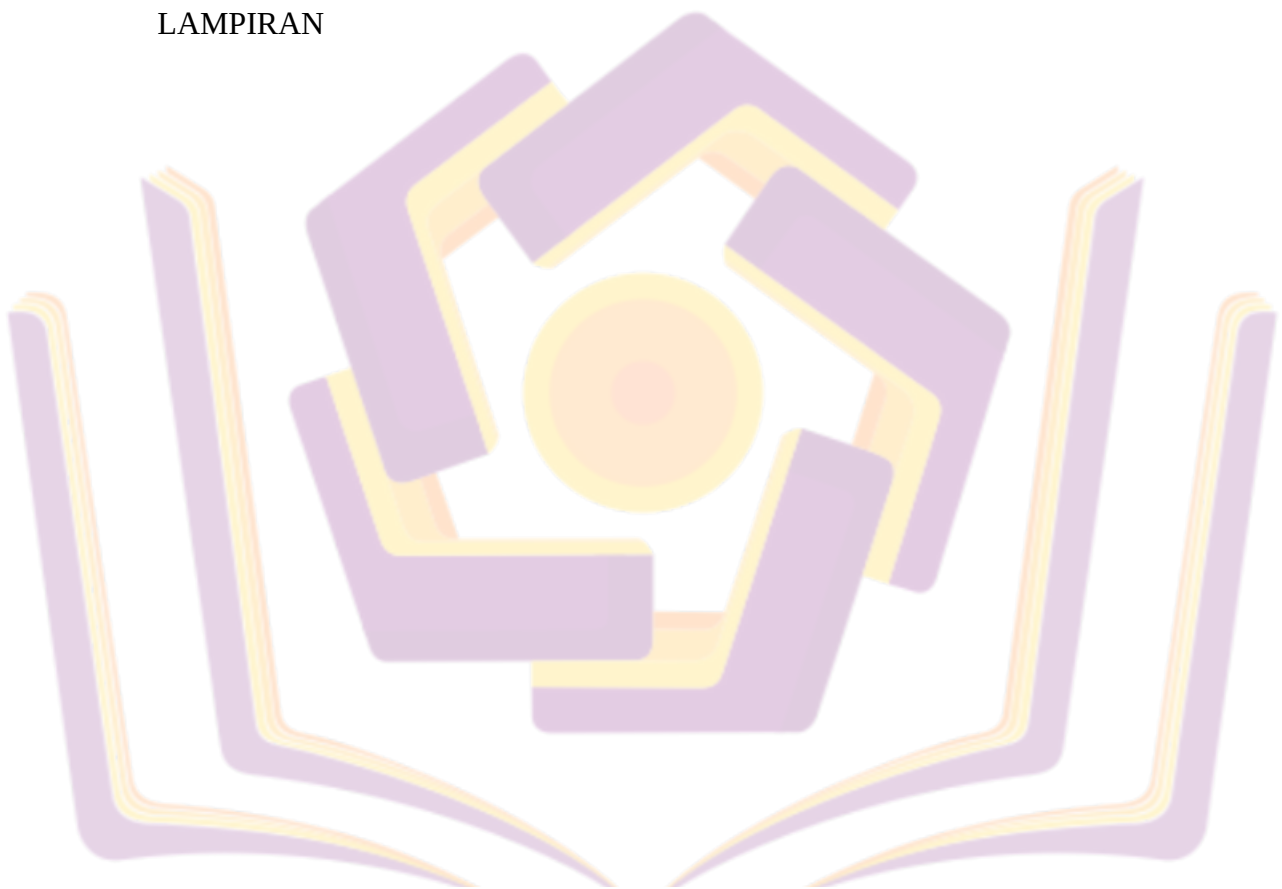


DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvii
ABSTRAK.....	xviii
<i>ABSTRACT</i>	xix
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	7
C. Batasan Masalah	8
D. Tujuan Penelitian	8
E. Manfaat Penelitian	9
BAB II TINJAUAN PUSTAKA.....	10
A. Landasan Teori.....	10
B. Penelitian Sebelumnya.....	21
BAB III METODE PENELITIAN.....	28
A. Tempat dan Waktu Penelitian.....	28
B. Metode Pengumpulan Data.....	28
C. Alat dan Bahan Penelitian.....	30
D. Konsep Penelitian	31
BAB IV HASIL DAN PEMBAHASAN	38

A. Hasil Tahap Perencanaan (<i>Planning Phase</i>).....	38
B. Tahap Penemuan (<i>Discovery Phase</i>)	40
C. Tahap Penilaian Kerentanan (<i>Review and Assessment</i>).....	46
D. Tahap Pelaporan (<i>Reporting</i>).....	82
BAB V PENUTUP.....	93
A. Kesimpulan	93
B. Saran	94
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya.....	26
Tabel 3. 1 Kategori <i>Scan Policy</i>	34
Tabel 4. 1 Rules of Engagement	39
Tabel 4. 2 Rekapitulasi Daftar Celah Keamanan Hasil Pemindaian.....	48
Tabel 4. 3 Ringkasan Nilai Kuantitatif Tingkat Risiko Base Metrics CVSS v3.1	81
Tabel 4. 4 SOP Server Apache (Disusun berdasarkan panduan resmi cPanel L.L.C., 2024 dan Apache Software Foundation, 2024)	83
Tabel 4. 5 Matriks Rekomendasi Perbaikan Keamanan Website	84
Tabel 4. 6 HTTP Header Response.....	87
Tabel 4. 7 Matriks Laporan Celah Keamanan Website Desa	90

DAFTAR GAMBAR

Gambar 4. 1 Log Traditional Spider	41
Gambar 4. 2 Log AJAX Spider.....	42
Gambar 4. 3 Direktori Site Tree OWASP ZAP	43
Gambar 4. 4 Akumulasi Log Alerts	47
Gambar 4. 5 Deskripsi Temuan Content Security Policy (CSP) Header Not Set.	50
Gambar 4. 6 Deskripsi Temuan Missing Anti-clickjacking Header	51
Gambar 4. 7 Deskripsi Temuan Server Leaks Version Information.....	53
Gambar 4. 8 Deskripsi Temuan Timestamp Disclosure-Unix	54
Gambar 4. 9 Deskripsi Temuan X-Content-Type-Options Header Missing	55
Gambar 4. 10 Deskripsi Temuan Strict-Transport-Security Header Not Set.....	57
Gambar 4. 11 Deskripsi Temuan Information Disclosure – Suspicious Comments	58
Gambar 4. 12 Deskripsi Temuan Re-examine Cache-control Directives	59
Gambar 4. 13 Deskripsi Temuan Charset Mismatch	60
Gambar 4. 14 Deskripsi Temuan Modern Web Application	60
Gambar 4. 15 Hasil Tingkat Risiko Vulnerable JS Library pada Kalkulator FIRST CVSS v3.1	62
Gambar 4. 16 Hasil Tingkat Risiko CSP pada Kalkulator Resmi FIRST CVSS v3.1	64
Gambar 4. 17 Hasil Tingkat Risiko Missing Anti-clickjacking Header pada Kalkulator Resmi FIRST CVSS v3.1	66
Gambar 4. 18 Hasil Tingkat Risiko X-Content-Type-Options pada Kalkulator Resmi FIRST CVSS v3.1	68
Gambar 4. 19 Hasil Tingkat Risiko Server Leaks Version Information.....	71
Gambar 4. 20 Hasil Tingkat Risiko Strick-Transport-Security Header Not Set...	73
Gambar 4. 21 Hasil Tingkat Risiko Cross-Domain JavaScript Source File Inclusion	75
Gambar 4. 22 Hasil Tingkat Risiko Timestamp Disclosure-Unix	77
Gambar 4. 23 Skrip Proteksi	87

DAFTAR ISTILAH

1. **Active Scanning (Pemindaian Aktif):** Metode pemindaian keamanan dengan cara mengirimkan muatan (payload) serangan buatan ke target untuk menguji secara langsung apakah suatu celah keamanan dapat dieksploitasi.
2. **AJAX Spidering:** Fitur perayapan *website* dinamis dengan memanfaatkan headless browser untuk mengeksplorasi elemen-elemen web yang memanipulasi Document Object Model (DOM) JavaScript secara asinkronus.
3. **Attack Surface (Permukaan Serangan):** Seluruh titik masuk, direktori, parameter, atau fungsi yang terdapat pada sebuah sistem aplikasi yang berpotensi dieksploitasi oleh aktor ancaman siber.
4. **Common Vulnerability Scoring System (CVSS):** Standar industri terbuka dan terukur yang digunakan untuk mengalkulasi nilai keparahan risiko dari suatu celah keamanan perangkat lunak berdasarkan metrik tertentu.
5. **Content Injection:** Jenis serangan siber yang memasukkan kode atau konten ilegal ke dalam suatu halaman web secara tidak sah (dalam hal ini, iklan judi online ilegal).
6. **Content Management System (CMS):** Perangkat lunak atau sistem yang digunakan untuk mengatur, mengelola, dan mempublikasikan konten pada *website* tanpa harus membangun kode dari awal (contohnya: WordPress).
7. **CWE (Common Weakness Enumeration):** Sistem pengelompokan formal berskala internasional untuk mengidentifikasi tipe kerentanan yang pada arsitektur, desain, maupun kode perangkat lunak.
8. **E-Government:** Pemanfaatan teknologi informasi dan komunikasi oleh instansi pemerintah untuk memberikan pelayanan publik yang efisien, transparan, dan akuntabilitas.
9. **False Positive:** Alarm palsu atau kondisi ketika alat pemindai keamanan menemukan celah keamanan pada sistem, tetapi setelah divalidasi, sistem tetap aman.
10. **Hardening (Server Hardening):** Proses penguatan konfigurasi sistem keamanan secara berlapis pada server dengan tujuan memperkecil permukaan serangan.
11. **Header HTTP (Response Header):** Komponen informasi metadata yang dikirimkan ke browser pengguna oleh server untuk memberikan instruksi khusus, termasuk instruksi tentang pengamanan data.
12. **.htaccess:** Berkas konfigurasi tingkat direktori yang digunakan pada web server berbasis Apache untuk mengatur hak akses, mengalihkan URL, dan injeksi instruksi keamanan.
13. **NIST SP 800-115:** Panduan teknis standar internasional oleh National Institute of Standards and Technology (NIST) sebagai kerangka kerja metodologis untuk pengujian keamanan data.

14. **OWASP ZAP (Zed Attack Proxy):** Alat audit pengujian penetrasi aplikasi web open-source yang digunakan secara pasif maupun aktif untuk menemukan kerentanan keamanan.
15. **Passive Scanning:** Metode pemindaian keamanan yang memeriksa dan menganalisis lalu lintas data (request dan response HTTP) tanpa mengubah data atau mengirimkan serangan aktif.
16. **Site Tree:** Representasi visual dalam bentuk pohon hierarki yang merangkum seluruh direktori, file, dan parameter URL yang berhasil ditemukan pada *website* target.
17. **Traditional Spidering:** Fitur perayapan otomatis standar yang menelusuri seluruh tautan yang muncul di dalam struktur kode HTML dasar situs web.
18. **Vulnerability Assessment:** Proses peninjauan sistematis yang bertujuan untuk menemukan, mengukur tingkat risiko, dan memprioritaskan penanganan celah keamanan infrastruktur digital.
19. **Vulnerable JS Library:** Penggunaan pustaka JavaScript (library) versi lama pada aplikasi web yang telah diketahui memiliki masalah keamanan publik dan belum diperbarui.

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Dosen Pembimbing 1

Lampiran 2. Kartu Bimbingan Dosen Pembimbing 2

Lampiran 3. Surat Izin Penelitian

Lampiran 4. Skrip Wawancara

