara pasif. Subfinder dapat melakukan indentifikasi *subdomain* dari suatu target tanpa harus melakukan interkasi secara langsung dilakukan dengan memanfaatkan beragam sumber data publik *application programming interface* (API) pihak ketiga. Subfinder dapat melakukan verifikasi *subdomain* yang ditemukan dan mampu mengeliminasi *subdomain* yang sama. *Tool* ini menjadi fundamental dalam fase *reconnaissance* pada uji penetrasi, *bug bounty*, atau audit keamanan karena dapat memberikan cangkupan target yang lebih luas dari sebuah *domain* utama. (https://github.com/projectdiscovery/subfinder)

2.10 Whatweb

Whatweb merupakan *tool* yang dirancang untuk mengidentifikasi teknologi yang diguakan dalam sebuah *website*. Whatweb melakukan *request http* guna mengetahui *framework, content management system* (CMS), *library javascript,*

web server dan komponen lainnya yang membentuk sebuah *website*. Dalam uji penetrasi whatweb digunakan dalam *information gathering* atau *reconnaissance* awal untuk membantu dalam proses pengumpulan informasi dan menjadi fondasi dalam melakukan uji penetrasi. (https://github.com/rezad/whatweb)

2.11 Nmap

Nmap (*Network Mapper*) adalah *tool* yang digunakan untuk pemindai *port open-source powerful* dan sangat fleksibel. *Tool* dapat melakukan pemindaian *host* aktif, mengidentifikasi *open port*, dan mengetahui layanan apa yang berjalan dalam *port* tersebut. Nmap menjadi pondasi dalam aktivitas audit keamanan, menajemen inventaris jaringan, hingga *network penetration testing.* (https://nmap.org/)

2.12 Httpx

Httpx merupakan *tools* yang berfungsi untuk melakukan validasi dan indenfitikasi *website*. Httpx memeriksa setiap *host* untuk memastikan aktif dan merespon melalui protokol *http* atau *htpps*. (https://github.com/projectdiscovery/httpx)

III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Pelaksanaan

Penelitian tugas akhir ini dilaksanakan di instansi Diskominfo Kabupaten Meusji. Waktu penelitian dapat dilihat pada tabel 3.

Tabel 3.1 Waktu Penelitian

No.	Kegiatan	Bulan							
		Apr	Mei	Jun	Jul	Agu	Sep	Okt	Nov
1.	Studi Literatur								
2.	Perancangan Proposal								
3.	Seminar Proposal								
4.	Pengujian Sistem								
5.	Analisis Data								
6.	Penulisan Laporan Hasil								
7.	Seminar Hasil								
8.	Komprehensif								

3.2 Alat dan Bahan Penelitian

3.2.1 Perangkat Lunak (*Software*)

Adapun perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut :

Tabel 3.2 Perangkat Lunak

No	Perangkat Lunak
1.	Sistem Operasi Windows 11
2.	Sistem Operasi Parrot *Security* 6.3
3.	Oracle Virtual Box 7.0.22
4.	Peramban Microsoft Edge
5.	Microsoft Word 2021
6.	Sqlmap v1.8.12
7.	Xray v1.9.11 *community*
8.	Subfinder v2.7.1
9.	Whatweb v0.5.5
10.	Nmap

3.2.2 Perangkat Keras (*Hardware*)

Adapun perangkat keras yang digunakan dalam penelitian ini sebagai berikut :

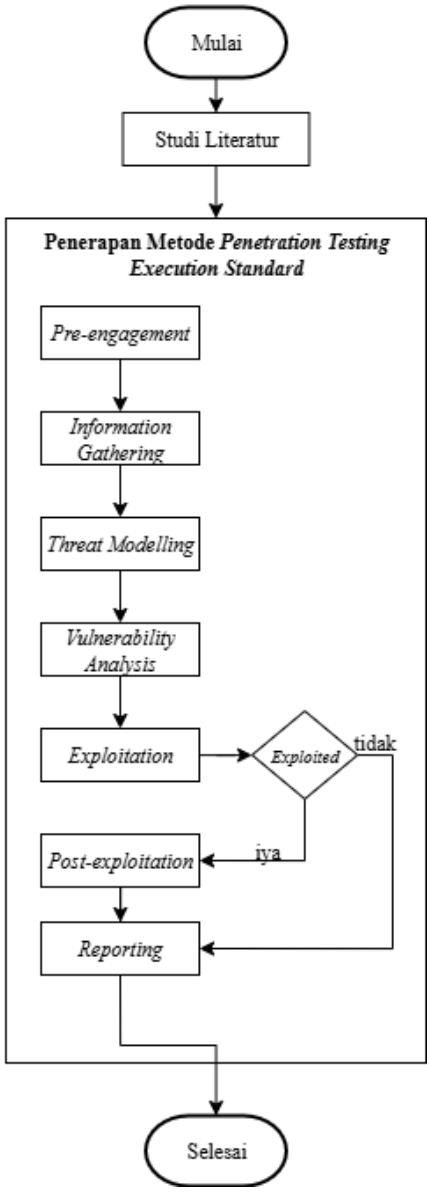
Tabel 3.3 Perangkat Keras

Perangkat Keras	
Jenis	Thinkpad X1 Yoga
CPU	Intel(R) Core(TM) i7-7600 CPU @ 2.80GHz (4 CPUs), ~2.9Ghz
RAM	16.0 GB
Storage	237 GB

3.2.3 Objek Peneliian

Objek pada penelitian ini berfokus pada *Domain* dan *Subdomain* pada *website* yang dikelola Dinas Komunkasi dan Informatika Kabupate Mesuji, yang memiliki kerentanan dan dapat berdampak kebocoran data.

3.3 Diagram Alir Penelitian



Gambar 3.1 Diagram Alir Penelitian [19]

Berdasarkan Gambar 2 Diagram alir penelitian diatas menunjukkan penelitian ini dimulai dengan melakukan studi literatur yang berkaitan dengan penelitian yang akan dilakukan. Lalu melakukan penerapan metode *Penetration Testing Execution Standard* (PTES), yang dimana tahap pertama pada metode ini adalah *pre-engagement*, apa tujuan dari uji penetrasi dan kemudian ruang lingkup dari uji penetrasi, yang dimana tujuannya adalah untuk mengetahui apakah terdapat

kerentanan pada *domain* dan *subdomain* aplikasi *website* yang dikelola Diskominfo Kabupate Mesuji. Kemudian tahap kedua dari metode ini adalah *intelligence gathering* yang dimana tahap ini mengumpulkan informasi mengenai target yang akan dilakukan uji penetrasi, yang meliputi informasi teknis berupa *IP address*, versi perangkat lunak, dan seluruh *subdomain website*. Pada tahap tersebut menggunakan *tools Whatweb* untuk mengetahui *IP address* pada *domain* dan mengetahui versi dari perangkat lunak yang digunakan, kemudian menggunakan *tools* Katana untuk melakukan *crawling* seluruh *sudomain* pada aplikasi *website* Diskominfo Kabupaten Mesuji.

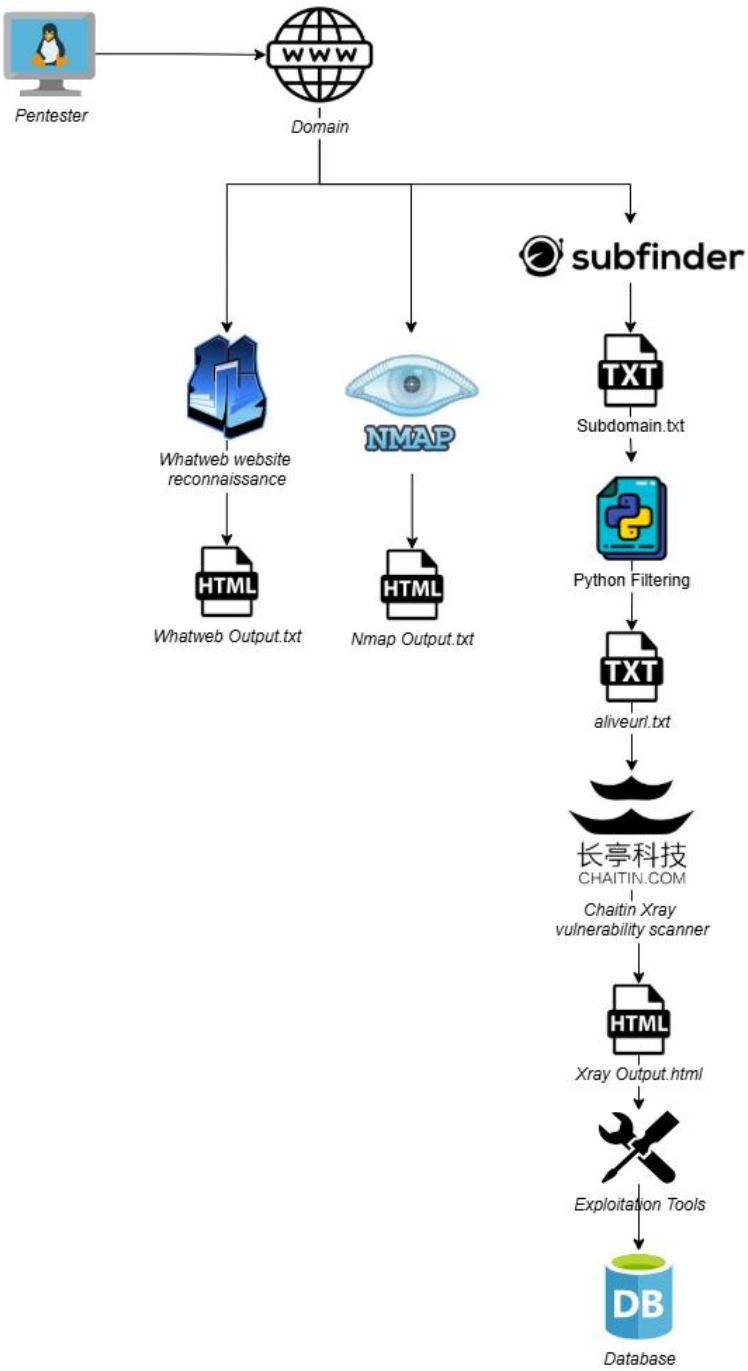
Selanjutnya adalah tahap *Threat Modelling*, pada tahap ini fokus untuk mengidentifikasi potensi ancaman yang akan dilakukan oleh pelaku kejahatan siber. Selanjutnya adalah tahap ke-4 *Vulnerability Analysis*, pada tahap ini melakukan indentifikasi kerentanan yang ada pada aplikasi *website* menggunakan *automatic scanning tools* yaitu *Xray*, *tools* ini dapat melalukan *scanning* secara menyeluruh mulai dari *domain* hingga *subdomain* target dan kemudian jika terdapat kerentan maka *output* disimpan dalam *file html*.

Tahap selanjutnya adalah *Exploitation*, pada tahap ini uji penetrasi berfokus pada memanfaatkan kerentanan yang teridentifikasi pada tahap sebelumnya, *exploitasi* dilakukan secara hati-hati sesuai dengan batasan masalah agar menghinadri kerusakan atau mengganggu kinerja dari aplikasi *website*. *Tools* yang dapat digunakan *burpsuite* untuk memanipulasi *request user* untuk melihat *POST* atau *GET*, dan dapat menggunakan *automatic exploitation tools sqlmap* ketika terdapat kerentanan *SQL Injection*.

Selanjutnya adalah tahap *Post-Exploitation*, pada tahap ini setelah berhasil melakukan eksploitasi melihat dampak apa yang dihasilkan dari eksploitasi. Pada tahap ini melihat apakah ada kebocoran data dari kerentanan yang telah diindentifikasi dan dieksploitasi menggunakan *tools* pada tahap sebelumnya. Kemudian tahap terakhir adalah *reporting*, tahap ini berfokus pada memberikan rekomendasi perbaikan dan dokumentasi secara menyeluruh terkait uji penetrasi yang dilakukan. Dokumentasi dapat berupa video *Proof-of-Concpet* atau dapat berupa dokumen tulisan agar pihak keamanan dapat memahami bagaimana cara

pelaku kejahat untuk melakukan aksinya dan melakukan perbaikan melalui rekomendasi.

3.4 Diagram Arsitektur



Gambar 3.2 Arsitektur diagram

Berdasarkan gambar arsitektur diagram, diagram ini untuk menjelaskan alur kerja dari uji penetrasi. Uji penetrasi ini dilakukan dengan pendekatan *black box,* dimana tidak memiliki informasi awal apapun terkait *website*. Semua proses dimulai layaknya seorang pelaku kejahat siber yang tidak memiliki akses maupun data kredensial apapun. Menggunakan subfinder *crawler tool* untuk mengetahui *subdomain* apa saja yang terhubung dengan *domain*. Kemudian *output* dari subfinder mencakup semua *status code* 100 sampai 500. Python *Filtering* digunakan untuk mengelompokkan *subdomain* berdasarkan *status codenya* mulai dari 100 sampai 500 dan juga mengelompokkan *subdomain* yang tidak memiliki *status code*. Penggunaan *tools* whatweb untuk mengetahui versi dari perangkat lunak yang digunakan sebuah *website,* ketika terdapat perangkat lunak yang tidak terbaru untuk menghindari kerentana maka dapat dimasukkan kedalam rekomendasi perbaikan untuk menghindari kerentanan *Vulnerable and Outdated Components*. Kemudian penggunaan *tools* Nmap untuk mengetahui *port* mana saja yang terbuka dan *output*-nya dijadikan sebuah rekomendasi, dikarenakan fokus uji penetrasi dari penelitian ini adalah *website* maka ketika terdapat *port* yang dapat dieksploitasi hanya akan menjadi catatan rekomendasi perbaikan kepada divisi keamanan. Kemudian menggunakan *tools* Chaitin Xray untuk melakukan *vulnerability analysis*, *tools* ini dapat mengindentifikasi kerentanan yang dapat menyebabkan kebocoran data seperti *sql injection, cross site scripting, remote command execution*. *Output* yang diindentifikasi *tools* Chaitin Xray selanjutnya di-eksploitasi menggunakan *exploitation tools* untuk melihat *database* yang terdapat di sebuah *web.*

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Dalam pengumpulan informasi *subdomain*, Diskominfo Kabupaten Mesuji memiliki 845 *subdomain* yang terdaftar, dengan 14 *subdomain* yang memiliki *status code* 200, kemudian 103 *subdomain* yang memiliki *status code* 300, lalu 30 *subdomain* yang memiliki *status code* 400, 2 *subdomain* yang memiliki *status code* 500, dan 696 *subdomain* yang tidak memiliki *status code*.

2. Ditemukan kerentanan *sql injection* pada *subdomain* https://web.mesujikab.go.id/ dan https://jdih.mesujikab.go.id/ pada Diskominfo Kabupaten Mesuji dilakukan dengan Xray *vulnerability scanner* dengan memanfaatkan *subdomain* yang memiliki *status code* 200.

3. Dalam proses membuktikan kerentanan *sql injection* yang berhasil diidentifikasi *tools* xray *scanner* dilakukan eksploitasi menggunakan *tools* sqlmap dengan *payload* dan parameter rentan pada *subdomain*. *Payload* dan *parameter* spefisik yang terdapat pada *output* xray *scanner* disimpan dalam 6 *file* berformat teks sesuai dengan kerentanan yang berhasil diidentifikasi. Kemudian *file* di proses menggunakan *tools* sqlmap guna membuktikan kerentanan yang berhasil diidentifikasi bersifat *true* ada benar tidak ada kesalahan dalam proses *scanning*. Kerentanan yang diidentifikasi seluruhnya bersifat *true* atau benar adanya dan tidak ada kesalahan dalam proses *scanning*.

4. Kerentanan *sql injection* pada *subdomain* https://web.mesujikab.go.id/ menyebabkan kebocoran data berupa 4 NIK dan *password* yang berbentuk *hash bcrypt*. Kemudian kerentanan *sql injection* pada *subdomain*

https://jdih.mesujikab.go.id/ menyebabkan kebocoran data berupa stuktur *database management system* (DBMS) dapat dilihat tanpa harus menggunakan *user database*.

5.2 Saran

1. Untuk mengatasi kerentanan *sql injection* yang ditemukan, lakukan perbaikan dengan mengimplementasikan *prepared statements.* Hal ini dilakukan untuk memisahkan data dari *query* untuk mencegah serangan *sql injection* dan juga untuk mencegah pelaku kejahatan siber untuk mengubah logika dari *query sql*.

2. Menghapus *subdomain* yang tidak memiliki *status code* agar ketika melakukan pemindaian kerentanan secara berkala lebih menghemat waktu dikarenakan *subdomain* dan *domain* yang terdaftar jelas.

3. Melakukan *maintenance* secara berkala tidak hanya ketika terjadi peretasan saja.

4. Memasang *web application firewall* untuk melakukan blokir terhadap *client* yang berusaha melakukan serangan siber seperti menyisipkan *script sql* atau *cross-site scripting*, dan memblokir *client* yang mengirim banyak permintaan dalam satu waktu pada halaman tertentu seperti *login*.

DAFTAR PUSTAKA

[1] N. K., ‘Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)’, vol. 3, 2022.

[2] A. F. Hasibuan and D. Handoko, ‘Analisis Keretanan Website Dengan Aplikasi Owasp Zap’, vol. 2, 2023.

[3] B. Ghozali, K. Kusrini, and S. Sudarmawan, ‘Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating’, *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, Jan. 2019, doi: 10.24076/citec.2017v4i4.119.

[4] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, ‘Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard’, *MULTINETICS*, vol. 6, no. 2, pp. 169–178, Dec. 2020, doi: 10.32722/multinetics.v6i2.3432.

[5] H. A., ‘Web Application Security Exploitation and Cointern Measures for Modern Web Application’, *OReilly Media Inc*, 2020.

[6] B. B. Gupta and P. Chaudhary, *Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures*, 1st edn. CRC Press, 2020. doi: 10.1201/9780429351327.

[7] W. L. Jaelani and F. Khoirunnisa, ‘Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan Website Pada Instansi (Redacted)’, vol. 05, no. 01, 2023.

[8] ‘Analisis Keamanan Website Pemerintah Desa Curug Menggunakan Open Web Application Security Project (Owasp)’.

[9] S. D. Hilda, N. Heryana, and A. A. Ridha, ‘Website Security Analysis Curug Village Government Using Open Web Application Security Project (OWASP)’, *J. Inform. Dan Tek. Elektro Terap.*, vol. 12, no. 3S1, Oct. 2024, doi: 10.23960/jitet.v12i3S1.5236.

[10] R. Farismana and D. Pramadhana, ‘Vulnerability Assessment Untuk Analisis Tingkat Keamanan Pada Sistem Informasi Repositori Karya Ilmiah Politeknik Xyz’, vol. 3, 2023.

[11] V. Vikas, G. Saisri, T. S. Meghana, A. S. Harshini, and G. Kaveri, ‘Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security’, *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 7, pp. 794–805, July 2023, doi: 10.22214/ijraset.2023.54658.

[12] Information Systems Study Program, Faculty of Engineering and Informatics, Gajayana University Malang, Indonesia *et al.*, ‘Identify Vulnerabilities on the

Ministry of Health's Ayo Sehat Website Through Penetration Testing', *Eng. Technol. J.*, vol. 09, no. 07, July 2024, doi: 10.47191/etj/v9i07.11.

[13] Y. Alkhurayyif and Y. Saad Almarshdy, 'Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations', *J. Inf. Secur. Cybercrimes Res.*, vol. 07, no. 01, pp. 51–66, Jan. 2024.

[14] M. F. Safitra, M. Lubis, and A. Widjajarto, 'Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website', in *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering*, Fukuoka Japan: ACM, Mar. 2023, pp. 139–145. doi: 10.1145/3592307.3592329.

[15] F. Putra Utama and R. M. Hilmi Nurhadi, 'Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method', *CommIT Commun. Inf. Technol. J.*, vol. 18, no. 1, pp. 39–51, Apr. 2024, doi: 10.21512/commit.v18i1.9384.

[16] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, 'Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)', *J. Komput. Dan Inform.*, vol. 11, no. 1, pp. 91–95, Mar. 2023, doi: 10.35508/jicon.v11i1.9809.

[17] I. M. E. Listartha and G. A. J. Saskara, 'Pengujian Keamanan Dengan Metode Penetration Testing Execution Standard (Ptes) Untuk Menemukan Kerentanan Misconfigurations Pada Perangkat Jaringan', vol. 10.

[18] L. F. Burhani and D. Priyawati, 'Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (PTES)', *JIPI J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 9, no. 1, pp. 307–319, Feb. 2024, doi: 10.29100/jipi.v9i1.4455.

[19] A. I. Kusumarini and H. B. Seta, 'Information System Security Analysis to Determine Server Security Vulnerability with Penetration Testing Execution Standard (PTES) Method at VWX University', in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, Jakarta, Indonesia: IEEE, Oct. 2021, pp. 7–12. doi: 10.1109/ICIMCIS53775.2021.9699285.

[20] F. Z. Lidanta, A. Almaarif, and A. Budiyono, 'Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang', in *2021 International Conference on ICT for Smart Society (ICISS)*, Bandung, Indonesia: IEEE, Aug. 2021, pp. 1–5. doi: 10.1109/ICISS53185.2021.9533216.

[21] F. S. Hamdi and I. Maita, 'Pelatihan Pembuatan Website Memanfaatkan Wix Untuk Blog Pribadi Pada Siswa SMAN 2 Gunung Talang: Website Development Training Using Wix for Personal Blogs for Students of SMAN 2 Gunung Talang', *CONSEN Indones. J. Community Serv. Engagem.*, vol. 2, no. 2, pp. 64–69, Nov. 2022, doi: 10.57152/consen.v2i2.471.

[22] J. Bakti, 'PELATIHAN PEMBUATAN WEBSITE CARRD . CO SEBAGAI MEDIA PERSONAL BRANDING UNTUK', vol. 0, 2022.

[23] PTES. 2014. Pre-Engagement Interaction. 'http://www.penteststandard.org/index.php/Pre-engagement'. Diakses pada 29 November 19:00 WIB.

[24] PTES, 2014, Threat Modelling, ‘http://www.pentest-standard.org/index.php/Threat_Modeling’.
[25] PTES, 2014, Vulnerability Analysis, ‘http://www.penteststandard.org/index.php/Vulnerability_Analysis’, Diakses pada 29 November 19:00 WIB.
[26] PTES, 2014, Exploitation, ‘http://www.penteststandard.org/index.php/Exploitation’, Diakses pada 29 November 19:00 WIB.
[27] PTES, 2014, Post-Exploitation, ‘http://www.pentest-standard.org/index.php/Post_Exploitation’, Diakses pada 29 November19:00 WIB.
[28] PTES, 2014, Post-Exploitation, ‘http://www.penteststandard.org/index.php/Reporting’ . Diakses pada 29 November 19:00 WIB.
[29] Open Web Application Project, 2025, OWASP Top Ten 2025, ‘https://owasp.org/www-project-top-ten’, Diakses pada 29 November 19:00 WIB.
[30] Parrotsec, 2013, What is ParrotOS?, ‘https://parrotsec.org/docs/introduction/what-is-parrot’, . Diakses pada 29 November 19:00 WIB.
[31] sqlmap ‘https://sqlmap.org/’, . Diakses pada 29 November 19:00 WIB.
[32] Github Chaitin, 2024, xray, ‘https://github.com/chaitin/xray/blob/master/README_EN.md’, . Diakses pada 29 November 19:00 WIB.