



SKRIPSI

**ANALISIS CELAH KEAMANAN WEBSITE
DINAS SOSIAL SURABAYA MENGGUNAKAN
METODE PENETRATION TESTING OWASP
TOP 10 DAN MITRE ATT&CK**

BREGAS ARYA BAGASKARA
NPM 20081010108

DOSEN PEMBIMBING

Dr. Ir. Mohammad Idhom, SP., S.Kom., MT.
Henni Endah Wahanani, ST., M.Kom.

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

LEMBAR PENGESAHAN

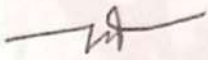
ANALISIS CELAH KEAMANAN WEBSITE DINAS SOSIAL SURABAYA MENGUNAKAN METODE PENETRATION TESTING OWASP TOP 10 DAN MITRE ATT&CK

Oleh :
BREGAS ARYA BAGASKARA
NPM. 20081010108

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada tanggal 21 Januari 2025

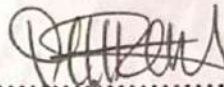
Menyetujui

Dr. Ir. Mohammad Idhom, SP., S.Kom., MT.
NIP. 19830310 2021211 006


.....

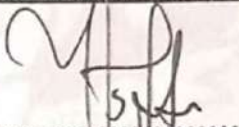
(Pembimbing I)

Henni Endah Wahanani, ST., M.Kom.
NIP. 19780922 2021212 005


.....

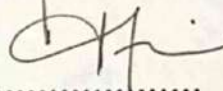
(Pembimbing II)

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.
NIP. 19681126 199403 2 001

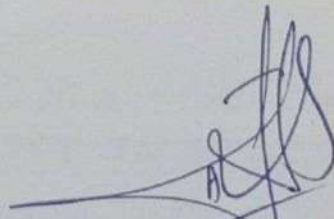
LEMBAR PERSETUJUAN

ANALISIS CELAH KEAMANAN WEBSITE DINAS SOSIAL SURABAYA
MENGUNAKAN METODE PENETRATION TESTING
OWASP TOP 10 DAN MITRE ATT&CK

Oleh:
BREGAS ARYA BAGASKARA
NPM. 20081010108

Menyetujui,

Koordinator Program Studi Informatika
Fakultas Ilmu Komputer



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

NIP. 19820211 2021212 005

SURAT PERNYATAAN BEBAS PLAGIASI

Saya yang bertanda tangan dibawah ini :

Nama : Bregas Arya Bagaskara
NPM : 20081010108
Program : Sarjana(S1)
Program Studi : Informatika
Fakultas : Ilmu Komputer

Menyatakan bahwa dalam dokumen ilmiah 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/Tesis/Desertasi ini, 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, 11 Maret 2025

Yang Membuat pernyataan



Bregas Arya Bagaskara

20081010108

ABSTRAK

Nama Mahasiswa / NPM : Bregas Arya Bagaskara / 20081010108
Judul Skripsi : Analisis Celah Keamanan Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing OWASP Top 10 Dan MITRE ATT&CK
Dosen Pembimbing : 1. Mohammad Idhom, SP., S.Kom., MT.
2. Henni Endah Wahanani, ST., M.Kom.

Keamanan sistem informasi merupakan aspek penting dalam pengembangan teknologi informasi, terutama pada aplikasi pelayanan publik seperti *website* Dinas Sosial Surabaya. Kemajuan teknologi meningkatkan potensi munculnya celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada *website* tersebut menggunakan metode *penetration testing* dengan pendekatan OWASP Top 10 dan MITRE ATT&CK. Proses pengujian melibatkan lima tahap utama, yaitu *information gathering, footprinting & scanning, vulnerability assessment, exploitation, serta analyze & report*. Pendekatan OWASP Top 10 digunakan untuk mengevaluasi sepuluh kerentanan paling kritis pada aplikasi web, sementara MITRE ATT&CK membantu memahami taktik dan teknik serangan yang relevan. Hasil pengujian menunjukkan bahwa dari 17 kerentanan yang teridentifikasi, terdapat enam kerentanan utama yang terbukti, yaitu *Browsable Web Directories, web.config File Information Disclosure, Content Security Policy (CSP) Header Not Set, Strict-Transport-Security (HSTS) Header Not Set, Timestamp Disclosure - Unix, dan X-Content-Type-Options Header Missing*. Untuk mengatasi kerentanan tersebut, disarankan penerapan *header* keamanan seperti *CSP, HSTS, dan X-Content-Type-Options: nosniff*, serta pengamanan terhadap direktori dan file konfigurasi sensitif guna meminimalkan risiko kebocoran data. Penelitian ini memberikan wawasan penting dalam meningkatkan keamanan sistem informasi pada sektor pemerintahan sehingga mampu melindungi data pengguna dari ancaman siber secara optimal.

Kata kunci : *Penetration testing, OWASP Top 10, MITRE ATT&CK, Website, Siber, Keamanan, Kerentanan.*

ABSTRACT

Student Name / NPM : Bregas Arya Bagaskara / 20081010108
Thesis Title : Security Gap Analysis of Surabaya Social Service
Website Using OWASP Top 10 Penetration
Testing Method and MITRE ATT&CK
Advisor : 1. Mohammad Idhom, SP., S.Kom., MT.
2. Henni Endah Wahanani, ST., M.Kom.

Information system security is a crucial aspect of technological development, especially in public service applications such as the Surabaya Social Service website. Technological advancements increase the potential for security vulnerabilities that can be exploited by malicious actors. This study aims to identify and analyze vulnerabilities on the website using penetration testing methods with the OWASP Top 10 and MITRE ATT&CK approaches. The testing process involves five main stages: information gathering, footprinting & scanning, vulnerability assessment, exploitation, and analyze & report. The OWASP Top 10 approach is used to evaluate the ten most critical vulnerabilities in web applications, while MITRE ATT&CK helps understand relevant attack tactics and techniques. The testing results show that out of 17 identified vulnerabilities, six major vulnerabilities were confirmed, namely Browsable Web Directories, web.config File Information Disclosure, Content Security Policy (CSP) Header Not Set, Strict-Transport-Security (HSTS) Header Not Set, Timestamp Disclosure - Unix, and X-Content-Type-Options Header Missing. To address these vulnerabilities, the implementation of security headers such as CSP, HSTS, and X-Content-Type-Options: nosniff is recommended, along with securing directories and sensitive configuration files to minimize data leakage risks. This study provides valuable insights into improving information system security in the government sector, ensuring better protection of user data from cyber threats.

Keywords: Penetration testing, OWASP Top 10, MITRE ATT&CK, Website, Cyber, Security, Vulnerability.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT atas segala rahmat, hidayah dan karunia-Nya kepada penulis sehingga skripsi dengan judul **“Analisis Celah Keamanan Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing OWASP Top 10 Dan MITRE ATT&CK”** dapat terselesaikan dengan baik.

Penulisan laporan skripsi ini menerima bantuan dari berbagai pihak, baik itu berupa moril, spiritual maupun materil. Untuk itu, dengan tulus, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ir. Akhmad Fauzi, M.MT., selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Ibu Dr. Ir. Novirina Hendrasarie, M.T., selaku Dekan Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Ibu Fetty Tri Anggraeny, S.Kom., M.Kom., selaku Koordinator Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Dr. Eng. Ir. Anggraini Puspita Sari, MT., selaku Dosen Wali penulis.
5. Bapak Mohammad Idhom, SP., S.Kom., M.T., selaku Dosen Pembimbing I yang meluangkan waktu, tenaga, serta pikiran untuk membimbing dan mengarahkan penulis selama proses penyelesaian skripsi.
6. Ibu Henni Endah Wahanani, ST., M.Kom., selaku Dosen Pembimbing II yang telah memberikan arahan, dukungan, serta saran kepada penulis sehingga penulis dapat menyelesaikan penyusunan skripsi.
7. Seluruh Dosen Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jawa Timur yang telah memberikan ilmunya kepada penulis selama perkuliahan.
8. Kedua orang tua penulis dan keluarga penulis yang senantiasa untuk mendoakan, dan memberikan dukuan selama proses penulisan skripsi ini.
9. Amanda selaku perempuan yang saya temukan di masa perkuliahan yang selalu memberikan senyuman dan semangat, sehingga membuat saya semakin giat mengerjakan Skripsi.
10. Anggota Grup Densus 88 yang selalu menghibur ketika stress.

11. Seluruh teman teman pengurus HIMATIFA UPN “Veteran” Jawa Timur periode 2020/2021, dan periode 2022/2023 yang telah menemani hari hari saya berkuliah, dan menemani proses perkembangan softskill saya selama perkuliahan
12. Seluruh teman teman Angkatan 2020 Informatika UPN Veteran Jawa Timur.
13. Semua pihak pihak yang bersinggungan kepada saya, yang tidak dapat saya sebutkan satu persatu.

Penulis menyadari bahwa di dalam penyusunan skripsi ini banyak terdapat kekurangan. Untuk itu kritik dan saran yang membangun dari semua pihak sangat diharapkan demi kesempurnaan penulisan skripsi ini. Akhirnya, dengan segala keterbatasan yang penulis miliki semoga laporan ini dapat bermanfaat bagi semua pihak umumnya dan penulis pada khususnya.

Surabaya, 19 Desember 2024

Penulis

DAFTAR ISI

SKRIPSI.....	i
LEMBAR PENGESAHAN	iii
SURAT PERNYATAAN ORISINALITAS	vii
ABSTRAK	ix
KATA PENGANTAR.....	xiii
DAFTAR ISI.....	xv
DAFTAR GAMBAR.....	xix
DAFTAR TABEL	xxv
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 Masalah	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terdahulu	5
2.2. Gambaran Umum Instansi.....	8
2.2.1. Profil Instansi	8
2.2.2. Susunan Organisasi	9
2.3. Penetration Testing	10
2.3.1 Engagement.....	14
2.3.2 Information Gathering.....	15
2.3.3 Footprinting & Scanning.....	15
2.3.4 Vulnerability Assessment.....	15
2.3.5 Exploitation	15
2.3.6 Analyze & Report	16
2.4. CIA Triad	16
2.5. CVE & CWE.....	18
2.6. OWASP Top 10	19
2.7. MITRE ATT&CK.....	33
2.8. Google Dorking.....	41

BAB III DESAIN DAN IMPLEMENTASI SISTEM	53
3.1. Studi Literatur	53
3.2. Objek Penelitian	53
3.3. Cara Kerja Sistem	53
3.4. Metode Penelitian	55
3.4.1. Pendekatan OWASP Top 10 dan MITRE ATT&CK dalam Penetration Testing.....	55
3.4.2. Alur Penelitian	57
3.4.3. Alat Bantu Penelitian	68
BAB IV PENGUJIAN DAN ANALISA	71
4.1. Information Gathering	71
4.1.1. Wappalyzer.....	71
4.1.2. Nslooup	72
4.1.3. Whois	72
4.1.4. Nmap.....	73
4.1.5. Dirsearch	74
4.1.6. Google Dorking.....	76
4.2. Footprinting & Scanning	77
4.2.1. OWASP ZAP	77
4.2.2. Nessus.....	77
4.2.3. OpenVAS	78
4.3. Vulnerability Assessment.....	79
4.4. Exploitation	80
4.4.1. Big Redirect Detected (Potential Sensitive Information Leak)	81
4.4.2. <i>Cookie</i> No HttpOnly Flag	83
4.4.3. <i>Cookie</i> Without Secure Flag	86
4.4.4. Cross-Domain JavaScript Source File Inclusion.....	88
4.4.5. Strict-Transport-Security Header Not Set.....	90
4.4.6. Timestamp Disclosure – Unix.....	94
4.4.7. X-Content-Type-Options Header Missing.....	97
4.4.8. Browsable Web Directories	99

4.4.9. web.config File Information Disclosure.....	103
4.4.10. Absence of Anti-CSRF Tokens.....	105
4.4.11. Content Security Policy (CSP) Header Not Set	107
4.4.12. Multiple X-Frame-Options Header Entries.....	111
4.4.13. Vulnerable JS Library	114
4.4.14. SQL Injection – SQLite.....	115
4.4.15. CGI Generic SQL Injection (Blind).....	120
4.4.16. Open Redirect.....	124
4.4.17. Cross-Site Scripting.....	126
4.5. Analyze & Report.....	130
4.5.1. Hasil	130
4.5.2. Rekomendasi Perbaikan	131
4.5.3. Validasi Kerentanan Yang Diperbaiki	140
BAB V.....	143
5.1. Kesimpulan	143
5.2. Saran.....	144
DAFTAR PUSTAKA	147
LAMPIRAN.....	153

DAFTAR GAMBAR

Gambar 2.1 Logo Dinas Sosial Surabaya	8
Gambar 2.2 Struktur organisasi Dinas Sosial Surabaya.....	9
Gambar 2.3 CIA Triad	16
Gambar 2.4 Perubahan OWASP Top 10 2021.....	19
Gambar 2.5 Logo Mozilla Firefox	43
Gambar 2.6 Logo Wappalizer	44
Gambar 2.7 Logo VirtualBox	44
Gambar 2.8 Logo Kali Linux	45
Gambar 2.9 Logo Nmap.....	46
Gambar 2.10 Logo Dirsearch.....	47
Gambar 2.11 Logo Nessus	47
Gambar 2.12 Logo SQLMap	48
Gambar 2.13 Logo Bettercap	48
Gambar 2.14 Logo OpenVAS.....	49
Gambar 2.15 Logo OWASP ZAP	50
Gambar 2.16 Logo Burp Suite	50
Gambar 3.1 Halaman utama <i>website</i> Dinas Sosial Surabaya.....	54
Gambar 3.2 Diagram Use Case <i>website</i> Dinas Sosial Surabaya.....	54
Gambar 3.3 Flowchart Alur Penelitian	57
Gambar 3.4 Hasil <i>scanning</i> menggunakan OWASP ZAP.....	61
Gambar 3.5 Hasil <i>scanning</i> menggunakan Nessus	62
Gambar 3.6 Hasil <i>scanning</i> menggunakan OpenVAS.....	62
Gambar 3.7 Tampilan <i>dashboard</i> Burp Suite	67
Gambar 4.1 Hasil <i>scan</i> web dengan Wappalyzer.....	71
Gambar 4.2 Hasil <i>scan</i> web dengan Nslookup	72
Gambar 4.3 Hasil <i>scan</i> web dengan Whois	72
Gambar 4.4 Hasil <i>scan</i> web dengan Nmap	73
Gambar 4.5 Hasil <i>scan</i> web dengan Nmap secara detail	74
Gambar 4.6 Hasil <i>scan</i> web dengan Dirsearch	74
Gambar 4.7 Hasil detail <i>scan website</i> dengan Dirsearch.....	75
Gambar 4.8 Hasil <i>scanning</i> menggunakan OWASP ZAP.....	77

Gambar 4.9 Hasil <i>scanning</i> menggunakan Nessus	78
Gambar 4.10 Hasil <i>scanning</i> menggunakan OpanVAS	78
Gambar 4.11 Hasil pemindaian kerentanan <i>Big Redirect Detected (Potential Sensitive Information Leak)</i> dengan ZAP	81
Gambar 4.12 Beberapa halaman yang terindikasi <i>Big Redirect Detected (Potential Sensitive Information Leak)</i>	81
Gambar 4.13 Penangkapan <i>request</i> untuk URL https://dinassosial.surabaya.go.id/assets menggunakan Burp Suite <i>Intercept</i>	82
Gambar 4.14 <i>Response</i> untuk URL https://dinassosial.surabaya.go.id/assets	82
Gambar 4.15 Tampilan <i>website</i> pada URL https://dinassosial.surabaya.go.id/assets	82
Gambar 4.16 Modifikasi <i>Response</i> untuk URL https://dinassosial.surabaya.go.id/assets	83
Gambar 4.17 Tampilan <i>website</i> setelah <i>response</i> dimodifikasi	83
Gambar 4.18 Hasil pemindaian kerentanan <i>Cookie No HttpOnly Flag</i> dengan ZAP	84
Gambar 4.19 Hasil inspeksi <i>cookie browser</i> pada halaman profil	84
Gambar 4.20 <i>Request website</i> untuk halaman profil	85
Gambar 4.21 <i>Response website</i> untuk halaman profil	85
Gambar 4.22 Percobaan memasukan skrip menggunakan <i>console browser</i> pada <i>website</i>	85
Gambar 4.23 Hasil pemindaian kerentanan <i>Cookie Without Secure Flag</i> dengan ZAP	86
Gambar 4.24 Hasil inspeksi <i>cookie browser</i> pada halaman profil	86
Gambar 4.25 <i>Response website</i> pada halaman profil	87
Gambar 4.26 <i>Response website</i> pada halaman profil	87
Gambar 4.27 Tampilan <i>website</i> setelah <i>cookie</i> berhasil diedit	88
Gambar 4.28 Hasil pemindaian kerentanan <i>Cross-Domain JavaScript Source File Inclusion</i> dengan ZAP	89
Gambar 4.29 Hasil deteksi <i>file</i> JavaScript dari <i>domain</i> lain pada URL https://dinassosial.surabaya.go.id/	89

Gambar 4.30 Hasil deteksi <i>file</i> JavaScript dari <i>domain</i> lain pada URL https://dinassosial.surabaya.go.id/pelayanan	90
Gambar 4.31 Hasil pemindaian kerentanan <i>Strict-Transport-Security Header Not Set</i> dengan ZAP	91
Gambar 4.32 Implementasi HSTS pada <i>website</i> Cloudflare.....	91
Gambar 4.33 <i>Response header website</i> Dinas Sosial Surabaya bagian profil	92
Gambar 4.34 Bettercap untuk melacak data sensitif pada <i>website</i> Dinas Sosial Surabaya.....	92
Gambar 4.35 Perhitungan CVSS 3.1 terhadap kerentanan <i>Strict-Transport-Security Header Not Set</i>	93
Gambar 4.36 Hasil pemindaian kerentanan <i>Timestamp Disclosure – Unix</i>	94
Gambar 4.37 Tampilan URL yg terindikasi rentan <i>Timestamp Disclosure – Unix</i>	94
Gambar 4.38 Respon header URL yg terindikasi rentan <i>Timestamp Disclosure – Unix</i>	95
Gambar 4.39 Respon header URL yg terindikasi rentan <i>Timestamp Disclosure – Unix</i>	95
Gambar 4.40 Perhitungan CVSS 3.1 terhadap kerentanan <i>Timestamp Disclosure – Unix</i>	96
Gambar 4.41 Hasil pemindaian kerentanan <i>X-Content-Type-Options Header Missing</i> dengan ZAP	97
Gambar 4.42 <i>Response web</i> pada Youtube.....	97
Gambar 4.43 <i>Response web</i> pada <i>website</i> Dinas Sosial Surabaya.....	98
Gambar 4.44 Perhitungan CVSS 3.1 terhadap kerentanan <i>X-Content-Type-Options Header Missing</i>	98
Gambar 4.45 Hasil pemindaian kerentanan <i>Browsable Web Directories</i> dengan Nessus	99
Gambar 4.46 Tampilan <i>website</i> pada <i>endpoint</i> pertama	100
Gambar 4.47 Tampilan <i>parent directory</i> pada <i>endpoint</i> pertama	100
Gambar 4.48 Tampilan <i>website</i> pada <i>endpoint</i> kedua	101
Gambar 4.49 Tampilan <i>website</i> pada <i>endpoint</i> ketiga	101

Gambar 4.50 Perhitungan CVSS 3.1 terhadap kerentanan <i>Browsable Web Directories</i>	102
Gambar 4.51 Hasil pemindaian kerentanan <i>web.config File Information Disclosure</i> dengan Nessus.....	103
Gambar 4.52 <i>Request</i> yang didapatkan dari Nessus	103
Gambar 4.53 <i>Response</i> yang diberikan oleh <i>website</i>	104
Gambar 4.54 Perhitungan CVSS 3.1 terhadap kerentanan <i>web.config File Information Disclosure</i>	105
Gambar 4.55 Hasil pemindaian kerentanan <i>Absence of Anti-CSRF Tokens</i> dengan ZAP	106
Gambar 4.56 <i>CSRF Tokens</i> pada <i>website</i> shopee	106
Gambar 4.57 Tampilan <i>website</i> yang terdeteksi <i>Absence of Anti-CSRF Tokens</i>	107
Gambar 4.58 Hasil pemindaian kerentanan <i>Content Security Policy (CSP) Header Not Set</i> dengan ZAP Halaman Utama.....	107
Gambar 4.59 Hasil pemindaian kerentanan <i>Content Security Policy (CSP) Header Not Set</i> dengan ZAP Halaman Login.....	108
Gambar 4.60 Implementasi <i>Content Security Policy (CSP)</i> pada <i>id.pinterest.com</i>	108
Gambar 4.61 <i>Output console</i> web <i>id.pinterest.com</i>	109
Gambar 4.62 <i>Response headers</i> pada halaman utama	109
Gambar 4.63 <i>Output console</i> halaman utama	109
Gambar 4.64 <i>Response headers</i> pada halaman <i>login</i>	110
Gambar 4.65 <i>Output console</i> halaman <i>login</i>	110
Gambar 4.66 Perhitungan CVSS 3.1 terhadap kerentanan <i>Content Security Policy (CSP) Header Not Set</i>	111
Gambar 4.67 Hasil pemindaian kerentanan <i>Multiple X-Frame-Options Header</i>	112
Gambar 4.68 Hasil pemindaian kerentanan <i>Multiple X-Frame-Options Header</i>	112
Gambar 4.69 Kode <i>website</i> sederhana menggunakan <code><iframe></code>	113
Gambar 4.70 Tampilan <i>website</i> dari kode sederhana.....	113
Gambar 4.71 Hasil pemindaian kerentanan <i>Vulnerable JS Library</i> dengan ZAP	114
Gambar 4.72 Tampilan <i>website</i> pada url yang terindikasi kerentanan	114

Gambar 4.73 Hasil pemindaian kerentanan <i>SQL Injection</i> – <i>SQLite</i> dengan ZAP	115
Gambar 4.74 <i>Request</i> saat melakukan <i>login</i>	116
Gambar 4.75 <i>Response</i> saat melakukan <i>login</i>	116
Gambar 4.76 Waktu Pemrosesan <i>Request</i>	116
Gambar 4.77 <i>Request</i> saat melakukan <i>login</i> yang disuntikan skrip SQL	117
Gambar 4.78 <i>Response</i> saat melakukan <i>login</i> yang disuntikan skrip SQL.....	117
Gambar 4.79 Waktu Pemrosesan <i>Request</i> skrip SQL <code>randblob(1000000000)</code>	117
Gambar 4.80 <i>Request</i> saat melakukan <i>login</i> yang disuntikan skrip SQL berbeda	118
Gambar 4.81 <i>Response</i> saat melakukan <i>login</i> yang disuntikan skrip SQL berbeda	118
Gambar 4.82 Waktu Pemrosesan <i>Request</i> skrip SQL <code>randblob(10000000000)</code>	118
Gambar 4.83 Waktu Pemrosesan percobaan kedua mengirim <i>Request</i> skrip SQL <code>randblob(1000000000)</code>	119
Gambar 4.84 Waktu Pemrosesan percobaan kedua mengirim <i>Request</i> skrip SQL <code>randblob(10000000000)</code>	119
Gambar 4.85 Waktu Pemrosesan percobaan mengirim <i>Request</i> dengan skrip SQL <code>randblob(5000000000)</code>	119
Gambar 4.86 Hasil percobaan serangan <i>SQL Injection</i> menggunakan <code>sqlmap</code> pada halaman <i>login</i>	120
Gambar 4.87 Hasil pemindaian kerentanan <i>CGI Generic SQL Injection (Blind)</i>	121
Gambar 4.88 Hasil muatan URL dengan parameter “keyword” kosong	121
Gambar 4.89 Hasil muatan URL dengan parameter yang terindikasi	122
Gambar 4.90 Hasil muatan URL dengan mengganti isi parameter “keyword” ..	122
Gambar 4.91 Hasil percobaan memasukan skrip <i>SQL Injection</i>	123
Gambar 4.92 Percobaan serangan <i>SQL Injection</i> menggunakan <code>sqlmap</code>	124
Gambar 4.93 <i>Redirect detected</i> pada halaman <i>login</i>	125
Gambar 4.94 Hasil dari percobaan <i>open redirect</i>	125
Gambar 4.95 <i>Request</i> yang memungkinkan terdapat kerentanan XSS.....	126

Gambar 4.96 <i>Request</i> yang berisi skrip XSS	127
Gambar 4.97 Hasil menyuntikan skrip javascript pada fitur <i>search</i>	127
Gambar 4.98 Uji Coba teknik Brute Force menggunakan Burp Suite Intruder	128
Gambar 4.99 <i>Payloads</i> skrip javascript untuk teknik Brute Force	128
Gambar 4.100 Hasil pengujian menggunakan teknik Brute Force	129
Gambar 4.101 Contoh konfigurasi pada <i>.htaccess</i>	132
Gambar 4.102 Penempatan konfigurasi <i>.htaccess</i> pada direktori yang ingin diarahkan ke halaman 403 <i>Forbidden</i>	132
Gambar 4.103 Sebelum penambahan konfigurasi <i>.htaccess</i> pada direktori	133
Gambar 4.104 Sesudah penambahan konfigurasi <i>.htaccess</i> pada direktori	133
Gambar 4.105 Contoh konfigurasi pada <i>nginx.conf</i>	134
Gambar 4.106 Letak <i>file web.config</i>	134
Gambar 4.107 <i>Response</i> sebelum penambahan konfigurasi	134
Gambar 4.108 <i>Response</i> sebelum penambahan konfigurasi	135
Gambar 4.109 Contoh implementasi CSP pada <i>website</i> sederhana	136
Gambar 4.110 Tampilan <i>website</i> sederhana	136
Gambar 4.111 Percobaan menyuntikan skrip pada <i>console browser</i>	136
Gambar 4.112 Contoh implementasi HSTS pada <i>website</i> sederhana	137
Gambar 4.113 <i>Response headers</i> sebelum penambahan konfigurasi HSTS	137
Gambar 4.114 <i>Response headers</i> setelah penambahan konfigurasi HSTS	137
Gambar 4.115 Contoh konfigurasi mengatur <i>timestamp disclosure</i>	138
Gambar 4.116 Contoh implementasi <i>X-Content-Type-Options</i>	139
Gambar 4.117 <i>Response headers</i> sebelum penambahan <i>X-Content-Type-Options</i>	139
Gambar 4.118 <i>Response headers</i> setelah penambahan <i>X-Content-Type-Options</i>	140
Gambar 4.119 Kerentanan <i>web.config file information disclosure</i>	140
Gambar 4.120 <i>Request</i> yang sama dari Nessus	141
Gambar 4.121 <i>Response website</i> setelah perubahan	141
Gambar 4.122 <i>Response</i> pada pada halaman <i>website</i>	142

DAFTAR TABEL

Tabel 3.1 Perencanaan pengumpulan data dan informasi.....	58
Tabel 3.2 Daftar kerentanan yang akan dieksploitasi	63
Tabel 4.1 Rencana pengujian pada daftar kerentanan.....	64
Tabel 4.2 Hasil pemindaian dengan Google Dorking.....	76
Tabel 4.3 Hasil <i>vulnerability assessment</i>	79
Tabel 4.4 Hasil <i>information gathering</i>	130
Tabel 4.5 Hasil pengujian eksploitasi	131
Tabel 4.6 Rekomendasi perbaikan	132

