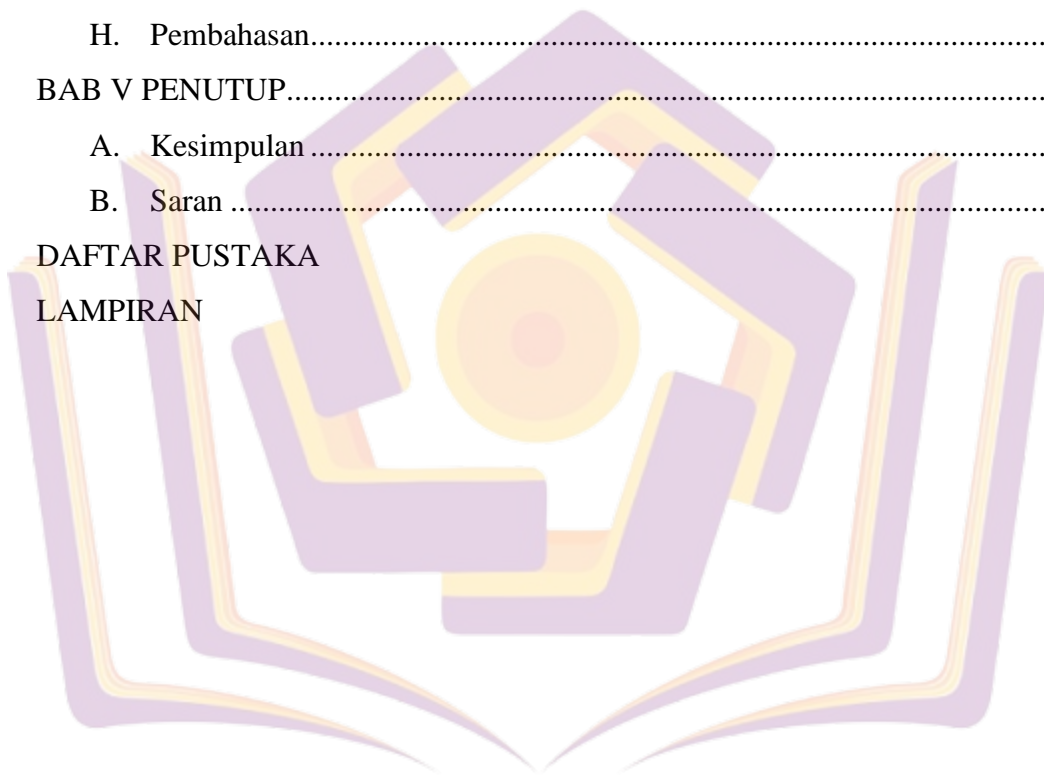


DAFTAR ISI

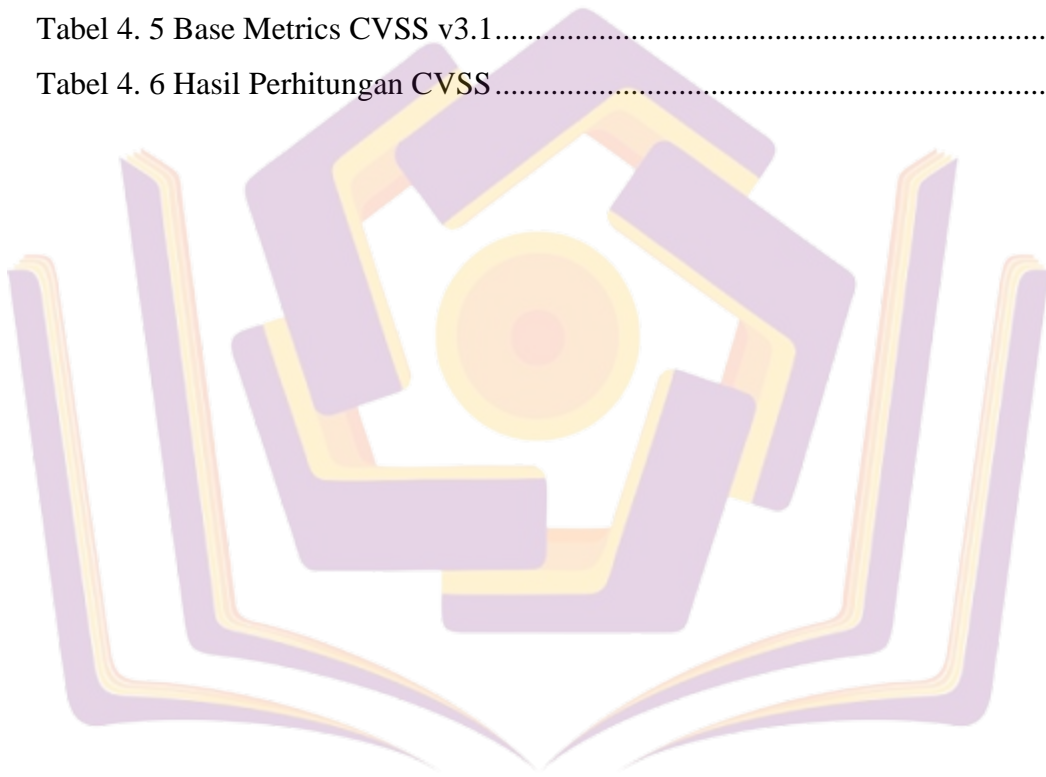
HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR ISTILAH	xvi
DAFTAR LAMPIRAN.....	xvii
INTISARI.....	xviii
<i>ABSTRACT</i>	xix
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	7
C. Batasan Masalah	7
D. Tujuan Penelitian	8
E. Manfaat Penelitian	8
BAB II TINJAUAN PUSTAKA.....	10
A. Landasan Teori.....	10
B. Penelitian Sebelumnya.....	25
BAB III METODE PENELITIAN.....	31
A. Tempat dan Waktu Penelitian.....	31
B. Metode Pengumpulan Data.....	31
C. Alat dan Bahan Penelitian.....	33
D. Konsep Penelitian	34

BAB IV HASIL DAN PEMBAHASAN	39
A. <i>Planning</i>	39
B. <i>Information Gathering</i>	40
C. <i>Vulnerability Scanning</i>	44
D. <i>Penetration Testing</i>	63
E. <i>Reporting</i>	68
F. Analisis Risiko Keamanan dengan CVSS	69
G. Rekomendasi Perbaikan	75
H. Pembahasan	76
BAB V PENUTUP	81
A. Kesimpulan	81
B. Saran	82
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 CVSS Score	22
Tabel 2. 2 Penelitian Terdahulu	29
Tabel 4. 1 Hasil Information Gathering	43
Tabel 4. 2 Kategori Alert pada OWASP ZAP	45
Tabel 4. 3 Klasifikasi kerentanan berdasarkan OWASP Top 10 2021	60
Tabel 4. 4 Reporting hasil Penetration Testing	68
Tabel 4. 5 Base Metrics CVSS v3.1	70
Tabel 4. 6 Hasil Perhitungan CVSS	72



DAFTAR GAMBAR

Gambar 1. 1 Dokumentasi Insiden Spam Pendaftaran Pasien	3
Gambar 2. 1 Tools WhatWeb.....	13
Gambar 2. 2 Tools Nmap	14
Gambar 2. 3 Tools OWASP Zed Attack Proxy (ZAP)	15
Gambar 2. 4 Tools Kali Linux	16
Gambar 2. 5 Kerentanan OWASP Top !0 2021	17
Gambar 2. 6 CVSS Metric Groups	22
Gambar 3. 1 Alur Penelitian Metode VAPT	35
Gambar 4. 1 Website Target	39
Gambar 4. 2 Hasil Information Gathering dengan WhatWeb.....	40
Gambar 4. 3 Hasil Information Gathering dengan Nmap	42
Gambar 4. 4 Hasil vulnerability scanning menggunakan OWASP ZAP.....	44
Gambar 4. 5 CSP: Failure to Define Directive with No Fallback.....	46
Gambar 4. 6 CSP: Wildcard Directive.....	47
Gambar 4. 7 CSP: script-src unsafe-inline.....	47
Gambar 4. 8 CSP: style-src unsafe-inline	48
Gambar 4. 9 Hidden File Found.....	49
Gambar 4. 10 Missing Anti-clickjacking Header	50
Gambar 4. 11 Cookie Without Secure Flag	50
Gambar 4. 12 Cross-Domains JavaScript Source File Inclusion	51
Gambar 4. 13 Server Leaks Information via "X-Powered-By"	52
Gambar 4. 14 Server Leaks Information via "Server"	53
Gambar 4. 15 Strict-Transport-Security Header Not Set	54
Gambar 4. 16 X-Content-Type-Options Header Missing.....	55
Gambar 4. 17 Information Disclosure – Suspicious Comments.....	56
Gambar 4. 18 Re-examine Cache-control Directives	57
Gambar 4. 19 Session Management Response Identified.....	58
Gambar 4. 20 User Agent Fuzzer.....	59
Gambar 4. 21 Pengujian SQL Injection Menggunakan SQLMap	63

Gambar 4. 22 Hasil Pengujian SQL Injection Menggunakan SQLMap.....	64
Gambar 4. 23 Script HTML untuk pengujian Clickjacking.....	65
Gambar 4. 24 Hasil pengujian Clickjacking	66
Gambar 4. 25 Hasil pengujian pembanding Anti-clickjacking Header	67



DAFTAR ISTILAH

Vulnerability Assessment and Penetration Testing (VAPT)

OWASP Top 10

Common Vulnerability Scoring System (CVSS)

Black Box Testing

OWASP ZAP

SQL Injection

Penetration Testing



DAFTAR LAMPIRAN

Lampiran 1 Hasil Wawancara

Lampiran 2 Surat Permohonan Izin Penelitian

Lampiran 3 Surat Tanggapan Izin Penelitian

Lampiran 4 Kartu Bimbingan

