

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR.....	i
PENGESAHAN PENGUJI.....	ii
LEMBAR PERNYATAAN KEASLIAN.....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
HALAMAN PERSEMBAHAN DAN MOTTO.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN.....	I-1
1.1 Latar Belakang.....	I-1
1.2 Rumusan Masalah.....	I-4
1.3 Tujuan Penelitian.....	I-5
1.4 Manfaat Penelitian.....	I-6
1.5 Batasan Masalah.....	I-6
BAB II TINJAUAN PUSTAKA.....	II-1
2.1 Landasan Teori.....	II-1
2.1.1 Keamanan Aplikasi Web.....	II-1
2.1.2 Web Application Penetration Testing.....	II-1
2.1.3 OWASP Top 10.....	II-2
2.2 Penelitian Terkait.....	II-7
2.2.1 State of The Art.....	II-7
2.3 Matriks Penelitian.....	II-15
2.4 <i>Research Gap</i>.....	II-21
BAB III.....	III-1
METODOLOGI PENELITIAN.....	III-1
3.3 Tahapan Penelitian.....	III-1
BAB IV HASIL DAN PEMBAHASAN.....	IV-1
4.1 Gambaran Umum Pengujian.....	IV-1
4.2 <i>Scanning Vulnerability</i> OWAS ZAP.....	IV-2

4.2.1	Input <i>URL Website</i>	IV-2
4.2.2	Hasil Ancaman (<i>Alerts</i>)	IV-3
4.3	Hasil Pemindaian <i>OWAS ZAP</i>	IV-4
4.3.1	<i>Summary Alerts</i>	IV-4
4.3.2	<i>Alerts Detail</i>	IV-4
4.3.3	Klasifikasi <i>Alerts</i>	IV-6
4.4	Validasi Manual Temuan	IV-8
4.4.1	Pengujian <i>Cross-Site Scripting (XSS)</i>	IV-8
4.4.2	Pengujian <i>SQL Injection</i>	IV-12
4.4.3	Pengujian <i>Clickjacking (UI Redressing)</i>	IV-13
4.4.5	<i>Insecure Direct Object Reference (IDOR)</i>	IV-19
4.6	Analisis Dampak Terhadap CIA	IV-24
	Tabel 4.6 Manajemen Risiko Keamanan Informasi	IV-27
	Level Risiko Kuantitatif (CVSS)	IV-27
	Strategi Mitigasi/ Remediasi	IV-27
	Prioritas Penanganan	IV-27
	Medium (6.8)	IV-27
	Menerapkan atribut <i>HttpOnly</i> , <i>Secure</i> , dan <i>SameSite=Lax</i> pada cookie sesi	IV-27
	P1 (Utama)	IV-27
	Medium (5.4)	IV-27
	Menambahkan response header <i>X-Frame-Options: SAMEORIGIN</i> atau <i>CSP frame-ancestors 'self'</i>	IV-27
	P1 (Utama)	IV-27
	Low (3.7)	IV-27
	Mengkonfigurasi web server (Nginx/Apache) untuk menghapus header <i>X-Powered-By</i>	IV-27
	P2 (Sekunder)	IV-27
BAB V KESIMPLAN DAN SARAN		V-1
5.1	Kesimpulan	V-1
5.2	Saran	V-2
DAFTAR PUSTAKA		

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait (<i>State of the art</i>).....	II-5
Tabel 2.2 Tabel Matriks Penelitian.....	II-13
Tabel 4.1 <i>Summary Alerts</i>	IV-5
Tabel 4.2 <i>Alerts</i>	IV-5
Tabel 4.3 <i>Alerts Detail</i>	IV-6
Tabel 4.4 Ringkasan Hasil Pengujian Keamanan.....	IV-31

DAFTAR GAMBAR

Gambar 1.1	Diagram 10 Negara dengan kebocoran data terbesar	I-3
Gambar 3.1	Alur Penelitian	III-1
Gambar 4.1	Antar Muka Owas ZAP	IV-2
Gambar 4.2	<i>Scanning Owas ZAP</i>	IV-3
Gambar 4.3	Hasil <i>Scanning (Alerts)</i>	IV-4
Gambar 4.4	Proses Instalasi Paramspider	IV-9
Gambar 4.5	Proses Instalasi Paramspider	IV-9
Gambar 4.6	Proses Instalasi Dalfox	IV-10
Gambar 4.7	Proses Eksploitasi Menggunakan Paramspider	IV-10
Gambar 4.8	<i>Results</i> Eksploitasi <i>Web Sintesys</i>	IV-11
Gambar 4.9	Proses <i>Scanning</i> Menggunakan Dalfox	IV-12
Gambar 4.10	Proses <i>Scanning</i> dan Eksploitasi <i>Web SINTESYS</i>	IV-12
Gambar 4.11	Proses Pembuatan <i>Exploit Payload</i>	IV-13
Gambar 4.12	Pembuatan <i>Payload Clickjacking</i>	IV-13
Gambar 4.13	Eksekusi <i>Payload</i> Menggunakan <i>Firefox</i>	IV-14
Gambar 4.14	Hasil Eksploitasi <i>Clickjacking</i>	IV-15
Gambar 4.15	Pengambilan Data <i>Cookie</i> Melalui <i>JavaScript</i>	IV-15
Gambar 4.16	Ekstraksi <i>Cookie</i> Sesi	IV-16
Gambar 4.17	Penggunaan Netcat Sebagai <i>Listener</i>	IV-17
Gambar 4.18	Implementasi Kode Penarikan <i>Cookie</i> Pada <i>Console</i>	IV-18
Gambar 4.19	Hasil Monitoring Lalu Lintas Data Menggunakan Netcat	IV-18
Gambar 4.20	Antar Muka <i>Dahsboard</i> Mahasiswa Pada <i>Website</i> Terintegrasi Burpsuite	IV-19

Gambar 4.21 *Log Transmisi HTTP Request* Pada Panel Proxy Burp Suite..... IV-20

Gambar 4.22 Permintaan HTTP (*Request*) Pada Fitur *Repeater* Burp SuiteIV-219