



SKRIPSI

**PENGUJIAN KEAMANAN WEBSITE ERP
DENGAN TEKNIK PENETRATION TESTING
MENGUNAKAN METODE PTES
BERDASARKAN OWASP TOP 10
(STUDI KASUS: PT. XYZ)**

MOCHAMMAD YOGA FIRNANDA
NPM 21081010152

DOSEN PEMBIMBING

Henni Endah Wahanani, S.T., M.Kom.

Achmad Junaidi, S.Kom., M.Kom.

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA
2025**



SKRIPSI

**PENGUJIAN KEAMANAN WEBSITE ERP
DENGAN TEKNIK PENETRATION TESTING
MENGUNAKAN METODE PTES
BERDASARKAN OWASP TOP 10
(STUDI KASUS: PT. XYZ)**

MOCHAMMAD YOGA FIRNANDA
NPM 21081010152

DOSEN PEMBIMBING

Henni Endah Wahanani, S.T., M.Kom.

Achmad Junaidi, S.Kom., M.Kom.

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA
2025**

Halaman ini sengaja dikosongkan

LEMBAR PENGESAHAN

PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)

Oleh :
MOCHAMMAD YOGA FIRNANDA
NPM. 21081010152

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur pada tanggal 16 Mei 2025

Menyetujui

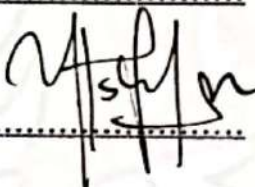
Henni Endah Wahanani, S.T., M.Kom.
NIP. 19780922 2021212 005


..... (Pembimbing I)

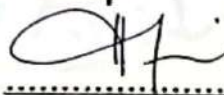
Achmad Junaidi, S.Kom., M.Kom.
NIP. 3 7811 04 0199 1


..... (Pembimbing II)

Yisti Vita Via, S.ST., M.Kom.
NIP. 19860425 2021212 001


..... (Ketua Penguji)

Afina Lina Nurlaili, S.Kom., M.Kom.
NIP. 1993121 3202203 2010


..... (Anggota Penguji)

Mengetahui,
Dekan Fakultas Ilmu Komputer



Prof. Dr. Ir. Novirina Hendrasarie, MT.
1968126-199403 2 001

Halaman ini sengaja dikosongkan

LEMBAR PERSETUJUAN

**PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION
TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10
(STUDI KASUS: PT. XYZ)**

Oleh:

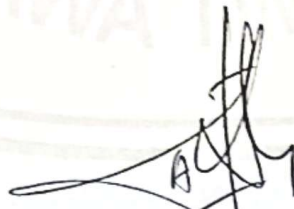
MOCHAMMAD YOGA FIRNANDA

NPM. 21081010152

Menyetujui,

Koordinator Program Studi

Fakultas Ilmu Komputer



Fetty Tri Anggraeny, S.Kom., M.Kom.

NIP. 19820211 2021212 005

Halaman ini sengaja dikosongkan

SURAT PERNYATAAN BEBAS PLAGIASI

Yang bertandatangan di bawah ini:

Nama : Mochammad Yoga Firnanda
NPM : 21081010152
Program : Sarjana (S1)
Program Studi : Informatika
Fakultas : Ilmu Komputer

Menyatakan bahwa dalam dokumen ilmiah Tugas Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan secara lengkap dalam daftar pustaka.

Dan saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi. Apabila dikemudian hari ditemukan indikasi plagiat pada Skripsi, saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari siapapun juga dan untuk dipergunakan sebagaimana mestinya.



Surabaya, 13 Juni 2025

Yang Membuat Pernyataan,



MOCHAMMAD YOGA FIRNANDA

NPM. 21081010152

Halaman ini sengaja dikosongkan

ABSTRAK

Nama Mahasiswa / NPM : Mochammad Yoga Firnanda / 21081010152
Judul Skripsi : PENGUJIAN KEAMANAN WEBSITE ERP DENGAN
TEKNIK PENETRATION TESTING MENGGUNAKAN
METODE PTES BERDASARKAN OWASP TOP 10
(STUDI KASUS: PT. XYZ)
Dosen Pembimbing : 1. Henni Endah Wahanani, S.T., M.Kom.
2. Achmad Junaidi, S.Kom., M.Kom.

Kemajuan teknologi yang pesat membawa banyak manfaat bagi sektor industri, sehingga banyak perusahaan yang bergantung pada teknologi untuk mendukung operasionalnya, namun ketergantungan ini juga membuka peluang bagi *hacker* untuk mengeksploitasi kerentanan sistem dan mencuri informasi sensitif. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan mengeksploitasi kerentanan pada website ERP PT. XYZ, khususnya pada halaman yang dapat diakses oleh pengguna dengan *role* SPV Marketing, dengan teknik *penetration testing* menggunakan metode PTES yang mengacu pada OWASP Top 10 tahun 2021. Metode PTES yang digunakan mencakup tujuh tahapan, yaitu *pre-engagement interaction*, *intelligence gathering*, *threat modeling*, *vulnerability analysis* menggunakan ZAP, *exploitation*, *post-exploitation*, dan *reporting*. Berdasarkan pemindaian ZAP, ditemukan 23 celah keamanan, dengan 18 di antaranya termasuk dalam kategori OWASP Top 10, seperti *Broken Access Control*, *Injection*, *Insecure Design*, dan *Security Misconfiguration*, *Vulnerable and Outdated Components*, dan *Software and Data Integrity Failures*. Simulasi serangan yang berhasil dilakukan mencakup *Cross-Site Scripting* (XSS), *Session Hijacking*, dan *Cross-Site Request Forgery* (CSRF). Pengujian ini difokuskan pada kerentanan dengan risiko tinggi, seperti *Cloud Metadata Potentially Exposed* dan *Vulnerable JS Library*, serta risiko sedang, seperti *Absence of Anti-CSRF Tokens*, *Application Error Disclosure*, *CSP Header Not Set*, dan *Missing Anti-clickjacking Header*. Selain itu, juga ditemukan risiko rendah, seperti *Big Redirect Detected*, *Cookie No HttpOnly Flag*, *Cookie Without Secure Flag*, *Cookie without SameSite Attribute*, *Cross-Domain Javascript Source File Inclusion*, *Server Leaks Version Information via "Server" HTTP Response*, *Strict-Transport-Security Header Not Set*, *Timestamp Disclosure – Unix*, dan *X-Content-Type-Options Header Missing*. Rekomendasi perbaikan disesuaikan dengan teknologi ERP untuk memudahkan pemahaman tim pengembang dan meningkatkan keamanan sistem sesuai pedoman keamanan yang ditetapkan dalam OWASP Top 10.

Kata Kunci : Pengujian Keamanan, PTES, OWASP Top 10, Website ERP

Halaman ini sengaja dikosongkan

ABSTRACT

Student Name / NPM : Mochammad Yoga Firnanda / 21081010152
Thesis title : ERP WEBSITE SECURITY TESTING USING PENETRATION
TESTING TECHNIQUES WITH PTES METHOD BASED ON
OWASP TOP 10 (STUDY CASE: PT. XYZ)
Advisor : 1. Henni Endah Wahanani, S.T., M.Kom.
2. Achmad Junaidi, S.Kom., M.Kom.

Rapid technological advancements have brought numerous benefits to the industrial sector, leading many companies to rely on technology to support their operations. However, this dependency also opens opportunities for hackers to exploit system vulnerabilities and steal sensitive information. This research aims to identify, evaluate, and exploit vulnerabilities on the ERP website of PT. XYZ, particularly on pages accessible by users with the SPV Marketing role, using penetration testing techniques with the PTES method referring to the 2021 OWASP Top 10. The PTES method used includes seven stages: pre-engagement interaction, intelligence gathering, threat modeling, vulnerability analysis using ZAP, exploitation, post-exploitation, and reporting. Based on the ZAP scan, 23 security vulnerabilities were found, 18 of which are included in the OWASP Top 10 categories, such as Broken Access Control, Injection, Insecure Design, and Security Misconfiguration, Vulnerable and Outdated Components, and Software and Data Integrity Failures. Successful attack simulations include Cross-Site Scripting (XSS), Session Hijacking, and Cross-Site Request Forgery (CSRF). The testing focused on high-risk vulnerabilities, such as Cloud Metadata Potentially Exposed and Vulnerable JS Library, as well as medium-risk vulnerabilities such as Absence of Anti-CSRF Tokens, Application Error Disclosure, CSP Header Not Set, and Missing Anti-clickjacking Header. Additionally, low-risk vulnerabilities were also found, such as Big Redirect Detected, Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie without SameSite Attribute, Cross-Domain Javascript Source File Inclusion, Server Leaks Version Information via 'Server' HTTP Response, Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix, and X-Content-Type-Options Header Missing. The improvement recommendations are tailored to ERP technology to facilitate the understanding of the development team and enhance system security in accordance with the security guidelines set forth in the OWASP Top 10.

Keyword : Security Testing, PTES, OWASP Top 10, ERP Website

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul **“PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)”** dengan baik. Penulisan buku skripsi ini tidak dapat terwujud tanpa bantuan, motivasi, dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa hormat dan terima kasih kepada:

1. Kedua orang tua penulis yang selalu memberikan doa serta dukungan kepada penulis, baik dukungan materi dan non-materi, sehingga penulis dapat menyelesaikan perkuliahan dari awal hingga akhir dengan baik.
2. Bapak Prof. Dr. Ir. Akhmad Fauzi, M.MT., selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Ibu Dr. Novirina Hendrasarie, S.T, M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Fetty Tri Anggraeny S.Kom., M.Kom., selaku Koordinator Program Studi Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Andreas Nugroho Sihananto, S.Kom., M.Kom., selaku Koordinator Skripsi Program Studi Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
6. Ibu Henni Endah Wahanani, S.T., M.Kom., selaku dosen pembimbing pertama dalam membimbing dan mengarahkan penulis selama proses penyelesaian buku skripsi.
7. Bapak Achmad Junaidi, S.Kom., M.Kom., selaku dosen pembimbing dalam membimbing dan mengarahkan penulis selama proses penyusunan, usulan hingga penyelesaian buku skripsi.
8. Seluruh dosen, dan staff program studi Informatika UPN “Veteran” Jawa Timur yang telah mengajar, memberikan ilmu, serta pengalaman berharga selama masa perkuliahan.
9. Terima kasih kepada Staff IT dan HRD PT. XYZ atas kesempatan, bantuan administrasi, dan penyediaan sumber daya selama penelitian skripsi terhadap website ERP PT. XYZ.

10. Teman-teman seperjuangan yang selalu memberikan semangat, motivasi, serta menemani dan membantu penulis selama masa perkuliahan.
11. Seluruh keluarga besar dan kerabat yang senantiasa memberikan doa dan dukungan.
12. Semua pihak yang tidak dapat disebutkan satu per satu yang telah membantu secara langsung maupun tidak langsung dalam penyusunan skripsi.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak terdapat kekurangan. Oleh karena itu, kritik dan saran yang membangun dari berbagai pihak sangat diharapkan demi perbaikan dan penyempurnaan skripsi ini. Semoga laporan skripsi ini dapat menjadi referensi yang bermanfaat, khususnya bagi mahasiswa yang sedang menempuh skripsi sebagai syarat kelulusan, baik dari instansi yang sama maupun yang berbeda.

Surabaya, 11 Juni 2025



Mochammad Yoga Firnanda

NPM. 21081010152

DAFTAR ISI

LEMBAR PENGESAHAN.....	i
LEMBAR PERSETUJUAN.....	iii
SURAT PERNYATAAN BEBAS PLAGIASI.....	v
ABSTRAK.....	vii
ABSTRACT	ix
KATA PENGANTAR.....	xi
DAFTAR ISI	xiii
DAFTAR GAMBAR.....	xvii
DAFTAR TABEL	xxi
DAFTAR LAMPIRAN	xxiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian.....	4
1.4 Manfaat Penelitian	4
1.5 Batasan Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Terdahulu	5
2.2 PT. XYZ.....	7
2.3 Website	7
2.4 <i>Enterprise Resource Planning</i> (ERP).....	8
2.5 Penetration Testing	9
2.6 Penetration Testing Execution Standart (PTES).....	9
2.6.1 Pre-engagement Interactions	10
2.6.2 Intelligence Gathering.....	10
2.6.3 Threat Modeling	12
2.6.4 Vulnerability Analysis	13
2.6.5 Exploitation	14
2.6.6 Post-Exploitation	14

2.6.7	Reporting.....	14
2.7	OWASP Top 10.....	15
2.8	ISO/IEC 25010.....	20
2.9	Alat Bantu	20
2.9.1.	Kali Linux	21
2.9.2	Mozilla Firefox	21
2.9.3	Netcraft.....	22
2.9.4	Wappalizer	23
2.9.5	Nmap.....	24
2.9.6	OWASP Zed Attack Proxy (ZAP).....	24
2.9.7	Burp suite	26
2.9.8.	Bettercap	26
2.9.9.	XSS Hunter	27
BAB III METODOLOGI PENELITIAN		29
3.1	Tahapan Penelitian.....	29
3.2	Studi Literatur	30
3.3	Analisis Objek Penelitian.....	30
3.4	Pengujian dan Analisis.....	38
3.4.1	Pre-engagement Interaction.....	39
3.4.2	Intelligence Gathering.....	40
3.4.3	Threat Modeling	42
3.4.4	Vulnerability Analysis	42
3.4.5	Exploitation	43
3.4.6	Post-Exploitation	44
3.4.7	Reporting.....	45
BAB IV HASIL DAN PEMBAHASAN.....		47
4.1	Pre-engagement Interaction.....	47
4.2.	Intelligence Gathering	48
4.2.1.	Google Dorking	48
4.2.2.	Netcraft.....	50
4.2.3.	Wappalyzer.....	51
4.2.4.	Nmap.....	52
4.3	Threat Modeling	54

4.4	Vulnerability Analysis	59
4.5	Exploitation	62
4.5.1.	Cloud Metadata Potentially Expose	62
4.5.2.	Vulnerable JS Library.....	64
4.5.3.	Absence of Anti-CSRF Tokens	66
4.5.4.	Application Error Disclosure	68
4.5.5.	Content Security Policy (CSP) Header Not Set	71
4.5.6.	Cross-Domain Misconfiguration.....	74
4.5.7.	Missing Anti-clickjacking Header.....	76
4.5.8.	Big Redirect Detected (Potential Sensitive Information Leak)	78
4.5.9.	Cookie No HTTPOnly Flag	79
4.5.10.	Cookie Without Secure Flag	81
4.5.11.	Cookie without SameSite Attribute.....	82
4.5.12.	Cross-Domain Javascript Source File Inclusion.....	84
4.5.13.	Server Leaks Version Information via “Server” HTTP Response	85
4.5.14.	Strict-Transport-Security Header Not Set.....	86
4.5.15.	Timestamp Disclosure – Unix.....	88
4.5.16.	X-Content-Type-Options Header Missing.....	89
4.6	Post-Exploitation	91
4.6.1.	XSS	91
4.6.2.	Session Hijacking.....	94
4.6.3.	CSRF	96
4.7	Reporting.....	98
4.7.1.	Hasil	98
4.7.2.	Rekomendasi Perbaikan	101
BAB V	PENUTUP	109
5.1.	Kesimpulan	109
5.2.	Saran.....	110
DAFTAR PUSTAKA		111
LAMPIRAN		115

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

Gambar 2.1 Tahapan Metode PTES dalam Pengujian Penetrasi	9
Gambar 2.2 Perbedaan Passive dan Active Intelligence	11
Gambar 2.3 Daftar Kerentanan OWASP Top 10 Tahun 2017–2021.....	15
Gambar 2.4 Tampilan Awal Kali Linux.....	21
Gambar 2.5 Logo Mozilla Firefox	21
Gambar 2.6 Contoh Site Report Netcraft Pada Website UPN Jatim	22
Gambar 2.7 Contoh Hasil Identifikasi Teknologi dengan Wappalizer	23
Gambar 2.8 Tampilan Namp pada Kali Linux	24
Gambar 2.9 Tampilan Awal OWASP ZAP	25
Gambar 2.10 Logo Burp Suite.....	26
Gambar 2.11 Profil Github Bettercap	26
Gambar 2.12 Profil Github XSS Hunter	27
Gambar 3.1 Tahapan Penelitian.....	29
Gambar 3.2 Alur Tahapan Pengujian dan Analisis	38
Gambar 3.3 Alur Tahap Pre-engagement Interaction	40
Gambar 3.4 Alur Tahap Intelligence Gathering	41
Gambar 3.5 Alur Tahap Threat Modeling.....	42
Gambar 3.6 Alur Tahap Vulnerability Analysis	42
Gambar 3.7 Alur Tahap Exploitation.....	43
Gambar 3.8 Alur Tahap Post-Exploitation.....	44
Gambar 3.9 Alur Tahap Reporting	45
Gambar 4.1 Capture Google Dorking	49
Gambar 4.2 Site Report Netcraft Website ERP PT. XYZ.....	50
Gambar 4.3 Hasil Pemindaian Wappalyzer pada Website ERP PT. XYZ.....	51
Gambar 4.4 Kombinasi Pemindaian SYN dan Service Scan Nmap	52
Gambar 4.5 Pemindaian Port Manual dengan Nmap	53
Gambar 4.6 Session Aktif Setelah Manual Scan	59
Gambar 4.7 Automated Scan terhadap Website ERP PT. XYZ	60
Gambar 4.8 Hasil Scan Kerentanan dengan OWASP ZAP.....	60
Gambar 4.9 Detail Kerentanan Cloud Metadata pada Zaproxy.org.....	61
Gambar 4.10 Kerentanan Cloud Metadata pada Pemindaian OWASP ZAP	62
Gambar 4.11 Request ke Halaman Target Kerentanan	63

Gambar 4.12 Response Setelah Host Diubah	64
Gambar 4.13 Respons Halaman Kerentanan Setelah Host Diganti	64
Gambar 4.14 Kerentanan JS Library pada Pemindaian OWASP ZAP	65
Gambar 4.15 Hasil Pencarian Kerentanan pada Website CVE Details.....	66
Gambar 4.16 Kerentanan CSRF pada Pemindaian OWASP ZAP.....	67
Gambar 4.17 Pemeriksaan Page Source Halaman Rentan CSRF	67
Gambar 4.18 Contoh Pesan Kesalahan Stack Trace	68
Gambar 4.19 Kerentanan Error Disclosure pada Pemindaian OWASP ZAP.....	69
Gambar 4.20 Pengecekan Error Disclosure pada Halaman Profil	69
Gambar 4.21 Response Data dari Server ke halaman Profil	70
Gambar 4.22 Kerentanan CSP pada Pemindaian OWASP ZAP	71
Gambar 4.23 Contoh CSP Header di Halaman Github	72
Gambar 4.24 Pengujian CSP Gagal di Halaman Github.....	72
Gambar 4.25 Pengecekan CSP di Halaman Login ERP	73
Gambar 4.26 Pengujian Kode JS di Halaman Login ERP	74
Gambar 4.27 Kerentanban Cross-Domain Misconfiguration pada.....	75
Gambar 4.28 Request dan Response Kerentanan Cross-Domain Misconfiguration.....	75
Gambar 4.29 Kerentanan Clickjacking pada Pemindaian OWASP ZAP	76
Gambar 4.30 Langkah-langkah Penggunaan Burp Clickbandit.....	77
Gambar 4.31 Tampilan Burp Clickbandit Ketika Berhasil Dieksekusi	77
Gambar 4.32 Tampilan Ketika Pengujian Clickjacking Berhasil	78
Gambar 4.33 Kerentanan Big Redirect pada Pemindaian OWASP ZAP.....	78
Gambar 4.34 Request dan Response Kerentanan Big Redirect	79
Gambar 4.35 Kerentanan Cookie HttpOnly pada Pemindaian OWASP ZAP.....	79
Gambar 4.36 Contoh Cookie HttpOnly di Halaman Github	80
Gambar 4.37 Pengecekan Cookie HttpOnly di Halaman Dashboard ERP	80
Gambar 4.38 Pengujian Kode JS di Halaman Dashboard ERP	81
Gambar 4.39 Kerentanan Cookie Secure pada Pemindaian OWASP ZAP.....	81
Gambar 4.40 Lalu Lintas Jaringan HTTP dengan Bettercap.....	82
Gambar 4.41 Kerentanan Cookie Samesite pada Pemindaian OWASP ZAP	82
Gambar 4.42 Request dan Response Cookie Samesite Melalui CSRF	83
Gambar 4.43 Request dan Response Redirect ke Halaman Login Setelah CSRF	83
Gambar 4.44 Kerentanan JS Inclusion pada Pemindaian OWASP ZAP	84
Gambar 4.45 Hasil Pengecekan CVE Detail pada Library DevExpress	85

Gambar 4.46 Kerentanan Server Leaks pada Pemindaian OWASP ZAP	85
Gambar 4.47 Request dan Response Kerentanan Server Leaks Information	86
Gambar 4.48 Kerentanan Strict Transport pada Pemindaian OWASP ZAP	86
Gambar 4.49 Konfigurasi Percobaan MITM dengan Bettercap	87
Gambar 4.50 Percobaan Akses Website ERP dengan Jaringan HTTP	87
Gambar 4.51 Kerentanan Timestamp Disclosure pada Pemindaian ZAP	88
Gambar 4.52 Response Header pada Kerentanan Timestamp Disclosure	89
Gambar 4.53 Kerentanan Content Type Options pada Pemindaian ZAP	89
Gambar 4.54 Request dan Response Kerentanan Content Type Options	90
Gambar 4.55 Payload Percobaan Serangan XSS	92
Gambar 4. 56 Payload Percobaan Serangan XSS	92
Gambar 4.57 Alert Serangan XSS Berhasil Ditambahkan	93
Gambar 4.58 Dashboard XSS Hunter	93
Gambar 4.59 Alur Serangan Session Hijacking	94
Gambar 4.60 Cookie Pengguna yang Sudah Login pada Windows	95
Gambar 4.61 Request Response Session Hijacking pada Kali Linux	95
Gambar 4.62 Halaman imitasi untuk Serangan CSRF	96
Gambar 4.63 Form Eksekusi CSRF Melalui Tombol Apply	97
Gambar 4.64 Request Response Serangan CSRF	97
Gambar 4.65 Halaman Login setelah Serangan CSRF Dilakukan	98

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Tabel 2.1 Model Kualitas Produk Security pada ISO/IEC 25010	20
Tabel 3.1 Halaman pada aplikasi yang berinteraksi dengan SPV Marketing.....	31
Tabel 3.2 Informasi dan Legalitas Pengujian	39
Tabel 3.3 Tools dan Teknik Intelligence Gathering.....	40
Tabel 3.4 Tools Pengujian Kerentanan	44
Tabel 4.1 Hasil Kesepakatan dan Legalitas Pengujian	47
Tabel 4.2 Query Google Dorking	49
Tabel 4.3 Aset Perusahaan PT. XYZ	54
Tabel 4.4 Ancaman Terhadap Aset Perusahaan PT. XYZ	56
Tabel 4.5 Aset PT. XYZ yang Berpotensi Terancam	57
Tabel 4.6 Potongan Hasil Pemindaian Kerentanan OWASP ZAP	62
Tabel 4.7 Hasil Pengujian URL dengan Kerentanan Content Type	91
Tabel 4.8 Hasil Pengumpulan Data pada Tahap Intelligence Gathering.....	99
Tabel 4.9 Hasil Pengujian Kerentanan Tahap Exploitation	99
Tabel 4.10 Hasil Eksploitasi Lebih Dalam Tahap Post-Exploitation.....	101

Halaman ini sengaja dikosongkan

DAFTAR LAMPIRAN

Lampiran 1. Hasil Query Google Dorking pada Pencarian Google.....	115
Lampiran 2. Surat Pernyataan Kesiediaan Kerjasama – Bagian 1.....	116
Lampiran 3. Surat Pernyataan Kesiediaan Kerjasama – Bagian 2.....	117
Lampiran 4. Kuesioner Identifikasi Aktor Ancaman pada Website ERP	118
Lampiran 5. Detail Kerentanan Vulnerable JS Library pada Zaproxy.org.....	119
Lampiran 6. Detail Kerentanan Application Error Disclosure pada Zaproxy.org	119
Lampiran 7. Detail Kerentanan CSP Header Not Set pada Zaproxy.org	119
Lampiran 8. Detail Kerentanan Cross Domain Misconfiguration pada Zaproxy.org	120
Lampiran 9. Detail Kerentanan Missing Anti-clickjacking Header pada Zaproxy.org.....	120
Lampiran 10. Detail Kerentanan Big Redirect Detected pada Zaproxy.org.....	120
Lampiran 11. Detail Kerentanan Cookie No HttpOnly Flag pada Zaproxy.org.....	121
Lampiran 12. Detail Kerentanan Cookie Without Secure Flag di Zaproxy.org	121
Lampiran 13. Detail Kerentanan Cookie without SameSite Attribute pada Zaproxy.org.....	121
Lampiran 14. Detail Kerentanan Cross-Domain JS Inclusion pada Zaproxy.org.....	122
Lampiran 15. Detail Kerentanan Server Leaks Version Information pada Zaproxy.org	122
Lampiran 16. Detail Kerentanan Strict-Transport-Security Header pada Zaproxy.org	122
Lampiran 17. Detail Kerentanan Timestamp Disclosure – Unix pada Zaproxy.org.....	123
Lampiran 18. Detail Kerentanan X-Content-Type-Options Header pada Zaproxy.org	123
Lampiran 19. Detail Kerentanan Authentication Request Identified pada Zaproxy.org.....	123
Lampiran 20. Detail Kerentanan Information Disclosure pada Zaproxy.org	124
Lampiran 21. Detail Kerentanan Modern Web Application pada Zaproxy.org	124
Lampiran 22. Detail Kerentanan Retrieved from Cache pada Zaproxy.org.....	124
Lampiran 23. Detail Kerentanan Session Management Response pada Zaproxy.org	125
Lampiran 24. Detail Kerentanan User Agent Fuzzer pada Zaproxy.org.....	125
Lampiran 25. Detail Kerentanan User Controllable HTML Attribute pada Zaproxy.org.....	125
Lampiran 26. Rincian Hasil Pemindaian Kerentanan OWASP ZAP.....	126