

VULNERABILITY ASSESSMENT DAN PENETRATION TESTING
MENGGUNAKAN NIST SP 800-115 PENETRATION TESTING
METHODOLOGY TERHADAP WEBSITE
(STUDI KASUS : PROVINSI LAMPUNG)

(SKRIPSI)

Oleh

HAZEL FATHONI FRIANDRA

2115061112



FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2025

ABSTRAK

VULNERABILITY ASSESSMENT DAN PENETRATION TESTING MENGUNAKAN NIST SP 800-115 PENETRATION TESTING METHODOLOGY TERHADAP WEBSITE (STUDI KASUS : PROVINSI LAMPUNG)

Oleh

HAZEL FATHONI FRIANDRA

Keamanan aplikasi web merupakan aspek krusial dalam menjaga integritas dan kerahasiaan data. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan dua website milik instansi pemerintah daerah Provinsi Lampung, yaitu *website* dengan domain *lampungprov.go.id* dan *sigajahkerja.disnaker.lampungprov.go.id*, dengan menggunakan *Vulnerability Assessment* dan *Penetration Testing*. Metodologi yang digunakan mengacu pada standar NIST SP 800-115 *Penetration Testing Methodology* untuk tahapan pengujian serta pemanfaatan alat bantu OWASP ZAP dalam proses identifikasi kerentanan. Hasil pengujian menunjukkan bahwa kedua website memiliki total 12 kerentanan, yang terdiri dari 1 kerentanan dengan tingkat risiko tinggi, 4 menengah, dan 7 rendah. Beberapa kerentanan dengan tingkat menengah berhasil dieksploitasi, sedangkan kerentanan tinggi tidak dapat dieksploitasi secara langsung. Temuan mayoritas berkaitan dengan Security Misconfiguration dan Vulnerable and Outdated Components, yang termasuk dalam kategori OWASP Top 10 tahun 2021. Kesimpulan dari penelitian ini menekankan bahwa meskipun sistem tampak cukup terlindungi dari sisi permukaan, diperlukan pemeliharaan berkala, pembaruan komponen, dan penguatan konfigurasi internal untuk meminimalisir risiko serangan di masa mendatang.

Kata kunci: Keamanan web, *Vulnerability Assessment*, *Penetration Testing*, NIST SP 800-115, OWASP ZAP, OWASP Top 10.

ABSTRACT

VULNERABILITY ASSESSMENT AND PENETRATION TESTING USING NIST SP 800-115 PENETRATION TESTING METHODOLOGY ON WEBSITE (CASE STUDY: LAMPUNG PROVINCE)

By

HAZEL FATHONI FRIANDRA

Web application security is a crucial aspect in maintaining data integrity and confidentiality. This research aims to evaluate the security level of two websites owned by the regional government of Lampung Province, namely the websites with the domains `lampungprov.go.id` and `sigajahkerja.disnaker.lampungprov.go.id`, by performing Vulnerability Assessment and Penetration Testing. The methodology used refers to the NIST SP 800-115 Penetration Testing Methodology standard for the testing phases, as well as the utilization of the OWASP ZAP tool in the vulnerability identification process. The test results show that both websites contain a total of 12 vulnerabilities, consisting of 1 high-risk, 4 medium-risk, and 7 low-risk vulnerabilities. Some of the medium-risk vulnerabilities were successfully exploited, while the high-risk vulnerability could not be exploited directly. Most of the findings are related to Security Misconfiguration and Vulnerable and Outdated Components, which are part of the OWASP Top 10 category in 2021. In addition, the conclusion of this research emphasizes that although the systems appear fairly protected on the surface, periodic maintenance, component updates, and reinforcement of internal configurations are required to minimize the risk of future attacks.

Keywords: Web security, Vulnerability Assessment, Penetration Testing, NIST SP 800-115, OWASP ZAP, OWASP Top 10.

VULNERABILITY ASSESSMENT DAN PENETRATION TESTING
MENGGUNAKAN NIST SP 800-115 PENETRATION TESTING
METHODOLOGY TERHADAP WEBSITE
(STUDI KASUS : PROVINSI LAMPUNG)

Oleh
HAZEL FATHONI FRIANDRA

Skripsi
Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA TEKNIK

Pada
Program Studi S1 Teknik Informatika
Fakultas Teknik



FAKULTAS TEKNIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG

2025

Judul Skripsi : ***Vulnerability Assessment dan Penetration Testing Menggunakan NIST SP 800-115 Penetration Testing Methodology Terhadap Website (Studi Kasus : Provinsi Lampung)***

Nama Mahasiswa : ***Hazel Fathoni Friandra***

Nomor Pokok Mahasiswa : 2115061112

Program Studi : Teknik Informatika

Fakultas : Teknik



Pembimbing Utama

Pembimbing Pendamping

Resty Annisa, S.ST., M. KOM.
NIP. 199008302019032019

Rio Ariestia Pradipta, S.KOM., M.T.I.
NIP. 198603232019031013

2. Mengetahui

Ketua Jurusan
Teknik Elektro

Ketua Program Studi
Teknik Informatika


Herlinawati, S.T., M.T.
NIP. 19710314199903 2 001


Yessi Mulyani, S.T., M.T.
NIP. 197312262000122001

MENGESAHKAN

1. Tim Penguji

Ketua : Resty Annisa, S.ST., M. KOM.



Sekretaris : Rio Ariestia Pradipta, S.KOM., M.T.I.



Penguji : Mona Arif Muda, S.T.,M.T



2. Dekan Fakultas Teknik



Dr. Eng. Ir. Helmy Fitriawan, S.T, M.Sc.
NIP. 197509282001121002

Tanggal Lulus Ujian Skripsi : 30 Juli 2025

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah dilakukan orang lain dan sepanjang sepengetahuan saya tidak terdapat atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini sebagaimana yang disebutkan dalam daftar pustaka. Selain itu, saya menyatakan pula bahwa skripsi ini dibuat oleh saya sendiri.

Apabila pernyataan saya tidak benar, maka saya bersedia dikenai sanksi sesuai dengan hukum yang berlaku.

Bandar Lampung, 30 Juli 2025



Hazel Fathoni Friandra

NPM. 2115061112

RIWAYAT HIDUP



Hazel Fathoni Friandra atau sering dipanggil dengan Hazel, lahir di kota Padang, 08 September 2003. Penulis merupakan anak pertama dari tiga bersaudara, putra sulung dari pasangan Bapak Efrizaldi dan Ibu Lusi Andriani.

Penulis menempuh pendidikan pertama kali pada Taman Kanak-Kanak Jihad pada tahun 2009, lalu penulis menempuh pendidikan jenjang Sekolah Dasar Negeri 07 Silaing Bawah sampai dengan bangku kelas 6 dan lulus pada tahun 2014, lalu penulis melanjutkan pendidikan ke jenjang Sekolah Menengah Pertama Negeri 1 Kota Padang Panjang dan lulus pada tahun 2018, lalu penulis melanjutkan pendidikan ke jenjang Sekolah Menengah Atas Negeri 2 Kota Padang Panjang dan lulus pada tahun 2021, kemudian penulis melanjutkan pendidikan ke jenjang Perguruan Tinggi di Universitas Lampung pada Program Strata 1 (S1) Jurusan Teknik Elektro Program Studi Teknik Informatika dengan masuk jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN)

Selama menjalani masa perkuliahan, penulis aktif terlibat dalam organisasi kemahasiswaan, khususnya di Himpunan Mahasiswa Teknik Elektro (HIMATRO). Pada periode pertama keanggotaan penulis menjadi anggota Departemen Sosial dan Kewirausahaan. Pada periode kedua keanggotaan penulis diamanahkan untuk menjadi anggota Departemen Kaderisasi dan Pengembangan Organisasi. Di luar kegiatan akademik, penulis pernah menjadi pengurus dari Ikatan Mahasiswa Minang (IMAMI) dan diamanahkan menjadi anggota Departemen Komunikasi dan Informasi.

PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah, Atas Berkat Rahmat Allah yang Maha Kuasa

KUPERSEMBAHKAN KARYA INI UNTUK

Bapak dan Ibu Tercinta

Efrizaldi dan Lusi Andriani

Yang selalu jadi alasan utama terus melangkah, dengan cinta, doa, dan pengorbanan yang tak pernah terucap, namun jelas terasa dan nyata terlihat

Kedua Adikku

Titan Adyuta Friandra dan Masyaila Grania Friandra

Yang menjadi sandaran di balik langkah-langkah rapuh, dengan kasih tanpa suara, semangat yang tulus, dan kehadiran yang berarti lebih dari sekedar kata

Om dan Tante Tersayang

Ahmad Zaenudin dan Linda Novita

Yang telah menjadi tempat pulang di tanah rantau, menyediakan kasih, perhatian, dan kehangatan rumah saat jauh dari orang tua

Keluarga Besar yang selalu menjadi sumber semangat,
Dosen yang telah membimbing dengan tulus,
serta seluruh teman yang setia kebersamai setiap langkah perjalanan ini

MOTTO

"Sesungguhnya bersama kesulitan ada kemudahan."

(QS. Al-Insyirah: 6)

“Berbagai cobaan dan hal yang buat kau ragu, jadikan percikan tuk menempa tekad mu, jalan hidupmu hanya milik mu sendiri, raskan nikmatnya hidup mu hari ini”

(Hindia – Rasakan Nikmatnya Hidup)

“And when you want something, all the universe conspires in helping you to achieve it.”

(Paulo Coelho, *The Alchemist*)

“Ada makna dalam setiap perhentian, ada arah dalam setiap kebingungan. Hidup bukan soal tahu, tapi terus mencari”

(Penulis)

SANWACANA

Segala puji hanya milik Allah Subhanahu wa Ta'ala, atas rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak yang telah memberikan motivasi dan bantuan sepanjang prosesnya

Skripsi dengan judul ***“Vulnerability Assessment dan Penetration Testing Menggunakan NIST SP 800-115 Penetration Testing Methodology Terhadap Website (Studi Kasus : Provinsi Lampung)”*** ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung. Pada kesempatan ini, Penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada seluruh pihak yang berperan penting dalam perjalanan penulis untuk menyelesaikan skripsi ini.

1. Keluargaku, yaitu bapak, ibu, kedua adikku, serta om dan tante, yang tak henti mengirimkan doa di setiap langkah perjalanan penulis dan menjadi sumber motivasi agar penulis terus melangkah menyelesaikan apa yang telah dimulai.
2. Ibu Resty Annisa, S.ST., M. KOM.selaku dosen pembimbing utama penelitian yang selalu memberikan pengajaran, nasehat, motivasi serta kepercayaan yang telah diberikan kepada penulis.
3. Bapak Rio Ariestia Pradipta, S.KOM., M.T.I.selaku dosen pembimbing pendamping penelitian yang selalu memberikan masukan dan motivasi dalam proses pembuatan tugas akhir.
4. Bapak Mona Arid Muda, S.T.,M.T.selaku dosen penguji penelitian yang selalu memberikan saran dan masukan yang membangun dalam penelitian yang dilakukan oleh Penulis.
5. Bapak Dr. Eng. Ir. Helmy Fitriawan, S.T., M.Sc selaku Dekan Fakultas Teknik Universitas Lampung

6. Ibu Herlinawati, S.T., M.T selaku Ketua Jurusan Teknik Elektro Universitas Lampung
7. Ibu Yessi Mulyani, S.T., M.T.selaku Kepala Program Studi Teknik Elektro Universitas Lampung
8. Segenap Dosen di Jurusan Teknik Elektro yang telah memberikan ilmu yang bermanfaat, wawasan, motivasi, dan pengalaman bagi Penulis.
9. Mbak Rika dan Segenap Staff di Jurusan Teknik Elektro dan Fakultas Teknik yang telah sangat membantu penulis baik dalam hal administrasi dan hal-hal lainnya.
10. Keluarga Kost Ming yaitu Milano, Adil, Brilian, teman seperjalanan dalam ruang dan waktu yang sama, yang tidak hanya hadir sebagai rekan diskusi dan tawa, tetapi juga sebagai penanda bahwa perjuangan ini tidak pernah benar-benar sendiri.
11. Keluarga ANKER 21 yaitu Haqqu, Irfan, Mahesa, Jentrio, Matsal, Ojan, Agra, Aghas, Wayan, Rahmad, Ozi, Kadapi, Tegar, Bimo, Yozi, Azra, Rizki Febrian, Hazel, Sandi, Faris, Iqbal, Hud, Abi, dan Ridho, wajah-wajah yang hampir setiap hari mengisi keseharian di kampus, dengan tawa spontan, obrolan receh, dan candaan yang selalu berhasil mencairkan penat, kebersamaan ini bukan hanya pelengkap hari, tapi jadi alasan perjalanan ini terasa ringan, meski terkadang langkahnya berat.
12. Anggota Kaderisasi dan Pengembangan Organisasi Angkatan 2021, teman-teman yang menjadi rekan seperjalanan dalam dinamika organisasi, yang telah menjadi rumah kedua dalam hiruk-pikuk perjuangan, teman berbagai lelah dan tawa di setiap rapat,agenda, hingga larut malam, yang menjadikan HIMATRO bukan sekadar himpunan, tapi tempat tumbuh dan menguat bersama.
13. Damar Fachri dan Jihan Salsabila, teman seperjuangan sejak masa putih abu-abu. Meski tak lagi duduk di bangku yang sama, kalian tetap hadir lewat doa, cerita, dan semangat dari kejauhan. Kuucapkan terima kasih telah menjadi penguat di setiap langkah perjalanan ini.

14. THE JUNIORIOUS, teman-teman sepermainan sejak di kampung halaman, yang tak pernah hilang meski jarak dan waktu menjauh, selalu menjadi pengingat akan akar dan asal, tempat pulang yang tak pernah berubah meski waktu berlalu
15. Kepada Kepala Kampung, Perangkat Desa, Induk Semang dan Tim Kuliah Kerja Nyata (KKN) Periode 1 Kampung Aji Jaya KNPI, yang telah memberikan kenangan dan pengalaman hidup yang berarti bagi penulis.
16. Keluarga besar EXCALTO 2021, selaku teman satu angkatan penulis yang menemani perjalanan dari awal hingga akhir status sebagai “mahasiswa” serta menjadi warna dalam dunia perkuliahan penulis.
17. Keluarga besar HIMATRO, wadah tempat penulis tumbuh dan menempa diri, yang menghadirkan banyak pelajaran, tantangan, dan kebersamaan, serta menjadi salah satu bagian penting dalam proses pendewasaan selama masa perkuliahan.
18. Hazel, selaku penulis atau diri sendiri, yang tetap bertahan meski sempat ingin menyerah, yang terus melangkah meski tak selalu tahu arah, yang memilih bangkit setiap kali jatuh, dan belajar untuk tidak hanya kuat, tapi juga ikhlas, terima kasih telah sampai sejauh ini.
19. Seluruh pihak yang tidak bisa disebutkan satu persatu, namun turut hadir dan terlibat dalam setiap proses perkuliahan hingga penyusunan skripsi ini, penulis mengucapkan terima kasih atas segala bentuk bantuan, dukungan, dan kerja samanya.

Bandar Lampung, 29 Juli 2025

Hazel Fathoni Friandra

DAFTAR ISI

	Halaman
ABSTRAK	ii
LEMBAR PERSETUJUAN.....	v
LEMBAR PENGESAHAN	vi
SURAT PERNYATAAN	vii
RIWAYAT HIDUP	viii
PERSEMBAHAN	ix
MOTTO	x
SANWACANA	xi
DAFTAR ISI.....	xiv
DAFTAR TABEL	xviii
DAFTAR GAMBAR.....	xx
I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Manfaat Penelitian	4
1.5 Batasan Masalah.....	5
1.6 Sistematika Penulisan Laporan	5
II. TINJAUAN PUSTAKA	8
2.1 Konsep Sistem Informasi	8

2.2 Keamanan Informasi	10
2.3 <i>Website</i>	12
2.4 Kerentanan Sistem.....	14
2.5 <i>Vulnerability Assessment</i>	15
2.6 <i>Penetration Testing</i>	17
2.7 NIST SP 800-115 <i>Penetration Testing Methodology</i>	20
2.8 Tools.....	21
2.8.1 OWASP ZAP.....	21
2.8.2 Oracle VM Virtual Box	24
2.8.3 Kali Linux.....	24
2.8.4 Ping	25
2.8.5 Whois.....	25
2.8.6 Whatweb	26
2.8.7 WhatWaf.....	26
2.8.8 Nmap.....	27
2.8.9 Burp Suite	27
2.9 OWASP Top 10 2021.....	28
2.10 Penelitian Terkait.....	34
III. METODOLOGI PENELITIAN.....	40
3.1 Waktu dan Tempat Penelitian	40
3.2 Alat dan Bahan Penelitian	41
3.3 Objek Penelitian.....	43
3.3.1 lampungprov.go.id.....	43
3.3.2 sigajahkerja.disnaker.lampungprov.go.id	45

3.4 Tahapan Penelitian	47
3.4.1 <i>Planning</i>	48
3.4.2 <i>Discovery</i>	49
3.4.3 <i>Attack</i>	51
3.4.4 <i>Reporting</i>	52
IV. HASIL DAN PEMBAHASAN.....	53
4.1 <i>Planning</i>	53
4.2 <i>Discovery</i>	54
4.2.1 <i>Information Gathering</i>	54
4.2.1.1 Ping	54
4.2.1.2 Whois	57
4.2.1.3 WhatWeb.....	63
4.2.1.4 Whatwaf.....	79
4.2.1.5 Nmap <i>Port Scanning</i>	83
4.2.2 <i>Vulnerability Scanning</i>	90
4.3 Attack.....	93
4.4 <i>Reporting</i>	143
4.4.1 <i>Vulnerability Assessment Report</i>	143
4.4.2 <i>Penetration Testing Report</i>	162
4.4.3 OWASP Top 10 2021 <i>Based Vulnerability Mapping</i>	170
V. KESIMPULAN DAN SARAN.....	173
5.1 KESIMPULAN	173
5.2 SARAN.....	174
INDEKS	175

DAFTAR PUSTAKA.....	182
LAMPIRAN.....	190

DAFTAR TABEL

Tabel 2. 1 Penjelasan OWASP Top 10 2021 [43]	29
Tabel 3. 1 <i>Timeline</i> Penelitian.....	40
Tabel 3. 2 Alat dan Bahan Penelitian.....	41
Tabel 4. 1 Hasil Pengujian Ping <i>Website</i> lampungprov.go.id.....	55
Tabel 4. 2 Hasil Pengujian Ping <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id..	56
Tabel 4. 3 Hasil Pengujian Whois <i>Website</i> lampungprov.go.id.....	59
Tabel 4. 4 Hasil Pengujian Whois <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	61
Tabel 4. 5 Hasil Pengujian Whatweb <i>Website</i> lampungprov.go.id.....	67
Tabel 4. 6 Hasil Pengujian Whatweb <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	74
Tabel 4. 7 Hasil Pengujian Whatwaf <i>Website</i> lampungprov.go.id	80
Tabel 4. 8 Hasil Pengujian Whatwaf <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	82
Tabel 4. 9 Hasil Pengujian Nmap <i>Website</i> lampungprov.go.id	84
Tabel 4. 10 Hasil Pengujian Nmap <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	86
Tabel 4. 11 Hasil <i>Vulnerability Scanning Website</i> lampungprov.go.id	91
Tabel 4. 12 Hasil <i>Vulnerability Scanning Website</i> sigajahkerja.disnaker.lampungprov.go.id	92
Tabel 4. 13 Rencana Tindakan Eksploitasi	93
Tabel 4. 14 <i>Vulnerability Assessment Report Website</i> lampungprov.go.id	143
Tabel 4. 15 <i>Vulnerability Assessment Report Website</i> sigajahkerja.disnaker.lampungprov.go.id	153

Tabel 4. 16 <i>Penetration Testing Report Website</i> lampungprov.go.id	162
Tabel 4. 17 <i>Penetration Testing Report Website</i> sigajahkerja.disnaker.lampungprov.go.id	167
Tabel 4. 18 OWASP Top 10 2021 <i>Based Vulnerability Mapping Website</i> lampungprov.go.id	
Tabel 4. 19 OWASP Top 10 2021 <i>Based Vulnerability Mapping Website</i> sigajahkerja.lampungprov.go.id	171

DAFTAR GAMBAR

Gambar 2. 1 Konsep Sistem Informasi [4].....	8
Gambar 2. 2 CIA Triad <i>Methodology</i> [10].....	9
Gambar 2. 3 Cara Kerja <i>Website</i> [14].....	13
Gambar 2. 4 NIST SP 800-115 <i>Penetration Testing Methodology</i> [24].....	20
Gambar 2. 5 Cara Kerja OWASP ZAP [28]	22
Gambar 2. 6 OWASP Top 10 2021 <i>List</i> [42].....	29
Gambar 3. 1 Halaman Utama <i>Website</i> lampungprov.go.id [51]	45
Gambar 3. 2 Halaman Beranda <i>Website</i> lampungprov.go.id [51]	45
Gambar 3. 3 Tampilan Halaman Beranda <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	46
Gambar 3. 4 Tahapan Penelitian	47
Gambar 4. 1 Hasil Pengujian Ping <i>Website</i> lampungprov.go.id	55
Gambar 4. 2 Hasil Pengujian Ping <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	56
Gambar 4. 3 Hasil Pengujian Whois <i>Website</i> lampungprov.go.id.....	59
Gambar 4. 4 Hasil Pengujian Whois <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	61
Gambar 4. 5 Hasil Pengujian Whatweb <i>Website</i> lampungprov.go.id.....	66
Gambar 4. 6 Hasil Pengujian Whatweb <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	74
Gambar 4. 7 Hasil Pengujian Whatwaf <i>Website</i> lampungprov.go.id.....	80
Gambar 4. 8 Hasil Pengujian Whatwaf <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	81
Gambar 4. 9 Hasil Pengujian Nmap <i>Website</i> lampungprov.go.id.....	84

Gambar 4. 10 Hasil Pengujian Nmap <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	86
Gambar 4. 11 Hasil Vulnerability Scanning <i>Website</i> lampungprov.go.id	90
Gambar 4. 12 Hasil Vulnerability Scanning <i>Website</i> sigajahkerja.disnaker.lampungprov.go.id	
Gambar 4. 13 Tampilan Halaman Rentan dan Validasi Kerentanan Data Tables	96
Gambar 4. 14 Memasukkan Kata Kunci Pada <i>Form Input Search</i>	97
Gambar 4. 15 Hasil <i>Intercept</i> Menggunakan <i>Proxy</i> Burp Suite	98
Gambar 4. 16 Struktur Permintaan GET Pada Halaman Pengujian.....	99
Gambar 4. 17 Hasil Pengujian Manual Pada <i>Website</i>	100
Gambar 4. 18 Perubahan Nilai Input Pencarian di <i>Repeater</i>	102
Gambar 4. 19 Respon Server Terhadap Permintaan	103
Gambar 4. 20 <i>Intruder Attack</i> dan Posisi <i>Payload</i>	104
Gambar 4. 21 <i>Intruder Attack</i> Berjalan.....	105
Gambar 4. 22 Hasil Dari <i>Intruder Attack</i>	105
Gambar 4. 23 Perintah curl -s Untuk Pengujian	107
Gambar 4. 24 <i>Intercept Request</i> Halaman Lowongan Menggunakan Burp Suite	108
Gambar 4. 25 Hasil <i>Response</i> Halaman Lowongan Website sigajahkerja.disnaker.lampungprov.go.id	108
Gambar 4. 26 <i>Intercept Request</i> Halaman Detail 493 Menggunakan Burp Suite	109
Gambar 4. 27 Hasil <i>Response</i> Halaman Detail 493 Website sigajahkerja.disnaker.lampungprov.go.id	110
Gambar 4. 28 Tampilan Burp Suite <i>Collaborator</i>	113
Gambar 4. 29 Bar Side Burp Suite <i>Collaborator</i>	114
Gambar 4. 30 Halaman Target Pengujian	115
Gambar 4. 31 Notifikasi Pesan Berhasil Dikirimkan Pada Halaman Pengujian.....	115
Gambar 4. 32 Interaksi Server Burp Collaborator Dengan Target	116
Gambar 4. 33 Cookie Sesi yang Berhasil Didapatkan	116
Gambar 4. 34 Pengujian <i>Cross Site Scripting</i> untuk Antarmuka <i>Website</i>	117
Gambar 4. 35 <i>Payload</i> Berhasil Terkirim.....	118

Gambar 4. 36 Hasil Pengujian <i>Cross Site Scripting</i> pada <i>Website</i>	119
Gambar 4. 37 Pengecekan <i>Header</i> Pada Halaman Target Pengujian	120
Gambar 4. 38 Kode HTML Untuk Pengujian Kerentanan	121
Gambar 4. 39 Hasil Eksekusi Kode HTML Untuk Pengujian	122
Gambar 4. 40 Hasil Eksekusi Kode HTML Untuk Pengujian	123
Gambar 4. 41 Versi Bootstrap Yang Digunakan <i>Website</i> lampungprov.go.id	124
Gambar 4. 42 Versi jQuery Yang Digunakan <i>Website</i> lampungprov.go.id.....	124
Gambar 4. 43 Tampilan <i>Form</i> Pencarian Pada <i>Website</i>	125
Gambar 4. 44 Hasil Pencarian <i>Payload</i> Pada <i>Website</i>	126
Gambar 4. 45 Hasil Pengecekan Struktur Halaman Menggunakan <i>Developer Tools</i>	127
Gambar 4. 46 Hasil Pengujian Manipulasi URL Pada <i>Website</i>	128
Gambar 4. 47 Halaman Teridentifikasi Rentan Tanpa CSP <i>Header</i>	129
Gambar 4. 48 Hasil <i>Intercept</i> Halaman Menggunakan Burp Suite	130
Gambar 4. 49 Lokasi <i>Payload</i> Dimasukkan Pada <i>Request Website</i>	130
Gambar 4. 50 <i>Intruder Attack</i> Pada Halaman <i>Website</i>	131
Gambar 4. 51 Hasil Pengujian <i>Intruder Attack</i> Pada Halaman <i>Website</i>	131
Gambar 4. 52 Hasil <i>Intruder Attack</i> Dilihat Dari Browser	132
Gambar 4. 53 Hasil <i>Response</i> dari Server <i>Website</i>	132
Gambar 4. 54 <i>Header Response</i> Halaman <i>Website</i>	133
Gambar 4. 55 Kode HTML Untuk Pengujian.....	134
Gambar 4. 56 Hasil Eksekusi Kode HTML Pada <i>Website</i>	135
Gambar 4. 57 Pengecekan Menggunakan <i>Repeater</i> Pada Burp Suite	136
Gambar 4. 58 <i>Hidden File Found</i> Pada <i>Website</i>	137
Gambar 4. 59 Versi Bootstrap Yang Digunakan <i>Website</i>	138
Gambar 4. 60 Versi jQuery Yang Digunakan <i>Website</i>	139
Gambar 4. 61 Hasil <i>Intercept</i> Menggunakan Burp Suite	140
Gambar 4. 62 Bagian HTML Halaman <i>Website</i>	141
Gambar 4. 63 Hasil Manipulasi URL Pada <i>Website</i>	141

I. PENDAHULUAN

1.1 Latar Belakang

Pesatnya kemajuan dan perkembangan Teknologi Informasi telah membuat teknologi informasi menjadi sebuah aspek yang selalu hidup berdampingan dengan manusia, pemanfaatan teknologi informasi tidak lepas dari naiknya penggunaan internet [1]. Laporan dari International Telecommunication Union (ITU) mendokumentasikan pada tahun 2024, sekitar 5,5 miliar orang telah terhubung ke internet, yang mana angka ini mencakup 68 persen dari populasi dunia. Angka ini meningkat dibandingkan tahun 2023 sebanyak 3 persen [2]. Peningkatan jumlah pengguna internet tidak hanya dapat menciptakan peluang baru dalam akses layanan dan informasi, tetapi juga mendatangkan tantangan baru dalam penerapannya, ancaman ini sering dikenal dengan ancaman siber. Ancaman-ancaman seperti pencurian data, eksploitasi dan berbagai macam ancaman-ancaman lainnya juga turut berkembang seiring berkembangnya kemajuan Teknologi Informasi dan penggunaan internet [1]. Fenomena ini semakin nyata di Indonesia, dimana banyak sistem informasi milik pemerintah, baik di ranah nasional maupun daerah menjadi target dari serangan siber. Contoh kasus yang menonjol adalah serangan terhadap Pusat Data Nasional Sementara (PDNS) Juni 2024 yang sangat merugikan negara, selain itu banyak sistem informasi milik pemerintah terkena serangan *defacing*, dimana tampilan halaman mereka diubah oleh pihak tidak bertanggung jawab. Kasus-kasus ini menunjukkan bahwa ancaman siber terhadap sistem informasi pemerintah semakin meningkat, mengancam integritas data dan kepercayaan publik terhadap pemerintah.

Sistem Pemerintah Berbasis Elektronik (SPBE) merupakan sistem pemerintahan berbasis elektronik, aplikasi seluler, dan berbagai layanan elektronik [3]. Seiring

dengan implementasi SPBE, sistem informasi menjadi komponen kunci dalam pengelolaan data maupun penyampaian informasi. Penerapan sistem informasi yang efektif membuat organisasi tidak hanya mampu mengelola data dengan baik tetapi juga dapat meningkatkan efisiensi dan efektivitas [4]. Salah satu bentuk implementasi dari SPBE (Sistem Pemerintah Berbasis Elektronik) adalah *website* dari Provinsi Lampung.

Sistem informasi berbasis web yang sering digunakan termasuk dalam lingkungan pemerintahan, memiliki ancaman berbagai potensi celah keamanan seperti *Cross Site Scripting (XSS)* dan *SQL Injection* yang dapat dieksploitasi dengan serangan otomatis yang akan menyebabkan kerusakan serius bahkan kebocoran data [5]. Pengujian keamanan pada sistem informasi ini menjadi sebuah langkah yang dapat digunakan untuk mengurangi risiko serangan, salah satu cara yang sering digunakan untuk mengidentifikasi potensi kerentanan adalah *Vulnerability Assessment* dan *Penetration Testing*. *Vulnerability Assessment* merupakan proses untuk mengidentifikasi dan menganalisis potensi kerentanan pada sebuah sistem aplikasi [5]. Tujuan dari *Vulnerability Assessment* adalah melakukan proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan pada sistem. *Penetration testing* merupakan metode yang digunakan untuk menguji aplikasi atau komponen sebuah sistem, baik secara individu maupun keseluruhan, untuk mengevaluasi apakah ada kerentanan yang dapat dimanfaatkan, baik dalam komponen itu sendiri maupun antar komponen, yang dapat merusak aplikasi, data, atau sumber daya yang ada didalam sistem [6]. OWASP ZAP (*Open Web Application Security Project Zed Attacked Proxy*) merupakan sebuah alat yang dapat digunakan untuk melakukan pemindaian kerentanan yang aktif dan selalu diperbarui. OWASP ZAP sendiri merupakan sebuah proyek *open-source* dan dapat digunakan secara gratis [7]. OWASP ZAP mendukung pengujian berbasis *Black Box security testing* yang digunakan sebagai pendekatan pada penelitian ini karena pengujian tidak memiliki informasi apapun tentang sistem yang diuji, seperti sistem operasi, server maupun jaringan yang digunakan,[8].

Website Pemerintah Provinsi Lampung yang dapat diakses melalui URL lampungprov.go.id memiliki tujuan utama untuk memberikan informasi dan

transparansi pemerintahan kepada masyarakat, ketika diretas *website* ini dapat kehilangan fungsi utamanya. Peretasan dapat mengakibatkan manipulasi atau pengubahan informasi yang ditampilkan, sehingga menciptakan kesalahan informasi yang berpotensi memberikan informasi yang salah kepada masyarakat dan merusak kepercayaan publik terhadap pemerintahan. Selain itu gangguan pada aksesibilitas *website* juga dapat menghambat penyebaran informasi penting, termasuk layanan publik yang digunakan oleh masyarakat. Dampak lainnya adalah risiko pencemaran citra pemerintah akibat adanya penyisipan konten yang tidak semestinya atau propaganda yang dilakukan oleh orang yang tidak bertanggung jawab, yang dapat memberikan persepsi negatif terhadap komitmen pemerintah dalam menjaga keamanan dan transparansi data digitalnya.

Hal serupa juga berlaku pada *website* sigajahkerja.disnaker.lampungprov.go.id, yang dikelola oleh Dinas Tenaga Kerja Provinsi Lampung sebagai *platform* penyedia informasi lowongan kerja dan layanan ketenagakerjaan. Website ini menjadi sarana penting bagi pencari kerja dalam mengakses informasi peluang kerja yang tersedia serta bagi perusahaan dalam mempublikasikan lowongan. Jika *website* ini diretas, maka informasi lowongan dapat dimanipulasi, dihapus, atau diganti dengan konten yang tidak relevan maupun berbahaya, yang pada akhirnya akan mengacaukan proses pencarian kerja masyarakat. Gangguan akses atau kerusakan sistem juga dapat menghambat pelamar kerja dalam menggunakan layanan yang tersedia, serta merugikan pihak perusahaan yang tergantung pada *platform* ini untuk menjaring tenaga kerja.

Website ini menyediakan fitur pendaftaran akun bagi pengguna, terdapat data penting dan bersifat pribadi yang disimpan di dalam sistem, seperti nama lengkap, alamat email, nomor telepon, riwayat pendidikan, pengalaman kerja, serta dokumen pendukung seperti CV dan identitas diri. Jika sistem keamanan tidak memadai dan terjadi peretasan, data-data sensitif tersebut dapat terekspos, disalahgunakan, atau diperjualbelikan oleh pihak yang tidak bertanggung jawab. Hal ini dapat menurunkan tingkat kepercayaan publik terhadap keamanan sistem digital pemerintahan.

1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana cara pengujian keamanan dan identifikasi potensi kerentanan keamanan pada sistem informasi berbasis web dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id?
2. Apa saja jenis-jenis kerentanan keamanan yang ditemukan pada *website* dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id setelah melakukan *vulnerability assessment* dan *penetration testing*?
3. Bagaimana tingkat risiko keamanan dari kerentanan yang ditemukan pada *website* dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Menguji kerentanan-kerentanan *website* dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id
2. Mengetahui jenis-jenis kerentanan keamanan yang ditemukan pada *website* dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id.
3. Menganalisis dan Mengidentifikasi kondisi serta tingkat kerentanan pada *website* dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan sistem informasi pada *website* milik Pemerintah Provinsi Lampung, serta membantu pengelola *website* dalam mengidentifikasi dan mengatasi kerentanan keamanan.

Penelitian ini juga menjadi bagian penting dalam memenuhi persyaratan penyelesaian tugas akhir mahasiswa dan memperdalam pemahaman tentang pengujian keamanan sebuah sistem.

1.5 Batasan Masalah

Penelitian ini memiliki batasan tertentu agar fokus dan hasil penelitian dapat lebih terarah. Beberapa batasan masalah yang perlu diperhatikan adalah :

1. Penelitian hanya dilakukan pada *website* dengan domain *lampungprov.go.id* dan *sigajahkerja.disnaker.lampungprov.go.id*.
2. Pengujian keamanan sistem dilakukan menggunakan pendekatan atau metode *Black Box Security Testing* tanpa akses langsung terhadap struktur internal sistem.
3. Fokus pengujian hanya mencakup kerentanan keamanan berbasis *website* yang teridentifikasi oleh metode pengujian yang digunakan.
4. Penelitian ini memanfaatkan beberapa *tools* seperti OWASP ZAP untuk mendeteksi kerentanan.
5. Hasil penelitian ini tidak mencakup implementasi mitigasi atau perbaikan langsung terhadap kerentanan tersebut.
6. Proses eksploitasi kerentanan *website* dilakukan dengan cara yang aman dan tidak merusak dan mengganggu fungsionalitas sistem *website*.

1.6 Sistematika Penulisan Laporan

Adapun sistematika penulisan laporan Tugas Akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Penelitian ini dilatar belakangi oleh kebutuhan akan peningkatan keamanan pada *website* milik Pemerintah Provinsi Lampung, yang berperan penting dalam mendukung pelayanan publik dan administrasi pemerintahan. *Website* ini menjadi saran utama bagi

masyarakat untuk mengakses berbagai informasi dan layanan dari pemerintah. Seiring dengan semakin berkembangnya teknologi informasi, peran *website* pemerintah menjadi semakin vital, namun di sisi lain, potensi ancaman terhadap keamanan informasi yang terdapat pada *website* ini juga semakin meningkat. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan yang ada melalui pengujian keamanan berbasis *Black Box Testing*, yang menguji *website* dari perspektif pengguna tanpa pengetahuan tentang kode sumber sistem. Rumusan masalah dalam penelitian ini adalah bagaimana mengidentifikasi keamanan dan bagaimana pengujian berbasis *Black Box Testing*, batasan masalah mencakup objek penelitian serta metode pengujian yang digunakan. Manfaat dari penelitian ini adalah untuk memberikan gambaran tentang tingkat keamanan *website* pemerintah dan memberikan rekomendasi untuk perbaikan serta penguatan sistem keamanan, sehingga *website* ini dapat lebih aman dan dapat meningkatkan kepercayaan masyarakat terhadap pelayanan publik.

BAB II TINJAUAN PUSTAKA

Berisi tentang beberapa teori pendukung seperti konsep keamanan sistem informasi, teori mengenai pengujian yang dilakukan, *tools-tools* yang digunakan untuk penelitian, dan referensi materi yang diperoleh dari berbagai sumber seperti buku, jurnal, dan penelitian ilmiah yang digunakan untuk penulisan laporan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Berisi mengenai metodologi yang digunakan dalam penelitian ini. Penelitian dilakukan dari bulan Desember 2024 dengan fokus pada pengujian kewanaman *website* milik Pemerintah Provinsi Lampung, tepatnya pada domain provlampung.go.id. Pendekatan yang digunakan dalam penelitian ini adalah *Black Box Testing* untuk mengidentifikasi kerentanan tanpa memerlukan akses langsung terhadap sistem. Pada bab ini juga dijelaskan alat dan bahan yang menunjang penelitian ini, yang meliputi perangkat lunak untuk pengujian kerentanan, serta perangkat lain yang mendukung pelaksanaan pengujian keamanan. Metodologi penelitian mencakup pengumpulan data terkait target, pengujian kerentanan, analisis hasil pengujian, serta evaluasi hasil atau

rekomendasi perbaikan berdasarkan temuan kerentanan yang ditemukan selama proses pengujian.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang hasil pengujian keamanan *website* Pemerintah Provinsi Lampung terkhusus pada domain provlampung.go.id yang mana pengujian yang dilakukan adalah *Vulnerability Assessment* dan *Penetration Testing*. Pengujian difokuskan kepada potensi kerentanan yang ditemukan berdasarkan hasil pemindaian. Data yang diperoleh selama penelitian akan disajikan termasuk temuan kerentanan dan analisis potensi risiko yang akan ditimbulkan serta saran untuk perbaikan dan peningkatan keamanan pada *website*.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan dari penelitian yang dilakukan dan saran yang didasarkan pada hasil data mengenai perbaikan dan pengembangan lebih lanjut agar mendapatkan hasil yang lebih baik.

DAFTAR PUSTAKA

LAMPIRAN

II. TINJAUAN PUSTAKA

2.1 Konsep Sistem Informasi

Sistem informasi merupakan suatu kesatuan prosedur yang saling terkait untuk mencapai tujuan tertentu, dimana setiap langkah harus dilakukan secara berurutan dan terstruktur. Sistem ini terdiri dari beberapa komponen utama, yaitu perangkat keras, perangkat lunak, prosedur, jaringan komputer, basis data, dan sumber daya manusia [4] seperti yang dapat dilihat pada gambar dibawah ini



Gambar 2. 1 Konsep Sistem Informasi [4]

Sistem informasi merupakan sebuah sistem yang terintegrasi, dimana sistem ini dapat mengumpulkan, memproses, menyimpan serta mendistribusikan informasi, sistem ini sendiri bertujuan untuk membantu dan mendukung kebutuhan sebuah organisasi [9]. Dengan adanya sistem informasi, dapat memberikan manfaat untuk meningkatkan aksesibilitas data tepat waktu dan akurat, menjamin kualitas dan keterampilan pemanfaatan sistem, mengidentifikasi kebutuhan informasi untuk pengambilan

keputusan, dan mengembangkan proses perencanaan yang efektif. Dalam sistem informasi, terdapat hubungan yang saling terikat antara tiga elemen kunci, yaitu orang (*people*) yang memiliki peran penting dalam keberhasilan sebuah sistem informasi terutama keterlibatan dalam memahami kebutuhan organisasi, berkontribusi aktif dalam proses pengembangan, dan pengelolaan sistem informasi. Selanjutnya terdapat proses (*process*) yang memastikan semua komponen dalam sistem informasi saling terhubung secara optimal sehingga dapat meningkatkan efisiensi operasional, proses ini mencakup tahapan-tahapan seperti perancangan, implementasi hingga pengoperasian sistem informasi agar sesuai dengan kebutuhan. Terakhir teknologi (*technology*) yang menjadi pondasi utama yang mendukung integrasi aplikasi dan proses bisnis, sekaligus memastikan keamanan dalam sistem informasi [10]. Ketiga elemen ini sering dikenal dengan konsep *golden triangle* seperti pada gambar dibawah ini



Gambar 2. 2 CIA Triad Methodology [10]

Pemahaman tentang konsep dan komponen sistem informasi sangat penting dalam mendukung operasional dan pengambilan keputusan dalam sebuah organisasi. Sistem informasi, yang terdiri dari perangkat keras, perangkat lunak, prosedur, jaringan komputer, basis data, dan sumber daya manusia, bekerja secara sinergis untuk menghasilkan informasi yang akurat, tepat waktu, dan relevan. Dengan memperhatikan

elemen-elemen utama sesuai konsep *golden triangle*, organisasi dapat memaksimalkan potensi sistem informasi untuk meningkatkan efisiensi, efektivitas, dan daya saing [10].

Website lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id merupakan penerapan dari konsep sistem informasi yang mencakup perangkat keras, perangkat lunak, prosedur, jaringan komputer, dan sumber daya manusia untuk menyediakan layanan informasi publik secara transparan dan efektif. Sistem ini mendukung pelayanan publik yang efisien, sejalan dengan prinsip-prinsip CIA Triad yang memastikan keamanan data dan operasional *website* dalam menyediakan informasi yang akurat dan dapat diakses oleh masyarakat.

2.2 Keamanan Informasi

National Institute of Standards and Technology (NIST) mendefinisikan keamanan informasi adalah melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan yang tidak sah, modifikasi, atau penghancuran untuk memberikan kerahasiaan, integritas, dan ketersediaan atau sering dikenal dengan CIA [4], yang merupakan salah satu model yang paling banyak digunakan untuk memahami dan mengelola keamanan informasi, yang terdiri dari tiga prinsip utama

1. Kerahasiaan (*Confidentiality*)

Kerahasiaan adalah prinsip yang menjamin bahwa informasi hanya bisa diakses oleh pihak yang berwenang, sehingga melindungi data dari pihak yang tidak bertanggung jawab

2. Integritas (*Integrity*)

Integritas memastikan bahwa data tetap terjaga keasliannya dan tidak mengalami perubahan yang tidak sah, menjaga agar informasi tetap akurat dan dapat dipercaya

3. Ketersediaan (*Availability*)

Ketersediaan menjamin bahwa informasi dapat diakses oleh pihak yang berwenang kapan pun dibutuhkan, serta mengamankan jalur akses agar tetap aman dan dapat diandalkan [9].

Keamanan informasi adalah hal yang sangat penting untuk menjaga keberlanjutan dan integritas aset informasi dalam sebuah organisasi. Terdapat beberapa jenis keamanan informasi yang dapat dibagi menjadi beberapa kategori seperti berikut :

1. Keamanan Fisik (*Physical Security*)

Fokus pada strategi untuk melindungi sumber daya fisik dalam organisasi, seperti pegawai, aset, dan tempat kerja dari potensi ancaman seperti kebakaran, bencana alam, atau akses tidak sah.

2. Keamanan Pribadi (*Personal Security*)

Meliputi perlindungan terhadap individu dalam organisasi, baik yang berhubungan langsung dengan fisik maupun keselamatan mereka selama berinteraksi dengan perusahaan.

3. Keamanan Operasional (*Operational Security*)

Strategi yang memastikan kelancaran operasional organisasi tanpa gangguan yang dapat merusak jalannya proses.

4. Keamanan Komunikasi (*Communication Security*)

Bertujuan untuk mengamankan teknologi dan media komunikasi yang digunakan oleh organisasi, serta memastikan bahwa alat komunikasi tersebut digunakan dengan benar untuk mencapai tujuan organisasi.

5. Keamanan Jaringan (*Network Security*)

Fokus pada perlindungan infrastruktur jaringan, data yang dikirimkan, dan kemampuan organisasi untuk menggunakan jaringan secara aman untuk mendukung fungsi komunikasi data [11].

Keamanan informasi merupakan aspek vital yang harus diperhatikan dalam setiap organisasi untuk melindungi aset informasi dari berbagai ancaman. Dengan penerapan

prinsip-prinsip dasar seperti CIA Triad, organisasi dapat memastikan bahwa data sensitif tetap terjaga dan aman dari potensi penyalahgunaan. Berbagai kategori keamanan menunjukkan pentingnya pendekatan menyeluruh dalam melindungi informasi. Oleh karena itu, pemahaman yang mendalam tentang ancaman yang ada dan penerapan strategi keamanan yang efektif sangat diperlukan untuk menjaga keberlanjutan dan integritas sistem informasi dalam organisasi.

Website lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id sebagai sistem informasi publik, memerlukan penerapan prinsip CIA Triad untuk memastikan keamanan data. Kerahasiaan melindungi informasi dari penyalahgunaan, integrasi menjadi akurasi data, dan ketersediaan memastikan *website* selalu dapat diakses masyarakat tanpa gangguan. Penerapan prinsip ini penting untuk menjaga keberlanjutan dan integritas *website* pemerintah.

2.3 Website

Website adalah kumpulan halaman digital yang menyajikan informasi dalam bentuk teks, animasi, gambar, suara, video, atau kombinasi dari semuanya yang dapat diakses melalui internet, berdasarkan jenisnya *website* terbagi menjadi tiga jenis [12] :

1. Web Statis

Website dengan halaman yang tidak berubah kecuali diperbarui secara manual melalui pengeditan kode struktur.

2. Web Dinamis

Website yang dirancang untuk sering diperbarui, biasanya melalui halaman backend.

3. Web Interaktif

Website yang memungkinkan interaksi antar pengguna, seperti forum diskusi atau blog dengan moderator untuk mengatur jalannya diskusi [12].

Setiap *website* terdiri dari berbagai halaman yang membentuk keseluruhan situs, halaman utama atau *home page* berada pada posisi teratas dan halaman-halaman lain

yang terkait disebut sebagai *child page*. Halaman halaman ini biasanya berisi *hyperlink* yang menghubungkan satu halaman dengan halaman lainnya di dalam *website* tersebut. Dalam struktur *website*, *home page* berfungsi sebagai pusat informasi utama yang diikuti oleh halaman-halaman terkait lainnya.

Pada sebuah organisasi, *website* memiliki banyak kegunaan untuk menyampaikan informasi, seperti profil perusahaan, visi dan misi, produk maupun data perusahaan lainnya, sistem informasi berbasis *website* ini dijalankan di web server, yang bertujuan untuk memastikan integritas dan keamanan informasi yang disampaikan kepada pengguna [13].



Gambar 2. 3 Cara Kerja *Website* [14]

Gambar 2.3 merupakan gambar dari cara kerja sebuah web, pertama *user* akan mengakses sebuah *website* melalui *web browser*, dilakukan dengan menggunakan URL (*Uniform Resource Location*), selanjutnya *web browser* akan melanjutkan tugasnya dengan mengirimkan *HTTP Request* kepada *web server*, setelah itu *web server* akan memproses permintaan tersebut dan menyiapkan *HTTP Response* yang berisi file atau data yang diminta oleh *user*, namun file web tidak diberikan langsung kepada *user*, melainkan *web server* mengirimkan *HTTP Response* yang berisi informasi atau data yang diperlukan. Setelah itu, *web browser* akan melakukan *rendering* atau menampilkan file yang diterima dalam bentuk halaman web untuk ditampilkan kepada *user*.

Selain itu untuk mendukung kinerja dari sebuah *website*, dibutuhkan aplikasi pada sistem komputer yang berfungsi memberikan pelayanan atas permintaan akses dari komputer pengguna, seperti *FTP Server*, *DHCP Server*, *Mail Server*, *DNS Server*, dan *Database Server*. *Website* juga memiliki beberapa dimensi kualitas, yaitu kualitas sistem (*quality sistem*), kualitas informasi (*information quality*), dan kualitas layanan (*service quality*). Berdasarkan sifatnya, *website* terbagi menjadi dua jenis, *website* statis adalah *website* yang kontennya jarang diperbaru, biasanya menggunakan bahasa pemrograman HTML dan tidak menggunakan *database*, sementara itu *website* dinamis adalah *website* yang kontennya sering berubah dan menggunakan bahasa pemrograman seperti PHP, ASP, NET dan memanfaatkan *database* [8].

Website lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id merupakan *website* dinamis yang dikelola oleh Pemerintah Provinsi Lampung. *Website* lampungprov.go.id menyajikan informasi pemerintahan dan pelayanan publik, sedangkan sigajahkerja.disnaker.lampungprov.go.id digunakan untuk menyediakan informasi ketenagakerjaan, seperti lowongan kerja dan program lainnya. Keduanya diperbarui secara berkala, memanfaatkan sistem berbasis *database*, dan didukung oleh aplikasi sistem komputer untuk memastikan pengelolaan data yang efisien serta akses informasi yang cepat dan akurat bagi pengguna.

2.4 Kerentanan Sistem

Kerentanan sistem merupakan celah atau kelemahan dalam suatu sistem yang memungkinkan ancaman untuk dieksploitasi oleh pihak yang tidak berwenang. Kerentanan ini dapat muncul dalam berbagai bentuk. Ketika ancaman memanfaatkan kerentanan ini, maka akan terjadi potensi kerugian pada sistem, yang bisa berdampak pada integritas, kerahasiaan, dan ketersediaan data. Kerentanan dapat menjadi pintu masuk bagi ancaman yang beragam, baik yang bersifat pasif (mengakses informasi tanpa mengubah sumber daya sistem) maupun aktif (mengubah sumber daya atau mempengaruhi operasi sistem) [15]. Banyak hal yang dapat menyebabkan timbulnya

kerentanan seperti kesalahan dalam perancangan, implementasi, atau logika pengkodean suatu sistem, beberapa kerentanan muncul karena dukungan terhadap bahasa pemrograman tertentu, seperti HTML, CSS, JavaScript dan lain lain yang mungkin memiliki celah keamanan [7]. Semakin banyak kerentanan yang ditemukan dalam suatu sistem, semakin besar juga potensi ancaman yang ada. Peretas atau *hacker* memanfaatkan kerentanan ini melalui eksploitasi yang dirancang khusus untuk celah yang ditemukan, membuka peluang untuk mendapatkan akses ilegal ke sistem. Kerentanan dapat ditemukan baik secara sengaja maupun tidak sengaja [8]. Kerentanan yang paling banyak ditemukan terdapat pada jaringan komputer dan web server, kedua kerentanan ini merupakan isu penting yang perlu mendapatkan perhatian, banyak model kerentanan yang dapat ditemukan seperti *SQL Injection*, *Port Scan Attack*, *Denial of Service* (DoS), *MAC Address Spoofing*, dan juga serangan fisik. Setiap kerentanan akan memiliki dampaknya masing-masing. Untuk mengidentifikasi dan mengatasi kerentanan ini, maka diperlukan lah pengujian untuk kerentanan tersebut sebelum menjadi sebuah masalah serius terhadap suatu sistem.

Kerentanan sistem dapat menjadi celah bagi ancaman yang mengganggu integritas, kerahasiaan, dan ketersediaan informasi pada *website* lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id. Oleh karena itu, penting untuk memahami dan mengidentifikasi kerentanan agar dapat mengantisipasi potensi risiko yang dapat merusak sistem.

2.5 Vulnerability Assessment

Vulnerability Assessment adalah proses mengidentifikasi kerentanan atau celah keamanan yang terdapat pada suatu sistem atau jaringan, proses ini dilakukan menggunakan alat pemindai kerentanan [16]. Proses ini sebaiknya dilakukan secara rutin untuk menemukan dan memperbaiki kerentanan dalam sistem sebelum dapat dieksploitasi oleh penyerang. Dengan melakukan *vulnerability assessment* maka organisasi dapat memahami potensi kelemahan kritis yang dapat mempengaruhi

keamanan sistem secara keseluruhan, mencakup aspek informasi, pengelolaan sistem, konfigurasi, kesadaran keamanan pengguna, serta keamanan fisik [17].

Vulnerability assessment memberikan gambaran terkait kelemahan dalam lingkungan sistem informasi, juga memberikan arahan dalam menilai risiko dan ancaman yang terus berkembang. Proses ini dapat memberikan pemahaman mengenai aset organisasi, sistem keamanan, dan risiko yang dihadapi, serta mengurangi kemungkinan adanya *cybercriminal* yang akan menyerang sistem perusahaan. Maka dari itu *vulnerability assessment* dapat memberikan rekomendasi mitigasi dan remediasi yang tepat untuk mengurangi atau menghilangkan risiko [13].

Kerentanan-kerentanan yang ditemukan dalam *vulnerability assessment* dapat menyebabkan serangan pada sebuah sistem informasi, jenis-jenis serangan yang dapat terjadi karena kerentanan-kerentanan ini adalah

1. *Unauthorized Access*

Merupakan tindakan penyusupan yang dilakukan oleh pelaku secara ilegal dalam jaringan komputer, seperti aktivitas *probing* atau *port scanning*, yang dapat digunakan untuk mencari celah pada sistem [9].

2. *Cyber Espionage, Sabotage and Extortion*

- A. *Cyber Espionage* merupakan tindakan memata-matai suatu target dengan memanfaatkan jaringan internet untuk mengumpulkan informasi, baik mengenai organisasi maupun untuk kesenangan pelaku.

- B. *Sabotage and Extortion* adalah upaya mengganggu, merusak, atau memodifikasi data dan sistem komputer, sehingga aktivitas sistem tersebut tidak dapat berjalan sebagaimana mestinya atau sesuai keinginan pelaku [9].

3. *Sniffing*

Merupakan suatu tindakan pencurian data atau informasi yang dilakukan dengan menangkap paket data yang melewati jaringan tertentu [9].

4. *Defacing*

Merupakan serangan pada *website* atau aplikasi program dengan mengubah konten atau konfigurasi sistemnya. Hal ini dilakukan dengan cara menyisipkan file ke server, biasanya karena adanya celah keamanan yang dimanfaatkan oleh pelaku [9].

5. *Pharming*

Merupakan jenis serangan rekayasa sosial di mana pelaku memanipulasi lalu lintas situs web untuk mencari informasi pengguna atau menyebarkan *malware* melalui situs web palsu [9].

Vulnerability Assessment penting dilakukan terhadap *website* lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id untuk mengidentifikasi potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Pengujian ini memastikan keamanan *website* tetap terjaga sehingga dapat mendukung penyampaian informasi publik secara optimal dan terpercaya.

2.6 *Penetration Testing*

Penetration Testing adalah proses mensimulasikan skenario peretasan secara aman dengan mengeksploitasi kerentanan tanpa memberikan dampak besar pada sistem yang diuji [16]. *Penetration Testing* merupakan pengujian terhadap komponen biner individu maupun aplikasi secara keseluruhan untuk mengetahui apakah terdapat kerentanan intra-komponen atau antar-komponen yang dapat dieksploitasi. Kerentanan tersebut berpotensi mengkompromikan aplikasi, data, atau sumber daya lingkungannya [6].

Menurut National Institute of Standards and Technology (NIST), *penetration testing* merupakan jenis penilaian khusus yang dilakukan pada sistem informasi atau komponen sistem tertentu untuk mengidentifikasi kerentanan yang bisa dimanfaatkan oleh pihak yang berpotensi mengancam (*adversaries*) [18]. Dengan melakukan percobaan eksploitasi terhadap kerentanan yang telah diidentifikasi, pengujian

penetrasi akan memberikan penilaian praktis terhadap langkah-langkah keamanan yang diterapkan oleh organisasi yang akan memungkinkan organisasi untuk memperkuat pertahanan mereka secara proaktif dan melindungi dari potensi serangan [19]. *Penetration Testing* bertujuan untuk mengidentifikasi kelemahan, baik yang terdapat pada sistem komputer, server, aplikasi, ataupun konfigurasi yang tidak tepat. Pengujian ini juga berfungsi untuk melihat dan menilai sejauh mana sebuah sistem dapat bertahan. Tujuan utama dari *penetration testing* adalah mengukur potensi ancaman terhadap sistem serta mengevaluasi dampak yang mungkin timbul terhadap sumber daya dan operasi yang ada [20]. Terdapat tiga jenis pendekatan yang terdapat pada penetration testing, yaitu sebagai berikut :

1. *Black Box Testing*

Pendekatan dimana penguji tidak diberikan informasi apapun mengenai sistem yang akan diuji. Penguji akan mencari dan mengeksploitasi kerentanan dengan menggunakan teknik serangan yang umum digunakan dengan informasi terbatas yang dimiliki [21].

2. *White Box Testing*

Berbeda dengan *black box testing*, penguji memiliki akses penuh terhadap informasi mengenai sistem yang diuji, seperti rincian sistem operasi, alamat IP, serta informasi lainnya. Dengan pendekatan ini, penguji dapat menggunakan pengetahuan tentang sistem untuk mengidentifikasi potensi kerentanan [21].

3. *Grey Box Testing*

Merupakan kombinasi antara *black box* dan *white box*, dimana penguji memiliki informasi terbatas mengenai sistem yang diuji. Pendekatan ini menggabungkan aspek dari kedua pendekatan sebelumnya, yaitu pengujian baik dari sisi internal maupun eksternal sistem untuk mengidentifikasi kerentanan dengan lebih komprehensif [21].

Selain itu, terdapat beberapa metodologi yang dapat digunakan dalam penetration testing, beberapa metodologi yang dapat digunakan adalah sebagai berikut :

1. NIST SP 800-115 *Penetration Testing Methodology*

Merupakan sebuah pedoman teknis yang dikembangkan oleh National Institute of Standards and Technology (NIST) untuk pengujian dan penilaian keamanan informasi. Framework ini memiliki empat fase utama yaitu *planning*, *discovery*, *attack*, dan *report*. Tahapan-tahapan yang ada pada framework ini memberikan panduan tentang bagaimana merencanakan dan melaksanakan penetration testing serta bagaimana mengevaluasi kerentanannya [7].

2. Penetration Testing Execution Standard (PTES)

PTES adalah sebuah framework yang digunakan untuk mengarahkan dan membantu dalam pelaksanaan *penetration testing*. Framework ini mencakup tujuh fase utama : *Pre-engagement*, *Intelligence Gathering*, *Threat Modelling*, *Vulnerability Analysis*, *Exploitation*, *Post-Exploitation*, dan *Reporting*. PTES dirancang untuk memberikan pedoman bagaimana *penetration testing* harus dilakukan [22].

3. OWASP Web Testing Guide (WSTG)

WSTG memberikan panduan komprehensif untuk menguji sistem keamanan pada aplikasi web dan layanan web. WSTG terdiri dari beberapa tahapan yaitu *Information Gathering*, *Configuration and Deployment Management Testing*, *Identify Management Testing*, *Authentication Testing*, *Authorization Testing*, *Session Management Testing*, *Input Validation Testing*, *Testing for Error Handling*, *Testing for Weak Cryptography*, *Business Logic Testing*, dan *Client-Side Testing*, setiap tahapan ini berisi beberapa tes yang harus dilakukan dan akan didokumentasikan lewat WSTG Checklist untuk menilai kerentanan sebuah aplikasi web [23].

4. Open Source Security Testing Methodology Manual (OSSTMM)

Merupakan sebuah framework yang menyajikan metodologi audit keamanan yang luas, mencakup keamanan manusia, fisik, jaringan, dan komunikasi. Framework ini memberikan pendekatan yang komprehensif dan dapat diterapkan untuk memastikan kepatuhan pada standar-standar keamanan seperti PCI-DSS, ISO/IEC 27001, dan ISO/IEC 27005 [22].

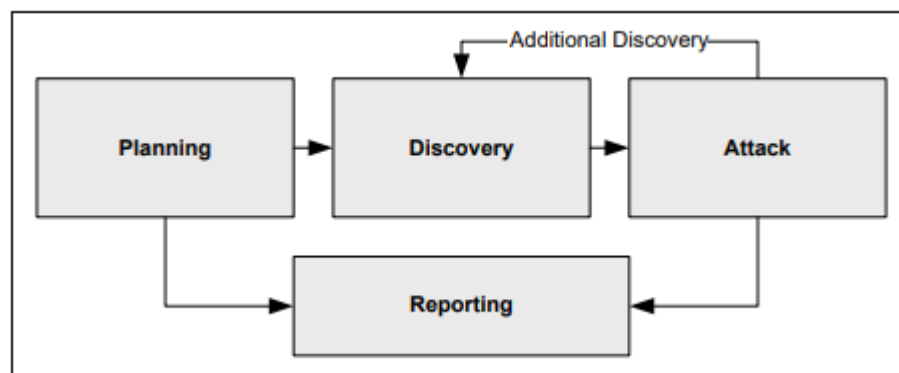
5. Information System Security Assessment Framework (ISAAF)

Merupakan sebuah framework yang lebih berfokus pada penilaian sistem jaringan dan aplikasi. Framework ini memiliki tiga area utama yaitu persiapan, penilaian, dan pelaporan [22].

Penetration Testing penting dilakukan pada *website* lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id untuk membuktikan kelemahan yang teridentifikasi pada pemindaian kerentanan. Pengujian ini dapat mengidentifikasi dampak nyata dari serangan, dengan begitu, hasil pengujian dapat digunakan untuk meningkatkan keamanan *website*, memastikan informasi tetap akurat, dan menjaga kepercayaan masyarakat terhadap layanan pemerintah.

2.7 NIST SP 800-115 *Penetration Testing Methodology*

NIST SP 800-115 merupakan sebuah metodologi pengujian untuk penetration testing yang dikembangkan oleh National Standards and Technology (NIST), adalah sebuah pendekatan yang diperkenalkan oleh badan pemerintah Amerika Serikat. Metode ini sangat efektif untuk digunakan dalam pengujian kerentanan serta proses penetration testing yang dilakukan secara rutin dan dalam jangnan waktu yang relatif singkat [7]. Metodologi NIST SP 800-115 sendiri terdiri dari empat tahapan utama yaitu *planning*, *discovery*, *attack*, dan *report*



Gambar 2. 4 NIST SP 800-115 *Penetration Testing Methodology* [24]

1. *Planning*

Merupakan tahap awal dari proses penetration testing, pada tahap ini ditentukan ruang lingkup pengujian, target pengujian dan tujuan pengujian [25].

2. *Discovery*

Pada tahap ini, dibagi menjadi dua tahapan, tahapan pertama adalah *information gathering*, dimana dilakukan pencarian terkait informasi mengenai sistem, seperti alamat IP, teknologi yang digunakan, dan semua informasi dasar dari target pengujian. Selanjutnya dilakukan *vulnerability scanning*, dimana dilakukan pemindaian kerentanan yang berfungsi untuk mengidentifikasi dan mendeteksi kerentanan yang terdapat pada sistem target, yang akan berfungsi untuk analisis lebih lanjut [25].

3. *Attack*

Pada tahap ini dilakukan analisis dari hasil pemindaian yang sudah dilakukan pada tahap sebelumnya dengan melakukan eksploitasi terhadap sistem target menggunakan alat yang tersedia [25].

4. *Reporting*

Tahapan untuk menyusun hasil dari setiap proses pengujian dan penilaian yang sudah dilakukan [25].

2.8 Tools

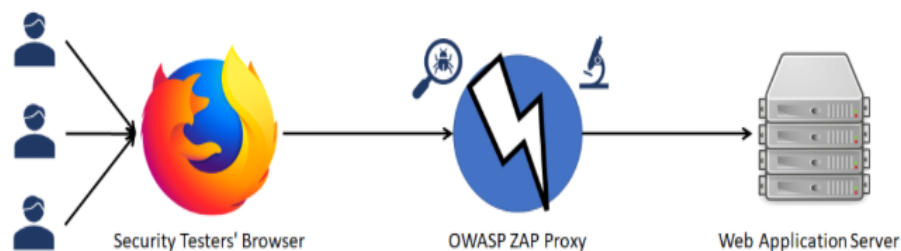
Penelitian ini menggunakan berbagai *tools* yang berperan penting dalam proses pengujian terhadap *website*. *Tools* tersebut terdiri dari perangkat lunak yang mendukung tahap-tahap penelitian. *Tools* yang digunakan pada penelitian adalah sebagai berikut.

2.8.1 OWASP ZAP

OWASP Zed Attacked Proxy (ZAP) merupakan sebuah aplikasi yang digunakan untuk pengujian penetrasi untuk mengidentifikasi kerentanan pada aplikasi web dengan cara

yang mudah. ZAP menawarkan pemindaian otomatis dan juga memungkinkan pengujian manual menggunakan alat khusus untuk mendeteksi kerentanannya[26]. ZAP merupakan sebuah *tools open source* yang dilengkapi dengan API yang sangat kuat, memungkinkan pengguna untuk melakukan hampir semua tindakan yang dapat dilakukan melalui antarmuka *desktop* [5]. Salah satu keunggulan ZAP adalah kemampuannya untuk berfungsi sebagai server proxy, yang memungkinkan pengguna untuk memanipulasi semua lalu lintas yang melewatinya, termasuk lalu lintas yang menggunakan HTTPS [27].

ZAP telah diakui sebagai salah satu yang terbaik dalam mengidentifikasi kerentanan pada aplikasi web. Selain itu, komunitas aktif yang mengembangkan ZAP yaitu OWASP (Open Web Application Security Project) memastikan bahwa ZAP selalu diperbarui dengan fitur keamanan terbaru, dengan berbagai fitur yang ditawarkan, ZAP memungkinkan pengguna melakukan pemindaian secara otomatis dan menghasilkan laporan yang mendetail. Selain itu ZAP juga sangat fleksibel dan dapat diintegrasikan dengan berbagai alat pengembangan dan platform yang ada [27].



Gambar 2. 5 Cara Kerja OWASP ZAP [28]

OWASP ZAP bekerja dengan mengidentifikasi kerentanan dari sebuah *website* dengan langkah-langkah seperti berikut :

1. *Intercepting Proxy*

OWASP ZAP berfungsi sebagai *proxy* server yang akan mengarahkan informasi antara *browser* dan aplikasi web yang akan diuji, sehingga setiap data yang dikirim akan dianalisis oleh OWASP ZAP untuk menemukan masalah keamanan [29].

2. *Crawler*

Setelah melakukan konfigurasi *proxy*, OWASP ZAP akan menggunakan *crawler* untuk mengumpulkan informasi tentang target, *crawler* akan menjelajahi semua halaman yang ada di dalam *website* target dan mengumpulkan data terkait struktur dan konten halaman-halaman. Informasi yang dikumpulkan ini akan digunakan untuk mendeteksi potensi kerentanan pada target [29].

3. Pemindaian Aktif

Setelah semua informasi berhasil dikumpulkan, OWASP ZAP akan melakukan pemindaian aktif menggunakan *scanner* dan akan mengeksplorasi potensi celah keamanan dengan mengirim berbagai permintaan yang mungkin berpotensi mengeksplorasi kelemahan yang ada. Jika sebuah kelemahan terdeteksi, maka OWASP ZAP akan mengeluarkan peringatan dan menunjukkan tingkat risikonya [29].

ZAP menyediakan berbagai fungsi, termasuk memindai permintaan web, merayapi situs web untuk mengidentifikasi file dan direktori, serta mencegah dan memodifikasi lalu lintas web antara *browser* dan server web. Alat ini membantu dalam mengidentifikasi kerentanan seperti *SQL Injection*, autentikasi yang rusak, eksposur data sensitif, konfigurasi yang tidak aman, *Cross-Site Scripting (XSS)*, dan lainnya. Dengan mengotomatisasi deteksi kerentanannya, OWASP ZAP berperan penting dalam mencegah masalah keamanan sebelum menjadi ancaman. OWASP ZAP menawarkan berbagai mode pemindaian, termasuk *Quick Scan*, *Default Scan*, *Attack Scan*, dan *AJAX Spider Mode*, yang masing masing memiliki tujuan khusus dalam pengujian kerentanannya. *Quick Scan* membantu mendeteksi kerentanannya yang umum dan cepat, sedangkan *Default Scan* memberikan penilaian menyeluruh terhadap keamanan aplikasi web. *Attack Scan* berfokus pada mengeksplorasi potensi kelemahan untuk melakukan verifikasi ketahanan aplikasi, dan *AJAX Spider Mode* yang dirancang khusus untuk menguji aplikasi web dinamis menggunakan AJAX [29].

2.8.2 Oracle VM Virtual Box

Oracle Virtual Box merupakan sebuah aplikasi yang memungkinkan penggunanya untuk menjalankan beberapa sistem operasi pada perangkat yang sama dengan membuat mesin virtual atau VM. Aplikasi ini dirancang untuk memanfaatkan inovasi dalam arsitektur x86. Arsitektur x86 merupakan desain prosesor yang dikembangkan oleh intel, yang sekarang banyak digunakan di berbagai perangkat komputer modern seperti laptop dan PC. Standar ini mendukung berbagai inovasi perangkat keras, sehingga memberikan performa optimal saat menjalankan sistem operasi di perangkat keras. Oracle VM Virtual Box mendukung virtualisasi dengan teknologi KVM [30]. Aplikasi ini memungkinkan pengguna menjalankan beberapa sistem operasi seperti Microsoft Windows, Mac OS X, Linux, dan Oracle Solaris secara bersamaan, aplikasi ini dirancang untuk melakukan pengujian, pengembangan, demonstrasi, dan penerapan solusi lintas platform [31].

Meskipun tampilannya sederhana, Virtual Box memiliki mesin virtualisasi yang sangat cepat dan kuat, fitur-fitur seperti *paravirtualization*, *bidirectional drag-and-drop*, dan enkripsi citra disk menjadikan Virtual Box sebuah solusi virtualisasi desktop yang unggul. Virtual Box menyediakan lingkungan aman dengan enkripsi untuk menjaga kerahasiaan data dalam mesin virtual, baik untuk penyimpanan lokal maupun berbasis *cloud* [31]

2.8.3 Kali Linux

Kali Linux merupakan sistem operasi berbasis Debian yang dikenal memiliki kekuatan luar biasa dalam bidang keamanan. Berbeda dengan banyak sistem operasi lainnya yang memerlukan instalasi alat-alat keamanan secara manual, Kali Linux sudah dilengkapi dengan berbagai program *built-in* yang dirancang khusus untuk pengujian penetrasi dan keamanan. Alat alat canggih seperti Nmap, Metasploit, Aircrack-ng tersedia di dalam distribusi ini, yang membuat Kali Linux menjadi salah satu pilihan utama para peneliti dan profesional di bidang keamanan [32].

Kali Linux dirilis pertama kali pada Maret 2013 dan dikembangkan oleh Khaled Baoween, Mati Aharoni, dan Devon Kearns. Kali Linux sendiri kompatibel dengan berbagai perangkat keras, termasuk platform x86, ARM, dan Android, serta tersedia melalui Windows Subsystem for Linux (WSL) pada windows 10[33]. Selain itu Kali Linux juga menawarkan fleksibilitas dengan antarmuka grafis dan baris perintah, keamanan Kali Linux sendiri dijaga dengan menggunakan model pengembangan berbasis repositori yang aman, menjamin integritas dari *tool-tool* yang digunakan. Kali Linux bersifat *open source* dan komunitas Kali Linux yang aktif membuat Kali Linux menjadi salah satu sumber daya utama di dunia keamanan [32].

2.8.4 Ping

Ping merupakan sebuah alat untuk menguji konektivitas suatu host di jaringan Protokol Internet (IP). Ping akan mengirimkan pesan berupa ICMP ECHO_REQUEST kepada host tujuan dan akan menunggu balasan berupa ICMP ECHO_RESPONSE, melalui pengujian ping, beberapa informasi penting dapat diperoleh, antara lain sebagai berikut:

1. Mengetahui apakah host tujuan aktif dan dapat dijangkau.
2. Mengukur waktu yang diperlukan paket untuk pergi ke host tujuan dan kembali lagi (*round-trip time*).
3. Menghitung tingkat kehilangan paket yang terjadi.

Hasil dari pengujian ping akan memberikan gambaran tentang jumlah paket yang dikirim dan diterima, tingkat kehilangan paket, serta statistik mengenai waktu bolak-balik, termasuk waktu rata-rata, minimum, dan maksimum [34].

2.8.5 Whois

Whois merupakan sebuah *tools* untuk mengumpulkan informasi yang digunakan untuk mengidentifikasi data unik dari sebuah sistem, whois berguna dalam pengumpulan

informasi awal mengenai domain atau alamat IP dengan cara mengakses *database* yang menyimpan informasi terkait registrasi domain dan alamat jaringan. Whois menjadi salah satu alat pertama yang digunakan dalam tahap pengumpulan informasi, dengan menjalankan perintah whois pada alamat IP target, informasi yang didapatkan bisa mencakup tanggal registrasi, nama jaringan, informasi orang yang mendaftarkan, hingga informasi lain yang relevan. Informasi yang dikumpulkan oleh whois sangat penting karena dapat memberikan gambaran mengenai lokasi, organisasi yang bertanggung jawab atas alamat IP tersebut, serta kontak yang dapat dihubungi. Data seperti nama kota, provinsi, kode pos, hingga negara dari target juga dapat diungkap oleh *tools* ini [35].

2.8.6 Whatweb

Whatweb adalah alat yang digunakan untuk mengidentifikasi berbagai aspek dari sebuah *website*, seperti sistem manajemen konten (CMS), *platform blogging*, *JavaScript*, *web server*, dan perangkat yang digunakan. Selain itu, whatweb juga dapat menampilkan informasi lain, seperti alamat email, nomor versi, ID akun, modul kerangka kerja web, dan kesalahan SQL. Whatweb bekerja dengan mengirimkan permintaan HTTP ke sebuah *website* dan menganalisis *response* yang diterima dari server. Whatweb akan mengidentifikasi berbagai aspek *website* dan menganalisis header, HTML, *JavaScript*, dan elemen halaman lainnya. Berdasarkan informasi yang didapatkan tersebut, whatweb akan menghasilkan laporan yang menyediakan rincian tentang teknologi yang digunakan [36].

2.8.7 WhatWaf

WhatWaf merupakan sebuah *tools* yang digunakan untuk mendeteksi *firewall* yang digunakan pada sebuah aplikasi *website* dengan tujuan untuk mengetahui apakah situs web dilindungi oleh Web Application Firewall (WAF). *Tools* ini bekerja dengan cara mendeteksi *firewall* yang ada pada sebuah situs *website* dengan mencoba melakukan

bypass terhadap *firewall* tersebut. WhatWaf sendiri memiliki berbagai fitur, seperti mendeteksi lebih dari 40 jenis *firewall*, dan dapat mencoba lebih dari 20 teknik pemalsuan untuk menghindari deteksi *firewall*. Selain itu WhatWaf juga memiliki kemampuan untuk secara otomatis menentukan protokol ke HTTP atau memaksa menggunakan HTTPS, serta menyediakan encoder untuk mengenkripsi *payload* ke dalam *bypass* yang ditemukan [37].

2.8.8 Nmap

Nmap merupakan singkatan dari “Network Mapper”, merupakan sebuah *tool open-source* yang dapat digunakan untuk penemuan jaringan dan audit keamanan. Nmap menggunakan paket IP mentah untuk menentukan host yang tersedia di jaringan. Nmap digunakan untuk memindai port dan mengetahui port mana yang terbuka pada host[19]. Nmap juga dapat menentukan layanan yang ditawarkan oleh host yang tersedia, termasuk nama dan versi aplikasi yang digunakan, sistem operasi yang berjalan atau filter paket yang digunakan. Nmap dikenal sebagai alat yang fleksibel, mudah digunakan, kuat, gratis, dan populer. Fitur utama dari Nmap sendiri meliputi penemuan host, pemindaian port, deteksi layanan, dan identifikasi sistem operasi [38].

Pada Nmap, tabel port dapat disajikan dengan daftar nomor port dan protokol, nama layanan, serta status dari port tersebut, Status port dapat berupa terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak difilter (*unfiltered*)[39]. Nmap menawarkan berbagai mode pemindaian, termasuk pemindaian TCP SYN, ACK, UDP, yang masing-masing dirancang untuk mendeteksi perilaku jaringan yang berbeda [40].

2.8.9 Burp Suite

Burp Suite pertama kali dikembangkan pada tahun 2004 oleh Dafydd Stuttard yang melihat adanya kebutuhan akan alat pengujian keamanan aplikasi web yang handal. Sejak itu, Burp Suite mengalami perkembangan pesat dan menambahkan berbagai fitur

baru yang bermanfaat untuk pengujian keamanan. Saat ini, Burp Suite telah menjadi salah satu alat utama yang digunakan untuk pengujian keamanan aplikasi web. Pengujian manual dalam keamanan aplikasi sangat bergantung pada dua hal utama, yaitu kemampuan penguji dan alat yang digunakan, Burp Suite merupakan salah satu alat yang mendukung untuk melakukan pengujian manual ini. Burp Suite sendiri menawarkan fleksibilitas dan keandalan yang memungkinkan penguji untuk dengan mudah mengidentifikasi serta mengeksploitasi kerentanan yang ada. Burp Suite menggabungkan kedua pendekatan dalam pengujian yaitu manual dan otomatis yang memungkinkan penguji untuk mengoptimalkan hasil pengujian dengan lebih efektif dan efisien [41].

Burp Suite Professional merupakan versi berbayar yang menyediakan fitur lengkap untuk pengujian keamanan aplikasi web secara menyeluruh. Versi ini mendukung otomatisasi pengujian, pemindaian kerentanan, serta alat lanjutan seperti *Intruder* penuh, *Scanner*, dan Burp *Collaborator*. Selain alat dasar seperti *proxy* dan *repeater*, versi ini juga memungkinkan eksploitasi dan deteksi kerentanan kompleks secara efisien dan akurat dalam proses pengujian keamanan.

2.9 OWASP Top 10 2021

OWASP Top 10 2021 adalah daftar yang dirilis oleh Open Web Application Security Project (OWASP), sebuah organisasi yang berfokus pada keamanan perangkat lunak. Daftar ini mencakup 10 kerentanan yang paling kritis dan umum ditemukan di perangkat lunak, daftar ini diperbarui secara berkala untuk mencerminkan perubahan dalam ancaman keamanan perangkat lunak. Sejak pertama kali dirilis pada tahun 2004, OWASP Top 10 telah mengalami beberapa perubahan, seperti pada 2007, 2010, 2013, dan 2017. Setiap pembaruan mencerminkan perubahan ancaman dalam keamanan perangkat lunak dan memperkenalkan kerentanan baru yang relevan.



Gambar 2. 6 OWASP Top 10 2021 List [42]

Versi terbaru adalah OWASP Top 10 2021, yang mencakup perubahan yang signifikan terkait ancaman di dunia maya dan memberikan pembaruan mengenai kerentanan. Daftar ini memberikan panduan penting untuk mengidentifikasi dan memilih alat penilaian kerentanan yang sesuai, dengan parameter yang telah ditentukan agar alat dapat menguji sesuai kerentanannya. Berikut adalah daftar dari OWASP Top 10 2021

Tabel 2. 1 Penjelasan OWASP Top 10 2021 [43]

Top 10 ID	Name of Vulnerability Items	Explanation
A01:2021	<i>Broken Access Control</i>	Setelah sebelumnya berada di posisi kelima, <i>Broken Access Control</i> kini naik ke posisi pertama, dengan 94% aplikasi yang diuji menunjukkan adanya masalah ini dalam berbagai bentuk. Akses kontrol merupakan aturan yang mengatur bahwa pengguna hanya bisa melakukan aksi sesuai izin yang diberikan. Kegagalan kontrol ini bisa mengakibatkan pengaksesan informasi yang tidak sah, modifikasi data, atau pelanggaran batasan fungsi bisnis yang diperbolehkan

		untuk sebuah <i>user</i>. Contoh serangan bisa terjadi jika pengguna yang tidak terautentikasi dapat mengakses halaman <i>admin</i>, atau jika pengguna <i>non-admin</i> bisa mengakses halaman yang seharusnya hanya bisa diakses oleh <i>admin</i>, yang halaman yang seharusnya hanya bisa diakses oleh <i>admin</i>, yang jelas merupakan celah keamanan yang besar
A02:2021	<i>Cryptographic Failure</i>	Celah ini mengacu pada masalah yang lebih spesifik terkait dengan kegagalan dalam penggunaan kriptografi atau ketidakhadirannya, yang berujung pada paparan data sensitif. Contoh data yang sering menjadi sasaran adalah nomor kartu kredit, kata sandi, catatan medis, informasi pribadi, serta rahasia bisnis, yang semuanya membutuhkan perlindungan ekstra untuk menjaga kerahasiaannya.
A03:2021	<i>Injection</i>	<i>Injection</i> terjadi ketika data yang tidak terpercaya dikirimkan ke <i>interpreter</i> kode melalui formulir <i>input</i> atau metode lain dalam <i>website</i>. Sebagai contoh, seorang hacker bisa memasukkan kode SQL ke dalam formulir yang seharusnya hanya menerima data teks biasa. Jika formulir tersebut tidak dilindungi dengan

		baik, maka kode SQL tersebut dapat dieksekusi, memungkinkan akses yang tidak sah ke <i>database</i> .
A04:2021	<i>Insecure Design</i>	<i>Insecure design</i> merupakan kategori baru dalam OWASP Top 10 2021 yang menyoroti risiko yang muncul akibat masalah pada desain dan arsitektur sistem. Kategori ini mencakup penerapan pemodelan ancaman, penggunaan pola desain yang lebih aman, serta referensi arsitektur yang lebih baik. Desain yang tidak aman mengacu pada berbagai kelemahan yang disebabkan oleh kurangnya atau tidak efektifnya kontrol pada tahap perancangan sistem.
A05:2021	<i>Security Misconfiguration</i>	Sebuah sistem dianggap rentan terhadap kesalahan konfigurasi keamanan jika tidak memiliki perlindungan yang memadai atau <i>hardening</i> keamanan yang dibutuhkan di seluruh lapisan sistem. Selain itu, fitur-fitur yang tidak diperlukan masih aktif atau terinstal, seperti port, layanan, halaman, akun, atau privilege yang tidak digunakan.
A06:2021	<i>Vulnerable and Outdated Components</i>	Kerentanan terhadap komponen yang usang dan kadaluarsa bisa terjadi jika pengelola sistem tidak mengetahui versi semua komponen yang digunakan, baik

		di sisi <i>client</i> maupun server. Selain itu, kerentanan ini juga bisa muncul akibat kurangnya pemeliharaan rutin, termasuk pemindaian kerentanan secara berkala
A07:2021	<i>Identification and Authentication Failures</i>	Kerentanan yang sebelumnya dikenal sebagai <i>Broken Authentication</i> turun ke posisi tujuh, setelah sebelumnya berada di urutan kedua. Kategori kerentanan ini mencakup kelemahan pada sistem <i>login</i> yang memungkinkan peretas mendapatkan akses ke pengguna. Selain itu, peretas juga bisa menguasai seluruh sistem dengan meretas akun <i>admin</i> .
A08:2021	<i>Software and Data Integrity Failures</i>	Kegagalan integritas data dan perangkat lunak merupakan kategori baru pada tahun 2021 yang menyoroti masalah terkait pembaruan perangkat lunak, data kritis, dan <i>pipeline CI/CD</i> yang tidak memverifikasi integritas. Kerentanan ini terjadi ketika kode dan infrastruktur tidak dapat mencegah pelanggaran integritas. Contoh kasusnya adalah objek atau data yang telah disterialisasi dalam struktur yang dapat diakses dan dimodifikasi oleh penyerang.
A09:2021	<i>Security Logging and Monitoring Failures</i>	Kegagalan dalam keamanan <i>logging</i> dan <i>monitoring</i> adalah kategori yang penting untuk mendeteksi, meningkatkan, dan merespons terhadap potensi

		pelanggaran yang sedang berlangsung. Oleh karena itu, pencatatan dan pemantauan menjadi aspek yang cukup rumit dalam proses pengujian, karena biasanya memerlukan tindakan seperti wawancara atau bertanya apakah serangan telah terdeteksi selama pengujian dilakukan.
A10:2021	<i>Server-Side Request Forgery (SSRF)</i>	Kerentanan SSRF (<i>Server-Side Request Forgery</i>) terjadi ketika sebuah sistem web melakukan permintaan sumber daya jarak jauh tanpa memvalidasi URL yang diberikan oleh pengguna. Hal ini bisa dimanfaatkan oleh penyerang untuk memaksa aplikasi mengirimkan permintaan yang telah dimanipulasi ke alamat yang tidak diinginkan. Aplikasi web saat ini sering menyediakan fitur yang memudahkan pengguna, sehingga permintaan alamat URL menjadi hal yang umum. Oleh karena itu, insiden SSRF semakin meningkat, terutama karena layanan <i>cloud</i> dan kompleksitas arsitektur <i>cloud</i> yang semakin berkembang.

2.10 Penelitian Terkait

Kesamaan studi kasus dan penggunaan metode dalam pengembangan sistem adalah beberapa hal yang dapat dijadikan referensi untuk penelitian ini. Berikut adalah beberapa artikel atau jurnal ilmiah yang relevan dengan penelitian ini

1. Vippalapalli Vikas, G. Saisri, T. Sai Meghara, A. Sree Harshini, G. Kaveri dalam penelitiannya yang berjudul “*Web Security Audit and Penetration Testing : Identitying Vulnerabilities and Strengthening*” pada tahun 2023. Metode yang digunakan pada penelitian ini adalah *security assessment* yang memiliki beberapa tahapan yaitu identifikasi kerentanan, eksploitasi kerentanan, dan pelaporan, *tools-tools* yang digunakan pada penelitian ini adalah Nmap, Burp Suite, Dirbuster dan Dirb. Hasil dari penelitian ini menunjukkan adanya kerentanan dengan kategori sebagai berikut : 0 kerentanan *high*, 2 *medium*, 4 *low*, dan 4 *informational*. Kerentanan yang diidentifikasi dalam penelitian ini meliputi celah keamanan umum seperti *Cross-Site Scripting (XSS)*, *SQL Injection*, dan akses tidak sah ke direktori atau file tersembunyi yang ditemukan. Dengan hasil tersebut, penelitian ini memberikan panduan untuk mitigasi risiko dan meningkatkan keamanan aplikasi web [19]. (Internasional)
2. Yazeed Alkhurayyif dan Yazeed Saad Almarshady dalam penelitiannya yang berjudul “*Adopting Automated Penetration Testing Tools : A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations*”. Penelitian ini menggunakan metode *Automated Penetration Testing* dan *tools-tools* yang digunakan adalah ZAP, Nessus, dan Nmap. Penelitian ini fokus pada identifikasi kerentanan. Hasil dari penelitian ini menunjukkan bahwa ZAP dan Nmap lebih berguna untuk melakukan penilaian kerentanan pada *website* dan jaringan dan menunjukkan bahwa *tools* otomatis dapat digunakan dan efektif untuk proses keamanan yang berkelanjutan dan membantu dan meningkatkan siklus pengujian [6]. (Internasional)

3. Ancy Valentina S, Vishwashri S, Rajadurai T, dan Sharad SR dalam penelitiannya yang berjudul “*Finding Vulnerabilities in Web Application By Using Penetration Testing*”. Pada penelitian ini dilakukan *vulnerability assessment* menggunakan automation tools, tahapan dari penelitian ini adalah *reconnaissance, vulnerability scanning, gaining access, exploitation, post-exploitation*, dan *reporting*. Pada penelitian ini digunakan *tools* seperti OWASP ZAP dan mengimplementasikan kode python, pada penelitian ini dihasilkan temuan-temuan kerentanan seperti *SQL Injection, Cross Site Scripting (XSS)*, autentikasi yang tidak aman, dan lain lain sehingga membantu pemilik aplikasi untuk proaktif dalam mengatai masalah keamanan [44]. (Internasional)
4. Nagendran K, Adithyan A, Chethana R, Camilius p, Bala Sri Varshini K B dalam penelitiannya yang berjudul “*Web Application Penetration Testing*”. Penelitian ini menggunakan metode *penetration testing* yang dibagi menjadi beberapa tahapan yaitu *reconnaissance, scanning, exploitation, maintaning acces and privilege escalation*, dan *clearing tracks and reporting*. *Tools* yang digunakan pada penelitian ini adalah Nmap, Nikto, w3AF dan Acunetix, dari penelitian ini ditemukan beberapa kerentanan yang dilakukan percobaan untuk eksploitasi yaitu *SQL Injection, Cross-Site Scripting, Cross Site Request Forgery, Cross Origin Resource Sharing* yang terdapat pada target [45]. (Internasional)
5. Dhruv Mitesh Mori, Kiran R Dodiya, Akash Khnunt, Divya Patel dalam penelitiannya yang berjudul “*Shield and Swords : Navigating Vulnerability Assessment and Penetration Testing*” , penelitian ini menggunakan metode *vulnerability assessment and penetration testing*, penelitian ini mendapatkan beberapa kerentanan seperti *SQL Injection* menggunakan *tools SQL Map, OTP Bypass* yang didapatkan menggunakan *tools Burp Suite, Email Bypass* yang didapatkan menggunakan Burp Suite, *Clickjacking* yang dieksploitasi menggunakan baris kode HTML, *Clear Text PasswordSubmission* yang ditemukan menggunakan Burp Suite, *Directory Traversal*, dan HTML

Injection. Semua kerentanan yang ditemukan dibuktikan dengan pembuktian konseptual pada penelitian ini[46].

6. Mulya Akmal dalam penelitiannya yang berjudul “Analisis dan Uji Coba Tingkat Keamanan *Website* UIN Ar-Raniry Menggunakan ACUNETIX *Web Vulnerability Scanner*”. Metode yang digunakan pada penelitian ini adalah *vulnerability assessment* dengan pendekatan deksriptif analisis, alat yang digunakan dalam melakukan penelitian adalah Acunetix *Web Vulnerability Scanner*. Dalam penelitian tersebut digunakan Acunetix sebagai alat pemindai kerentanan aplikasi web sebanyak sepuluh kali untuk melihat dan menghasilkan hasil yang akurat. Hasil dari penelitian ini adalah ditemukannya kerentanan dengan nilai *high 0, medium 2, Low 4*, dan *4 informational*, serta diberikannya strategi mitigasi yang dapat digunakan untuk mengatasi kelemahan-kelemahan pada aplikasi web tersebut [47]. (National)
7. Esti Zakia Darajat, Eko Sedyono, dan Irwan Sembiring dalam penelitiannya yang berjudul “*Vulnerability Assessment Website e-Government* dengan NIST SP 800-115 dan OWASP Menggunakan *Web Vulnerability Scanner*”. Metode yang digunakan dalam penelitian ini adalah kuantitatif deskriptif dengan pedoman NIST SP 800-115 untuk mengetahui tingkat keamanan *website* E-Government Pemerintah daerah Kabupaten Semarang dan Desa Gunung Tumpeng. Alat yang digunakan untuk pemindaian adalah Acunetix dan Pentest-Tools, pada penelitian ini dilakukan pemindaian terhadap dua aplikasi web dengan hasil pemindaian terhadap *website* Kabupaten Semarang berlangsung selama 4 menit 21 detik menggunakan Acunetix dan mendapatkan 1 kerentanan *medium*, 2 kerentanan *low*, dan 2 kerentanan berjenis *informational*, sedangkan menggunakan Pentest-Tools berlangsung selama 12 detik dengan waktu persiapan 30 menit dan menghasilkan 1 kerentanan dengan skor *medium*, 7 *low*, dan 11 *informational*. Sedangkan pada *website* milik Desa Gunung Tumpeng pemindaian menggunakan Acunetix berlangsung dengan waktu 6 jam 24 menit dan menghasilkan 1 kerentanan dengan nilai *medium*, 2 *low*, dan 2 *informational*, sementara pemindaian menggunakan Pentest-Tool

berjalan selama 18 detik dengan waktu persiapan 45 menit, menghasilkan 1 kerentanan dengan nilai *medium*, 7 *low*, dan 11 *informational*. Semua kerentanan ini akan dicocokkan dengan OWASP Top 10 [17]. (National)

8. Muhammad Abdul Muin, Kapti, dan Tri Yusranto pada penelitiannya yang berjudul “*Campus Website Security Vulnerability Analysis Using Nessus*” Pada penelitian ini digunakan metode *vulnerability assessment*, dan tolak ukur dari nilai kerentanan menggunakan CVSS V2.0. Alat yang digunakan dalam penelitian ini adalah Nessus Vulnerability Scanner, dilakukan pemindaian terhadap *website* milik STMIK Bina Patria menggunakan alat ini dan menghasilkan. Hasil dari penelitian ini adalah ditemukan beberapa kerentanan pada setiap *website* dengan tingkat kerentanan yang beragam, terdapat tiga *website* yang memiliki kerentanan terbanyak, web pertama memiliki kerentanan sebanyak 14. Sementara kerentanan dengan tingkat sedang terbanyak ada pada web ke dua dengan persentase sebanyak 22%. Rata-rata kerentanan yang dihasilkan setelah melakukan pemindaian berasal dari Server DNS yang lemah [48]. (Internasional)
9. Fauzan Prasetyo Eko Putra, Ubaidi, Amir Hamzah, Walid Agel Pramadi, dan Alief Nuraini dalam penelitiannya yang berjudul “*Systematic Literature Review : Security Gap Detection On Websites Using OWASP ZAP*”. Penelitian ini menggunakan metode penelitian literatur dengan pendekatan proaktif dan sistematis dan dilakukan secara iteratif. Pada penelitian ini alat atau pemindai yang digunakan adalah OWASP ZAP untuk mendeteksi kerentanan keamanan pada aplikasi web dengan kerentanan yang terdeteksi adalah *SQL Injection*, *Misconfiguration*, dan *Exposure of Sensitive Data*. Hasil dari penelitian ini membuktikan bahwa OWASP ZAP efektif dalam mendeteksi kerentanan seperti *SQL Injection*, *Misconfiguration*, dan *Exposure of Sensitive Data*, penggunaan OWASP ZAP dapat meningkatkan keamanan aplikasi web secara signifikan [27]. (Nasional)
10. Diah Priyawati, Siti Rokhmah, dan Ihsan Cahyo Utomo dalam penelitiannya yang berjudul “*Website Vulnerability Testing and Analysis of Internet*

Management Information System Using OWASP". Penelitian ini menggunakan metode *penetration testing* dengan pendekatan *grey box penetration testing*, *tools* yang digunakan pada penelitian ini adalah OWASP ZAP, Penelitian ini berhasil menemukan 12 kerentanan pada *website* aplikasi pengelolaan internet Kragan, Karanganyar, dari 12 kerentanan tersebut, ditemukan 1 kerentanan *high*, 5 *medium*, 4 *low*, dan 2 *informational*. Pada penelitian ini dilakukan *reporting* dengan hanya memasukkan kerentanan yang mengacu atau berpotensi untuk menghasilkan serangan yang masuk ke dalam daftar OWASP Top 10 [49]. (Internasional)

11. Naufal Athif Syarifudin, dan Lila Setiyani dalam penelitiannya yang berjudul "*Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method*". Penelitian ini menggunakan metode *vulnerability assessment* yang meliputi langkah-langkah *footprinting*, *vulnerability scanning*, dan *vulnerability analysis*. *Tools* yang digunakan pada penelitian ini adalah zenmap, whois, wappalyzer, OWASP ZAP. Dari penelitian ini didapatkan 11 kerentanan pada sistem target dengan 5 kerentanan bernilai *medium*, dan 6 kerentanan bernilai *low* yang mana kerentanan-kerentanan yang dihasilkan memiliki potensi untuk memicu serangan yang lebih besar dan lebih berbahaya [50].

Penelitian-penelitian terkait sebelumnya dijadikan pendukung kesahihan dan juga keterkaitan dengan penelitian yang akan dilakukan, selain itu penelitian sebelumnya dijadikan sebagai referensi yang memberikan landasan teori dan metodologi yang relevan terhadap penelitian. Penelitian-penelitian terkait dijadikan sebuah acuan dikarenakan beberapa alasan.

Pertama, penggunaan metodologi yang serupa dan relevansi *tools* atau alat yang digunakan, beberapa penelitian yang dikaji menggunakan metode yang serupa dengan penelitian yang akan dilakukan, beberapa penelitian juga menggunakan *tools* yang sama dengan yang akan digunakan pada penelitian yaitu OWASP ZAP sebagai alat untuk melakukan pemindaian, sehingga membantu memberi

referensi dalam penyusunan metode dan proses melakukan pemindaian pada penelitian.

Kedua, beberapa penelitian memiliki fokus yang sama yaitu pengujian keamanan pada *website* pemerintahan, penelitian ini relevan dijadikan referensi dikarenakan memeberikan wawasan dan pengalaman dalam menerapkan metodologi yang sesuai untuk menilai kerentanan, yang sangat berguna untuk penelitian yang akan dilakukan.

Keempat, analisis kerentanan dengan menggunakan berbagai metode pendekatan, pendekatan mendalam yang digunakan pada penelitian terkait dapat dijadikan referensi sehingga membantu menyusun strategi analisis yang terstruktur, dengan adanya referensi dari penelitian terkait ini maka dapat memberikan panduan untuk mengidentifikasi kerentanan dan menyusun mitigasi yang tepat.

III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian tugas akhir ini dilaksanakan pada bulan Desember 2024 – Maret 2025. Penelitian ini dilaksanakan di Dinas Komunkasi Informatika dan Statistik Provinsi Lampung yang berada di JL. WR Monginsidi No.69 Kota Bandar Lampung. Berikut adalah tabel yang menunjukkan jadwal kegiatan penelitian yang dilakukan.

Tabel 3. 1 Timeline Penelitian

No.	Kegiatan.	2024	2025						
		Bulan	Bulan						
		12	1	2	3	4	5	6	7
1	<i>Planning</i>								
2	<i>Information Gathering</i>								
3	<i>Vulnerability Scanning</i>								
4	<i>Penetration Testing</i>								
5	<i>Generating Report</i>								
6	Penyusunan Laporan								

3.2 Alat dan Bahan Penelitian

Adapun alat dan bahan dalam penelitian ini adalah sebagai berikut

Tabel 3. 2 Alat dan Bahan Penelitian

No	Perangkat	Spesifikasi	Deskripsi
1.	Laptop	ASUS TUF GAMING FX 506 IH, Processor Intel Core i5-10300, RAM 24 GB, ROM 512 GB, Sistem Operasi Windows 11	Perangkat keras utama dalam penelitian
2.	Virtual Box	Versi 6.1, sistem operasi host windows, macOS, Linux, Solaris, Memori minimal 4GB RAM, Penyimpanan kosong minimal 20 GB, Jaringan NAT, Bridged Adapter, Internal Network, Host-Only Adapter	Perangkat lunak virtualisasi <i>open-source</i> untuk menjalankan sistem operasi tamu di dalam mesin virtual pada perangkat fisik
3.	Kali Linux	Virtualization : Oracle, Operating System : Kali GNU/ Linux Rolling, Kernel : Linux 6.1.0-kali0-amd64, Architecture : x86-64	Sistem operasi tamu yang dijalankan melalui virtual box untuk menjalankan alat-alat pemindaian.
4.	OWASP ZAP	Dukungan protokol : HTTP, HTTPS, Web Sockets, Antarmuka Pengguna : GUI, CLI. REST API, Bahasa : Java	Alat <i>open-source</i> untuk mengidentifikasi kerentanan dalam aplikasi web.
5.	Ping	Jenis : Command-line Network Diagnostic Tools, Protoko : ICMP	Alat sederhana yang digunakan untuk

			memverifikasi konektivitas jaringan antara dua perangkat di jaringan.
6.	Whois	Versi : 5.5.17	Alat yang digunakan untuk melakukan pencarian informasi terkait dengan domain atau alamat IP.
7.	WhatWeb	Versi : 0.5.5	Alat yang digunakan untuk melakukan pengumpulan informasi terkait teknologi web yang digunakan.
8.	Whatwaf	Interface : command-line Interface	Alat yang digunakan untuk melakukan identifikasi perlindungan WAF yang diterapkan pada situs web
5.	Nmap	Versi : 7.93, Platform : x86_64-pc-linuxx-gnu	Perangkat lunak yang berfungsi untuk melakukan pemindaian dan eksplorasi port

6.	Burp Suite		Perangkat lunak yang mampu memodifikasi jalur lalu lintas data.
7.	Microsoft Word		Perangkat lunak untuk menulis dan melaporkan hasil pengujian

3.3 Objek Penelitian

Penelitian ini dilakukan terhadap dua *website* milik Pemerintah Provinsi Lampung dengan domain lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id. Pengujian dilakukan dari sisi eksternal, tanpa akses langsung terhadap infrastruktur internal, sehingga simulasi dilakukan menyerupai skenario serangan dari pihak luar. Seluruh tahapan pengujian dilaksanakan menggunakan jaringan pribadi milik peneliti, bukan melalui jaringan internal milik Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Berdasarkan informasi yang diperoleh dari pihak terkait, diketahui bahwa server fisik yang menjalankan kedua *website* tersebut berada di lingkungan kantor Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung. Penjelasan lebih lanjut mengenai masing-masing *website* dapat dilihat pada uraian berikut.

3.3.1 lampungprov.go.id

Keamanan *website* lampungprov.go.id memegang peranan kritis sebagai tulang punggung layanan publik dan informasi pemerintahan di Provinsi Lampung. Berdasarkan hasil wawancara dengan penanggung jawab dari *website* lampungprov.go.id, diperoleh informasi bahwa sebagai domain utama (*parent domain*), *website* ini menjadi pusat bagi berbagai sub domain strategis yang

mendukung layanan penting seperti aplikasi keuangan daerah, absensi, layanan kesehatan, serta berbagai macam sistem administrasi lainnya, ketika terjadi serangan siber pada *parent* domain ini, seluruh sub domain yang bergantung akan terhenti operasionalnya. Dampak sistemik ini dapat berlangsung dalam jangka waktu yang signifikan apabila instansi terkait gagal memulihkan sistem sesuai tenggat waktu yang telah ditentukan oleh Kementerian terkait. Dalam kondisi ini, pihak berwenang dapat memutuskan untuk menonaktifkan *parent* domain, dan semua sub domain pun akan ikut dinonaktifkan.

Berdasarkan hasil wawancara yang dilakukan dengan penanggung jawab dari *website* lampungprov.go.id dan *browsing* secara pribadi di internet, diperoleh informasi bahwa situs resmi milik pemerintah sering menjadi target utama serangan dunia maya dalam bentuk manipulasi konten. Pelaku serangan siber sering memodifikasi konten halaman *website* menjadi tampilan yang mengarahkan pengguna ke situs perjudian daring. Aksi ini memanfaatkan celah keamanan pada sistem, dengan tujuan untuk mengelabui pengguna dan mendistribusikan konten yang dilarang oleh regulasi di Indonesia, mengingat akses langsung terhadap situs perjudian telah dibatasi oleh pemerintah. Serangan-serangan ini dapat mengganggu tiga pilar utama yang harus ada pada sebuah *website* yaitu CIA *Triad* yang wajib dijaga. Penanggung jawab *website* lampungprov.go.id memberikan informasi dalam wawancara yang dilakukan, bahwa dalam rentang seminggu terakhir (19 Januari 2025 – 25 Januari 2025) terdapat tiga belas juta kali percobaan serangan terhadap *website* ini dalam berbagai macam bentuk serangan. Selain itu, audit keamanan yang tidak dilakukan secara rutin dapat membuka potensi serangan yang lebih besar terhadap *website* ini, serta penelitian ini termasuk pada tahapan pra insiden yang dapat mencegah sebuah serangan terhadap *website* sebelum menimbulkan dampak yang lebih besar.



Gambar 3. 1 Halaman Utama Website lampungprov.go.id [51]



Gambar 3. 2 Halaman Beranda Website lampungprov.go.id [51]

3.3.2 sigajahkerja.disnaker.lampungprov.go.id

Website sigajahkerja.disnaker.lampungprov.go.id merupakan sebuah sistem informasi berbasis web yang dapat digunakan oleh masyarakat Provinsi Lampung, khususnya parap pencari kerja, untuk melakukan proses pendaftaran, pembuatan akun, serta melamar pekerjaan secara daring. Melalui platform ini, pengguna dapat mengisi data pribadi seperti nama lengkap, nomor induk kependudukan (NIK), tempat dan tanggal lahir, alamat, jenis kelamin, agama, hingga provinsi domisili. Selain itu, website ini juga mengharuskan pengguna untuk mengunggah dokumen penting seperti ijazah

terakhir, sertifikat kompetensi, serta berkas pendukung lainnya yang diperlukan dalam proses rekrutmen.

Website ini dikembangkan oleh Dinas Tenaga Kerja Provinsi Lampung bekerja sama dengan Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik) sebagai bentuk transformasi layanan ketenagakerjaan berbasis digital. Tidak hanya menyediakan akses bagi pencari kerja, *website* ini juga menjadi sarana bagi instansi-instansi maupun perusahaan swasta, maupun penyedia kerja lainnya untuk mempublikasikan lowongan pekerjaan secara resmi dan terpusat.

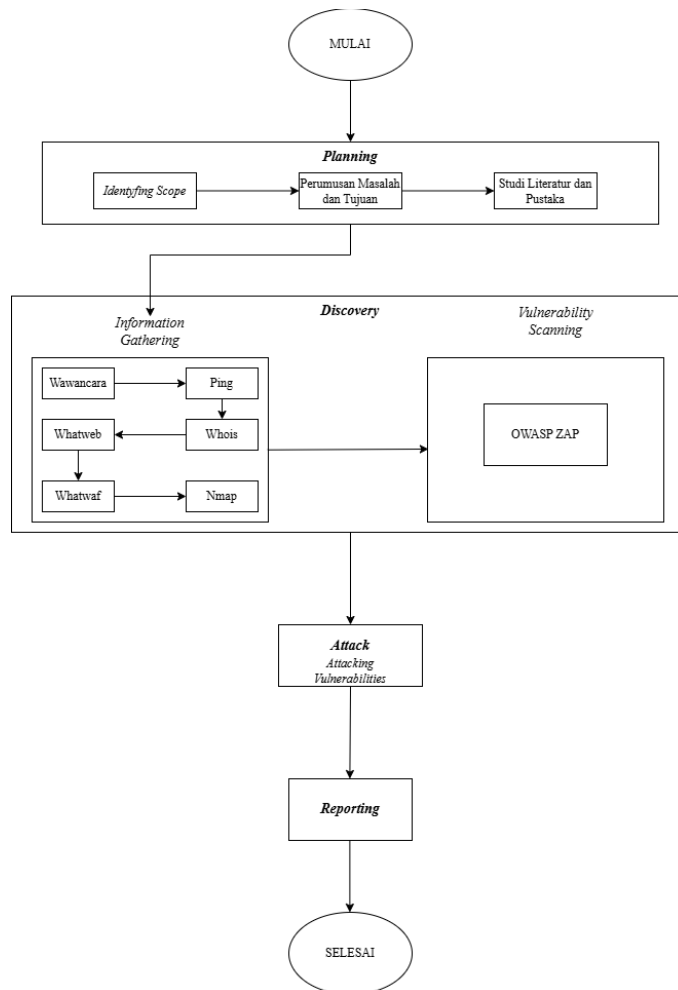
Diketahui bahwa sistem ini menyimpan dan mengelola informasi bersifat sensitif yang mencakup data identitas, riwayat pendidikan, dan dokumen resmi milik warga negara. Oleh karena itu, *website* ini ditetapkan sebagai objek penelitian karena tingginya kebocoran data serta dampak yang ditimbulkan jika terjadi serangan terhadap sistem. Selain itu, diketahui hingga saat ini, *website* tersebut belum pernah dilakukan pengujian keamanan secara menyeluruh, sehingga keamanannya belum dapat dipastikan secara objektif. Hal ini menjadi urgensi penggunaan *website* ini sebagai objek penelitian. Dengan demikian, penelitian ini dilakukan dalam konteks pra-insiden guna memberikan rekomendasi preventif demi menjaga integritas, kerahasiaan, dan ketersediaan layanan publik berbasis digital yang disediakan oleh pemerintah daerah.



Gambar 3. 3 Tampilan Halaman Beranda *Website* sigajahkerja.disnaker.lampungprov.go.id

3.4 Tahapan Penelitian

Tahapan penelitian ini terdiri dari beberapa tahapan yang dimulai dari *planning*, *discovery*, *attack*, dan *reporting* dimana setiap tahapannya memiliki tahap yang berbeda beda seperti pada diagram dibawah ini yang menjelaskan setiap alur dari penelitian yang akan dilakukan. Diagram ini menjadi dasar dan pedoman bagaimana penelitian dilakukan secara sistematis dan terarah sehingga hasil yang didapatkan dari penelitian ini sesuai dengan tujuan yang diharapkan.



Gambar 3. 4 Tahapan Penelitian

3.4.1 *Planning*

Tahapan pertama dalam penelitian ini adalah *planning* atau perencanaan. Pada tahap ini dilakukan beberapa kegiatan sebelum memasuki tahap berikutnya, yaitu identifikasi ruang lingkup atau *identyfing scope*. Kegiatan yang dilakukan dalam tahap ini meliputi identifikasi permasalahan, penentuan tujuan, studi literatur, dan penyusunan proposal penelitian.

Penelitian ini mengidentifikasi masalah terkait kerentanan pada aplikasi web yang diuji menggunakan pendekatan *Black Box Testing* dengan metodologi NIST SP 800-115. Masalah yang dihadapi oleh organisasi terhadap sebuah *website* adalah menjaga keamanan aplikasi web yang diidentifikasi melalui pengujian keamanan menggunakan teknik *penetration testing*. Pengujian ini dilakukan dengan menganalisis aplikasi web secara menyeluruh untuk menemukan potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Penilaian atau pemindaian dilakukan menggunakan alat OWASP ZAP, yang akan mendeteksi berbagai kerentanan pada *website*. *Penetration Testing* dilakukan dengan menggunakan beberapa *tools* yang akan disesuaikan dengan hasil temuan pada pemindaian sebelumnya.

Tujuan utama penelitian ini adalah untuk mengidentifikasi dan membuktikan kerentanan pada *website* yang diuji menggunakan OWASP ZAP untuk mengidentifikasi kerentanannya, sesuai dengan metodologi NIST SP 800-115 dengan pendekatan *Black Box Testing*, penelitian ini bertujuan memberikan gambaran yang jelas mengenai potensi ancaman pada *website* yang diuji serta menyediakan rekomendasi langkah-langkah mitigasi yang sesuai untuk mengatasi kerentanan tersebut.

Kebutuhan Fungsional :

1. Kemampuan OWASP ZAP untuk mendeteksi kerentanan
2. Kemampuan untuk melakukan pemindaian otomatis
3. Laporan hasil pengujian yang jelas dan terstruktur
4. Integrasi dengan sistem manajemen resiko

Kebutuhan Non-Fungsional

1. Keandalan pengujian
2. Konsumsi daya yang efisien
3. Keamanan dan kerahasiaan data
4. Kompatibilitas dengan berbagai platform

Studi literatur dilakukan untuk mempelajari dan memahami berbagai referensi yang relevan pelaksanaan *penetration testing* dengan metodologi NIST SP 800-115, alat OWASP ZAP, serta pengujian keamanan aplikasi web. Dari studi tersebut, dipilih pendekatan *Black Box Security Testing* yang cocok untuk penelitian ini, di mana pengujian dilakukan tanpa akses ke kode sumber aplikasi. Selain itu, dilakukan juga pemilihan referensi yang mendalami kerentanan yang termasuk dalam OWASP Top 10 2021, yang mana daftar ini sejalan dengan alat yang digunakan yaitu OWASP ZAP, dikarenakan berasal dari satu sumber yang sama yaitu OWASP (Open Web Application Security Project) yang mana akan memastikan bahwa pengujian mencakup ancaman yang paling signifikan terhadap aplikasi web.

Setelah melakukan identifikasi masalah, penetapan tujuan, dan studi literatur, proposal penelitian ini disusun untuk memberikan dasar teoritis dan metodologis dalam melaksanakan penelitian dimana terdapat tinjauan pustaka sebagai dasar teoritis dalam menjalankan penelitian. Pada akhir tahap ini, disusunlah proposal untuk melaksanakan penelitian.

3.4.2 Discovery

Tahap *discovery* merupakan langkah penting dalam melakukan *penetration testing*, dimana aktivitas ini bertujuan untuk mengumpulkan informasi dan mengidentifikasi potensi kerentanan pada *website* yang akan diuji. Dalam penelitian ini, tahap *discovery* dibagi menjadi dua tahapan yaitu *information gathering* dan *vulnerability scanning*.

3.4.2.1 *Information Gathering*

Tahapan ini dilakukan untuk mendapatkan data dan informasi awal mengenai target aplikasi *website* yang diuji. Sebelum melakukan proses *information gathering* menggunakan beberapa *tools*, dilakukan wawancara terlebih dahulu dengan penanggung jawab dari *website* yang menjadi target pengujian. Setelah itu dikumpulkan informasi dari *website* menggunakan beberapa *tools*. Informasi tersebut mencakup aspek teknis terkait infrastruktur, teknologi yang digunakan, serta potensi titik lemah yang dapat dimanfaatkan. Proses pengumpulan informasi dilakukan menggunakan beberapa *tools* berikut :

1. Ping

Digunakan untuk memverifikasi konektivitas jaringan antara perangkat pengujian dengan server target

2. Whois

Digunakan untuk mendapatkan informasi terkait domain, seperti pemilik domain, server DNS, tanggal pendaftaran domain, penyedia layanan, dan beberapa informasi teknis lainnya.

3. WhatWeb

Digunakan untuk mendeteksi teknologi yang digunakan dalam pengembangan aplikasi web, seperti *framework*, server web, atau sistem manajemen konten (CMS)

4. WhatWaf

Digunakan untuk mengidentifikasi keberadaan dan jenis *Web Application Firewall (WAF)* yang digunakan oleh target.

Hasil dari tahap ini akan memberikan wawasan awal mengenai struktur target aplikasi web, sehingga membantu penentuan strategi pengujian lebih lanjut

3.4.2.2 *Vulnerability Scanning*

Setelah tahap *information gathering*, langkah berikutnya adalah melakukan pemindaian menggunakan *tools* OWASP ZAP. *Tools* ini berfungsi untuk memindai aplikasi *website* secara otomatis guna mendeteksi *website* secara otomatis untuk mendeteksi adanya kerentanan keamanan yang terdapat pada *website* target, atau konfigurasi keamanan yang tidak memadai. Pemindaian ini bertujuan untuk mengidentifikasi potensi kerentanan yang ada secara sistematis, sehingga dapat digunakan sebagai dasar untuk tahapan eksploitasi yang lebih mendalam. OWASP ZAP akan bekerja dengan cara menganalisis struktur aplikasi *website*, termasuk parameter dan *endpoint* untuk menemukan kerentanan yang mungkin terdapat pada *website*.

Tahapan *discovery* secara keseluruhan memberikan gambaran menyeluruh terhadap potensi kerentanan pada aplikasi web yang diuji. Informasi dan hasil pemindaian yang diperoleh pada tahap ini akan digunakan untuk mendukung pengujian lebih lanjut pada tahap eksploitasi.

3.4.3 *Attack*

Tahap ini merupakan tahap melakukan *penetration testing* dengan cara melakukan eksploitasi pada sistem target, eksploitasi dalam penelitian ini dilakukan setelah kerentanan berhasil diidentifikasi pada tahap *discovery*. Tahap ini bertujuan untuk menguji kerentanan yang ditemukan dan membuktikan bahwa kerentanan tersebut benar-benar ada. Proses ini dilakukan sebagai bentuk *Proof of Concept (PoC)* untuk menunjukkan potensi celah keamanan yang ditemukan. Dengan melakukan eksploitasi, fokus utama adalah untuk membuktikan kerentanan yang sudah diidentifikasi sebelumnya dan mengamati kerentanannya. Semua aktivitas eksploitasi dilakukan dengan cara yang aman dan terkendali, dengan tujuan untuk memberikan gambar yang jelas tentang potensi risiko dan ancaman yang mungkin timbul dari kerentanan yang ditemukan, tanpa merusak data atau fungsionalitas sistem yang diuji.

3.4.4 Reporting

Pada tahap *reporting*, semua temuan yang diperoleh selama proses *discovery* dan eksploitasi akan didokumentasikan dengan detail. Laporan ini mencakup deskripsi rinci mengenai kerentanan yang ditemukan, termasuk tingkat keparahannya, cara kerentanannya dapat dimanfaatkan, dan potensi dampaknya terhadap sistem. Selain itu, pada tahap ini disajikan rekomendasi langkah-langkah mitigasi yang perlu diambil untuk mengatasi kerentanan yang teridentifikasi, dengan tujuan untuk meningkatkan keamanan aplikasi web yang diuji. Laporan ini disusun secara jelas dan sistematis agar dapat dipahami dengan mudah oleh pihak terkait, seperti pengembang, pemangku kebijakan, untuk segera melakukan perbaikan yang diperlukan.

V. KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan penelitian *Vulnerability Assessment* dan *Penetration Testing* yang telah dilakukan pada dua *website* target, yaitu *website* lampungprov.go.id dan sigajahkerja.disnaker.lampungprov.go.id, dapat disimpulkan beberapa hal sebagai berikut :

- 1 Penggunaan metodologi NIST SP 800-115 dan OWASP ZAP terbukti mampu mengarahkan proses pengujian secara sistematis dan menghasilkan temuan kerentanan yang valid. Metodologi ini menyediakan alur terstruktur pada setiap tahap pengujian, mulai dari *planning* hingga *reporting*, sedangkan OWASP ZAP terbukti efektif dalam mendukung proses pendeteksian kerentanan dengan baik. Kombinasi keduanya menghasilkan hasil yang efektif pada proses evaluasi keamanan kedua *website*
- 2 Berdasarkan hasil pengujian, kerentanan yang ditemukan menunjukkan kondisi keamanan pada kedua *website* secara umum berada dalam kategori baik, namun masih terdapat beberapa aspek teknis yang perlu ditindaklanjuti. Masing-masing *website* memiliki 1 kerentanan dengan tingkat *high*, 4 *medium*, dan 8 *low*. Beberapa kerentanan *medium* berhasil dieksploitasi, sedangkan kerentanan *high* tidak berhasil dieksploitasi. Temuan ini menunjukkan bahwa tingkat risiko kerentanan perlu dianalisis bersama konteks teknis sistem yang diuji. Jenis kerentanan yang paling banyak ditemukan berkaitan dengan kategori OWASP Top 10 2021, khususnya *Security Misconfiguration* dan *Vulnerable and Outdated Components*.

- 3 Hasil pengujian menunjukkan bahwa penguatan sistem keamanan perlu difokuskan pada konfigurasi internal dan pengelolaan komponen yang digunakan. Meskipun lapisan proteksi awal seperti Cloudflare mampu menyembunyikan infrastruktur dari proses *reconnaissance*, kelemahan seperti tidak diterapkannya *header* keamanan, penggunaan pustaka rentan, serta celah pada input *handling* masih ditemukan dan dapat dimanfaatkan. Hal ini menunjukkan perlunya pemeliharaan sistem secara berkala dan evaluasi menyeluruh terhadap kebijakan konfigurasi dan komponen yang digunakan.

5.2 SARAN

A. Bagi Pengelola *Website*

1. Melakukan optimalisasi konfigurasi keamanan sistem.
2. Melaksanakan pengujian keamanan secara berkala.
3. Meningkatkan pemahaman dan prosedur keamanan internal.
4. Menjalin komunikasi yang lebih erat dengan tim penguji keamanan untuk memberikan izin pengujian yang lebih luas dalam batas aman, guna memungkinkan eksploitasi lanjut tanpa merusak sistem

B. Bagi Peneliti Selanjutnya

1. Mengembangkan aspek eksploitasi lebih lanjut.
2. Melakukan pengujian keamanan menggunakan pendekatan *white-box* atau *grey-box security testing* untuk memperoleh gambaran yang lebih menyeluruh terkait kerentanan pada sistem.
3. Mengintegrasikan perhitungan tingkat kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS) untuk menghitung dan menganalisis tingkat risiko dari kerentanan yang ditemukan.
4. Melakukan pengujian dengan menyertakan teknik *social engineering* yang fokus pada sisi Sumber Daya Manusia sebagai bagian dari pengujian keamanan.

INDEKS

—

`_gid, _ga`

Cookie yang digunakan oleh Google Analytics untuk melacak pengunjung situs.,
109

A

ACK

Acknowledgment, pemindaian untuk menentukan status firewall menggunakan
paket ACK., 27

AJAX Spider Mode

Mode pemindaian yang digunakan untuk menjelajahi aplikasi web berbasis AJAX
guna menemukan halaman tersembunyi., 23

anycast routing

Teknik routing di mana satu alamat IP dialokasikan ke banyak lokasi yang berbeda
untuk efisiensi dan keandalan., 73

API

Application Programming Interface, antarmuka pemrograman aplikasi yang
memungkinkan sistem berkomunikasi atau bertukar data, 22, 41, 135

Attack Scan

Pemindaian lanjutan yang mencoba mengeksploitasi kerentanan yang ditemukan
sebelumnya., 23

B

bidirectional

Komunikasi dua arah antara dua entitas atau sistem., 24

C

Cache Poisoning

Teknik serangan di mana cache sistem DNS diisi dengan informasi palsu untuk mengarahkan trafik., 83

CIDR

Classless Inter-Domain Routing, format pengalamatan IP dengan notasi slash (/) untuk menentukan blok alamat IP., 59, 61

cloud

Infrastruktur komputasi yang disediakan melalui internet dengan sumber daya yang elastis., 24, 33

CMS

Content Management System, perangkat lunak untuk membuat dan mengelola konten website., 26, 50, 63

cookies

Data kecil yang disimpan browser untuk menyimpan informasi sesi atau preferensi pengguna., 133

CVE

Common Vulnerabilities and Exposures, sistem identifikasi standar untuk kerentanan keamanan yang telah terdokumentasi., 136, 145

D

Database Server

Server yang menyimpan dan mengelola data dalam sistem basis data, biasanya diakses oleh aplikasi atau sistem lain., 14

Default Scan

Pemindaian yang menggunakan konfigurasi standar dari alat keamanan tanpa kustomisasi lanjutan., 23

Denial of Service (DoS)

Serangan yang bertujuan membuat layanan sistem menjadi tidak tersedia dengan membanjiri trafik atau permintaan., 15

DHCP Server

Server yang secara otomatis memberikan alamat IP dan konfigurasi jaringan kepada perangkat dalam jaringan., 14

DNS Server

Server yang menerjemahkan nama domain menjadi alamat IP., 14

DNS Spoofing

Serangan di mana penyerang memalsukan data DNS untuk mengarahkan pengguna ke situs palsu., 83

drag-and-drop

Fitur antarmuka pengguna yang memungkinkan pemindahan elemen dengan cara menyeret dan meletakkannya., 24

E

endpoint

Titik akhir komunikasi antara klien dan server dalam jaringan atau API., 51, 100, 106, 125

F

FTP Server

Server yang menyediakan layanan pengiriman dan pengambilan file melalui protokol File Transfer Protocol., 14

I

input handling

Proses menerima, memvalidasi, dan memproses masukan dari pengguna., 132

interpreter

Program yang menjalankan perintah dalam bahasa pemrograman baris per baris tanpa kompilasi., 30

K**KVM**

Kernel-based Virtual Machine, teknologi virtualisasi berbasis kernel Linux., 24

L*load balancing*

Distribusi trafik ke beberapa server agar beban merata dan layanan tetap optimal., 73

M*MAC Address Spoofing*

Pemalsuan alamat MAC perangkat agar terlihat seperti perangkat lain di jaringan., 15

Mail Server

Server yang bertugas mengelola pengiriman, penerimaan, dan penyimpanan email., 14

malware

Perangkat lunak berbahaya yang dirancang untuk merusak atau mengakses sistem tanpa izin., 17, 104, 118, 134, 143

Man-in-the-Middle

Serangan di mana pelaku memotong atau mengubah komunikasi antara dua pihak tanpa sepengetahuan mereka., 140, 141, 149, 150

O*obfuscation*

Teknik penyamaran kode atau data agar sulit dibaca atau dianalisis, sering digunakan dalam malware., 151

open source

Perangkat lunak dengan kode sumber terbuka yang dapat digunakan, dimodifikasi, dan dibagikan secara bebas., 22, 25

Origins AS

Identitas jaringan otonom (Autonomous System/AS) asal yang mengumumkan rute IP tertentu dalam sistem routing global internet., 59, 61

output encoding

Teknik pengamanan dengan mengubah karakter berbahaya agar tidak dapat dieksekusi sebagai skrip., 93

P

paravirtualization

Teknologi virtualisasi di mana sistem tamu mengetahui bahwa ia berjalan dalam lingkungan virtual., 24

payload

Kode atau data yang dibawa oleh serangan, biasanya untuk dijalankan atau dieksekusi pada target., 27, 93, 94, 97, 98, 99, 105, 106, 108, 110, 115, 116, 119, 120, 131, 152, 153, 154, 158

phising

Teknik penipuan untuk memperoleh informasi sensitif dengan menyamar sebagai entitas terpercaya, 89, 115, 129

PHPSESSID

Cookie identifikasi sesi PHP yang menyimpan ID sesi pengguna., 109

pipeline CI/CD

Rangkaian proses otomatis yang digunakan dalam integrasi dan pengiriman perangkat lunak secara berkelanjutan, 32

platform blogging

Sistem yang memungkinkan pengguna membuat, mengelola, dan menerbitkan artikel atau tulisan di web., 26

plugin

Komponen tambahan yang memperluas fungsi perangkat lunak utama., 63

Port Scan Attack

Teknik pemindaian port untuk menemukan layanan yang terbuka pada suatu sistem., 15

Proof of Concept.

Demonstrasi sederhana bahwa suatu kerentanan dapat dieksploitasi secara nyata., 87, 88

Q

query

Permintaan data yang dikirim ke sistem basis data atau sistem informasi lainnya., 77, 93

Quick Scan

Jenis pemindaian jaringan atau sistem dengan waktu singkat dan cakupan terbatas., 23

S

server-side processing

Proses pengolahan data yang dilakukan di sisi server, bukan di sisi klien., 93, 94, 97

Session Hijacking

Teknik penyerangan dengan mengambil alih sesi pengguna aktif untuk mengakses sistem secara ilegal., 109, 110

session identifier

Penanda unik untuk membedakan sesi pengguna dalam aplikasi web., 109

SQL Injection

Teknik serangan di mana penyerang menyisipkan perintah SQL ke dalam input aplikasi untuk mengakses atau memodifikasi database., 2, 15, 23, 34, 35, 37

SYN

Synchronize, teknik pemindaian jaringan menggunakan paket SYN untuk mendeteksi layanan aktif tanpa menyelesaikan koneksi., 27, 77

T

TCP

Transmission Control Protocol, pemindaian menggunakan protokol TCP untuk mendeteksi port yang terbuka., 27, 79, 81, 84

timestamp

Penanda waktu yang menunjukkan kapan suatu peristiwa terjadi dalam sistem komputer., 142, 151

U

UDP

User Datagram Protocol, pemindaian menggunakan protokol UDP untuk menemukan layanan tidak terproteksi., 27

W

whitelist IP

Metode keamanan dengan hanya memperbolehkan alamat IP tertentu mengakses sistem., 136

X

XSRF-TOKEN

Token keamanan untuk melindungi aplikasi dari serangan Cross-Site Request Forgery (CSRF)., 109, 110

DAFTAR PUSTAKA

- [1] E. Novianto, E. I. Heri Ujianto, and R. Rianto, “Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Kepegawaian Dengan Defense in Depth,” *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 1–6, 2023, doi: 10.35508/jicon.v11i1.9139.
- [2] International Telecommunication Union (ITU), “Individuals Using the Internet,” International Telecommunication Union (ITU). Accessed: Jan. 06, 2025. [Online]. Available: <https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/>
- [3] L. Choirunnisa, T. H. C. Oktaviana, A. A. Ridlo, and E. I. Rohmah, “Peran Sistem Pemerintah Berbasis Elektronik (SPBE) Dalam Meningkatkan Aksesibilitas Pelayanan Publik di Indonesia,” *Sosio Yust. J. Huk. dan Perubahan Sos.*, vol. 3, no. 1, pp. 71–95, 2023, doi: 10.15642/sosyus.v3i1.401.
- [4] S. Yaakub *et al.*, *Pengantar Sistem Informasi Pt. Mifandi Mandiri Digital*, 1st ed. Medan: PT. Mifandi Mandiri Digital Redaksi:, 2022.
- [5] H. Setiawan, L. E. Erlangga, and I. Baskoro, “Vulnerability Analysis Using the Interactive Application Security Testing (IAST) Approach for Government X Website Applications,” *2020 3rd Int. Conf. Inf. Commun. Technol. ICOIACT 2020*, pp. 471–475, 2020, doi: 10.1109/ICOIACT50329.2020.9332116.
- [6] Y. Alkhurayyif and Y. Saad Almarshdy, “Adopting Automated Penetration Testing Tools,” *J. Inf. Secur. Cybercrimes Res.*, vol. 7, no. 1, pp. 51–66, 2024, doi: 10.26735/rjrt2453.
- [7] W. A. Tya, “Uji Kerentanan Pada Website Menggunakan Open Web Application Security Project (OWASP) Top 10 Tahun 2021 Studi Kasus

- (Domain uinjkt.ac.id),” pp. 1–78, 2023, [Online]. Available: [https://repository.uinjkt.ac.id/dspace/bitstream/123456789/75009/1/WAHYU ADI TYA-FST.pdf](https://repository.uinjkt.ac.id/dspace/bitstream/123456789/75009/1/WAHYU%20ADI%20TYA-FST.pdf)
- [8] M. Yaqi, *Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal* 2023. [Online]. Available: [https://repository.uinjkt.ac.id/dspace/handle/123456789/73422%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/73422/1/MUHAMMAD YAQI-FST.pdf](https://repository.uinjkt.ac.id/dspace/handle/123456789/73422%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/73422/1/MUHAMMAD%20YAQI-FST.pdf)
- [9] Irfan Murti Raazi, Ima Dwitawati, and Putri Nabila, “Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh,” *JINTECH J. Inf. Technol.*, vol. 4, no. 1, pp. 1–15, 2023, doi: 10.22373/jintech.v4i1.2409.
- [10] I. F. Agustina, *Buku Ajar Pengantar Sistem Informasi*, 1st ed., no. January. Surakarta: PT. Sonpedia Publishingn Indonesia, 2024. doi: 10.21070/2024/978-623-464-086-1.
- [11] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim),” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.
- [12] A. O. SARI, A. Abdillah, and Sunarti, *Web Programming I*, 1st ed. Jakarta: Graha Ilmu, 2022. doi: 10.1201/9781003316244-11.
- [13] R. Efendi *et al.*, “Uji kerentanan keamanan pada aplikasi berbasis web menggunakan metode Vulnerability Assessment,” vol. 21, no. 1, pp. 44–57, 2024, doi: <https://doi.org/10.24246/aiti.v21i1.44-57>.
- [14] R. J. Hosting, “Cara Kerja Website dan Fungsinya yang Perlu Kamu Tahu,” Jagoan Hosting. Accessed: Jan. 06, 2025. [Online]. Available:

<https://www.jagoanhosting.com/blog/cara-kerja-website/>

- [15] T. I. I. I. Year and I. I. Sem, *Digital Notes on Cyber Security(R18a0521) Department of Information Technology*, vol. 2. 2021.
- [16] V. K. Velu, *Mastering Kali Linux for Advanced Penetration Testing*, 4th ed. Birmingham: Packt Publishing Ltd., 2022.
- [17] E. Z. Darojat, E. Sedyono, and I. Sembiring, “Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner,” *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.
- [18] K. Božić, N. Penevski, and S. Adamović, “Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods,” no. January, pp. 229–234, 2019, doi: 10.15308/sinteza-2019-229-234.
- [19] 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, 2023, doi: 10.22214/ijraset.2023.54658.
- [20] R. Vallabhaneni and V. Veeramachaneni, “Understanding Penetration Testing for Evaluating Vulnerabilities and Enhancing Cyber Security Understanding Penetration Testing for Evaluating Vulnerabilities and Enhancing Cyber Security,” no. October, 2024, doi: 10.47191/etj/v9i10.12.
- [21] M. Alhamed and M. M. H. Rahman, “A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions,” *Appl. Sci.*, vol. 13, no. 12, 2023, doi: 10.3390/app13126986.
- [22] D. Collins, “Pen Testing Framework for IoT Devices MSc Research Project Cyber Security,” National College of Ireland, 2021.
- [23] OWASP, “OWASP Web Security Testing guide Version 4.2,” The OWASP

- Foundation. [Online]. Accessed: Jan. 07, 2025. Available: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/
- [24] NIST SP 800-115, “Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology,” *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2020, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800>
- [25] F. Mambo *et al.*, “Evaluasi Keamanan Website dengan Menggunakan Metode NIST SP,” vol. 3, 2024, doi: <https://doi.org/10.58192/populer.v3i4.2805>.
- [26] Riyan Farismana and Dian Pramadhana, “Vulnerability Assessment Untuk Analisis Tingkat Keamanan Pada Sistem Informasi Repositori Karya Ilmiah Politeknik Negeri Indramayu,” *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 1, pp. 26–33, 2023, doi: [10.55606/jutiti.v3i1.2208](https://doi.org/10.55606/jutiti.v3i1.2208).
- [27] F. P. E. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, and A. Nuraini, “Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap,” *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 348–355, 2024, doi: [10.47709/brilliance.v4i1.4227](https://doi.org/10.47709/brilliance.v4i1.4227).
- [28] Prabhu Vignesh Kumar Rajagopal, “OWASP ZAP – Zed Attack Proxy and its Features,” Digital Varys. Accessed: Jan. 12, 2025. [Online]. Available: <https://digitalvarys.com/owasp-zap-proxy/>
- [29] L. Q. Huy, “A Study in Advanced Methods for Website Security: Application of Tor and OWASP Zed Attack Proxy,” Oulu University of Applied Sciences, 2023. [Online]. Available: <https://www.theseus.fi/handle/10024/805570>
- [30] R. Pandey, “Comparing vmware fusion, oracle virtualbox, parallels desktop implemented as type-2 hypervisors,” *Natl. Coll. Irel.*, no. September, 2020, doi: [10.13140/RG.2.2.17080.78087](https://doi.org/10.13140/RG.2.2.17080.78087).
- [31] Oracle, “Oracle VM VirtualBox Overview,” 2021. Accessed: Jan. 15, 2025.

- [Online]. Available: <https://www.oracle.com/assets/oracle-vm-virtualbox-overview-2981353.pdf>
- [32] A. P. Walidin, F. P. Putri, and D. Kiswanto, “KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI,” vol. 9, no. 1, pp. 1188–1196, 2025, doi: <https://doi.org/10.36040/jati.v9i1.12661>.
- [33] Z. Bin Akhtar and A. T. Rawol, “Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective,” *Int. J. Adv. Network, Monit. Control.*, vol. 9, no. 2, pp. 11–22, 2024, doi: [10.2478/ijanmc-2024-0012](https://doi.org/10.2478/ijanmc-2024-0012).
- [34] Linux-Console.net, “Cara Menggunakan Perintah Ping di Linux dengan Contohnya.” Accessed: Jan. 07, 2025. Accessed: Jan. 15, 2025. [Online]. Available: <https://id.linux-console.net/?p=6853#gsc.tab=0>
- [35] M. Al Ismaili, *Enhancing Cybersecurity: Exploring Effective Ethical Hacking Techniques with Kali Linux*, vol. 5, no. November. 2023. doi: [10.9734/bpi/ratmcs/v5/6403e](https://doi.org/10.9734/bpi/ratmcs/v5/6403e).
- [36] “WhatWeb,” Morning Star Security. Accessed: Jan. 16, 2025. [Online]. Available: <https://morningstarsecurity.com/research/whatweb>
- [37] Do Son, “WhatWaf v1.9 releases: Detect & bypass web application firewalls and protection systems,” Security Online Info. Accessed: Jan. 16, 2025. [Online]. Available: <https://securityonline.info/whatwaf/>
- [38] K. Chhillar and S. Shrivastava, “University Computer Network Vulnerability Management using Nmap and Nexpose,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 6, pp. 3084–3090, 2021, doi: [10.30534/ijatcse/2021/021062021](https://doi.org/10.30534/ijatcse/2021/021062021).
- [39] S. Dwiyatno, “Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap,” *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 2, pp. 108–115, 2020, doi: [10.30656/prosisko.v7i2.2522](https://doi.org/10.30656/prosisko.v7i2.2522).
- [40] A. Singh, E. S. Sharma, B. K. Reddy, P. Soni, S. S. Ghuman, and U. S. Gill,

- “Automated Network Vulnerability Assessment with Nmap: A Comprehensive Approach,” *Proc. - 2024 2nd Int. Conf. Adv. Comput. Commun. Technol. ICACCTech* 2024, pp. 208–214, 2024, doi: 10.1109/ICACCTech65084.2024.00043.
- [41] S. Rahalkar, *Guide to Burp Suite*. Maharashtra: Apress, 2021. doi: <https://doi.org/10.1007/978-1-4842-6402-7> ISBN-13.
- [42] M. Hell, “OWASP Top 10, 2021 Edition: 10 things you need to know,” *debricked.com*. [Online]. Accessed: Jan. 17, 2025. Available: <https://debricked.com/blog/owasp-top-10-2021-edition/>
- [43] OWASP, “OWASP Top Ten,” *owasp.org*. Accessed: Jan. 17, 2025. [Online]. Available: <https://owasp.org/www-project-top-ten/>
- [44] A. Valentina, V. S., R. T., and S. S. R. -, “Finding Vulnerability in Web Application by using Pentesting,” *Int. J. Multidiscip. Res.*, vol. 6, no. 4, pp. 1–8, 2024, doi: 10.36948/ijfmr.2024.v06i04.24517.
- [45] K. Nagendran, A. Adithyan, R. Chethana, P. Camillus, and K. B. Bala Sri Varshini, “Web application penetration testing,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 1029–1035, 2019, doi: 10.35940/ijitee.J9173.0881019.
- [46] K. Dodiya, “Shields and Swords : Navigating Vulnerability Assessment and Penetration,” no. October, 2024, doi: 10.15680/IJIRCCE.2024.1210013.
- [47] Mulya Akmal, “Analisis Dan Uji Coba Tingkat Keamanan Website Uin Ar-Raniry Menggunakan Acunetix Web Vulnerability Scanner,” 2023.
- [48] M. Muin Abdul, Kapti, and T. Yusnanto, “Campus Website Security Vulnerability Analysis Using Nessus,” *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 03, no. 02, pp. 2745–9659, 2020, doi: <https://doi.org/10.29040/ijcis.v3i2.72>.
- [49] D. Priyawati, S. Rokhmah, and I. C. Utomo, “Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP,” *Int. J.*

- Comput. Inf. Syst. Peer Rev. J.*, vol. 3, no. 3, pp. 143–147, 2022, doi: 10.29040/ijcis.v3i3.90.
- [50] N. A. Syarifudin and L. Setiyani, “Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method,” *Int. J. Multidiscip. Approach Res. Sci.*, vol. 1, no. 03, pp. 332–344, 2023, doi: 10.59653/ijmars.v1i03.177.
- [51] Diskominfotik Provinsi Lampung, Accessed: Jan. 20, 2025 [Online]. Available: <https://lampungprov.go.id/>
- [52] “Sigajah Kerja - Home.” Accessed: Jun. 01, 2025. [Online]. Available: <https://sigajahkerja.disnaker.lampungprov.go.id/>
- [53] A. D. Praba, M. Safitri, and F. Faridi, “Implementasi Datatables Server-Side Untuk Mempercepat Load Halaman Pada Aplikasi E-Commerce,” *JIKA (Jurnal Inform.)*, vol. 5, no. 2, p. 139, 2021, doi: 10.31000/jika.v5i2.4339.
- [54] N. V. Database, “Cross site scripting in datatables.net,” GitHub. Accessed: Jun. 01, 2025 [Online]. Available: <https://github.com/advisories/GHSA-h73q-5wmj-q8pj>
- [55] A. Gustiyono, E. I. Alwi, and S. M. Abdullah, “Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing Analyze Website Vulnerability To Cross-Site Scripting (XSS) Attacks Using Penetration Testing,” vol. 7, no. 1, pp. 25–33, 2024, doi: <https://doi.org/10.14421/csecurity.2024.7.1.4432>.
- [56] Gat, M. Jamil, I. Wingdes, T. Widayanti, T. Wijaya, and Kusrini, “Using Server-side Processing Techniques to Optimize Data Presentation Responsiveness,” *2024 6th Int. Conf. Cybern. Intell. Syst. ICORIS 2024*, 2024, doi: 10.1109/ICORIS63540.2024.10903755.
- [57] L. A. Reis, *Personally identifiable information*, vol. 2. Indiana: Indiana Executive Council on Cybersecurity, 2024. doi: 10.1007/978-3-319-32010-

6_300167.

- [58] Y. M. Marbun, “Apa yang Terjadi Ketika Kita Mengisi Form " I ’ m Not a Robot " ? Apa yang Terjadi Ketika Kita Mengisi Form " I ’ m Not a Robot " ?,” no. October, 2024.
- [59] W. Wardana, A. Almaarif, and A. Widjarto, “Vulnerability Assessment and Penetration Testing On The Xyz Website Using Nist 800-115 Standard,” *Syntax Lit. ; J. Ilm. Indones.*, vol. 7, no. 1, p. 520, 2022, doi: 10.36418/syntax-literate.v7i1.5800.