

**PENGUJIAN CELAH KEAMANAN WEBSITE POSKETANMU
DENGAN GOOGLE PENETRATION TESTING DAN
METODE OWASP TOP 10 2021**

SKRIPSI



Oleh :

AIDA FITRIYA SEBRINA

NPM 20081010035

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2024**

**PENGUJIAN CELAH KEAMANAN WEBSITE
POSKETANMU DENGAN GOOGLE PENETRATION
TESTING DAN METODE OWASP TOP 10 2021**

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan Dalam Menempuh Gelar
Sarjana Komputer Program Studi Informatika



Oleh :

AIDA FITRIYA SEBRINA

NPM 20081010035

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2024**

LEMBAR PENGESAHAN SKRIPSI

**Judul : PENGUJIAN · CELAH KEAMANAN WEBSITE
POSKETANMU DENGAN GOOGLE PENETRATION
TESTING DAN METODE OWASP TOP 10 2021**

Oleh : Aida Fitriya Sebrina

NPM : 20081010035

**Telah Diseminarkan Dalam Ujian Skripsi Pada :
Hari Rabu, Tanggal 22 Mei 2024**

Mengetahui

1. **Dosen Pembimbing**



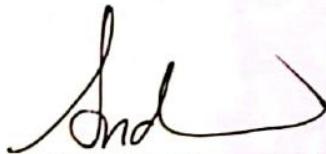
Achmad Junaidi, S.Kom., M.Kom
NPT : 378110401991

1. **Dosen Penguji**



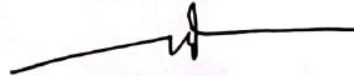
Henni Endah Wahanani, ST. M.Kom.
NIP. 19780922 2021212 005

2.



Andreas Nugroho Sihananto, S.Kom., M.Kom
NPT. 211199 00 412271

2.



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

Menyetujui

**Dekan
Fakultas Ilmu Komputer**



Prof. Dr. Ir. Novirina Hendrasarie, MT
NIP. 19681126 199403 2 001

**Koordinator Program Studi
Informatika**



Fetty Tri Anggraeny, S.Kom., M.Kom
NIP. 19820211 2021212 005

SURAT PERNYATAAN ANTI PLAGIAT

Saya mahasiswa Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur, yang bertanda tangan di bawah ini:

Nama : Aida Fitriya Sebrina

NPM : 20081010035

Dengan ini menyatakan bahwa judul skripsi atau tugas akhir yang saya ajukan dan kerjakan, yang berjudul:

“PENGUJIAN CELAH KEAMANAN WEBSITE POSKETANMU
MENGUNAKAN GOOGLE PENETRATION TESTING DAN METODE
OWASP TOP 10 2021”

Bukan merupakan plagiat dari skripsi atau tugas akhir maupun penelitian orang lain dan juga bukan merupakan produk atau software yang saya beli dari pihak lain. Saya juga menyatakan bahwa skripsi ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam daftar pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di Universitas Pembangunan Nasional “Veteran” Jawa Timur maupun institusi pendidikan lainnya.

Jika ternyata kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.



Surabaya, 28 Mei 2024

Hormat Saya,



Aida Fitriya Sebrina
NPM. 20081010035

PENGUJIAN CELAH KEAMANAN WEBSITE POSKTENAMU MENGUNAKAN TEKNIK GOOGLE PENETRATION TESTING DAN METODE OWASP TOP 10

Nama Mahasiswa : Aida Fitriya Sebrina

NPM : 20081010035

Program Studi : Informatika

Dosen Pembimbing : Achmad Junaidi, S.Kom., M.Kom.

: Andreas Nugroho Sihananto, S.Kom., M.Kom

ABSTRAK

Dalam era digital yang semakin berkembang, isu keamanan siber menjadi semakin penting. Website Posketanmu, sebagai platform yang mengelola dan menyimpan data penduduk Kabupaten Mojokerto, memiliki tanggung jawab untuk menjaga keamanan data tersebut dari potensi serangan siber. Oleh karena itu, penelitian ini dilakukan dengan tujuan untuk mengidentifikasi, mengevaluasi, dan mengeksploitasi kerentanan keamanan pada website Posketanmu dengan menggunakan metode *Google Penetration Testing* dan OWASP Top 10 2021. Penelitian ini melibatkan lima tahap penting dalam *penetration testing*. Tahap pertama adalah pengumpulan informasi dan pengenalan dengan menggunakan berbagai tools seperti Nmap, Nslookup, Wappalizer, Whatweb, Whois, dan *Google Hacking*. Tahap kedua adalah pemindaian kerentanan dengan menggunakan ZAP, yang menghasilkan temuan kerentanan dengan berbagai tingkat. Tahap ketiga adalah penilaian kerentanan, yang melibatkan uji manual dan kategorisasi berdasarkan OWASP. Tahap keempat adalah eksploitasi, di mana 11 kerentanan berhasil dieksploitasi. Tahap kelima adalah pelaporan dimana tahap ini berisi laporan hasil pengujian dan rekomendasi perbaikan dari celah keamanan yang berhasil di temukan berdasarkan OWASP Top 2021. Dengan menerapkan metode *Google Penetration Testing* dan OWASP Top 10 2021, penelitian ini berhasil mengungkap dan merekomendasikan solusi dari empat celah keamanan pada website Posketanmu. Celah keamanan tersebut yaitu, kerentanan XSS *stored*, CSP *header not set*, *Strict-Transport security header not set* dan kerentanan *open redirect*. Penerapan metode *Google Penetration Testing* dan OWASP top 10 2021 membantu meningkatkan keamanan website Posketanmu dan data penduduk Kabupaten Mojokerto lebih terlindungi keamanannya. Rekomendasi perbaikan yang diberikan dapat membantu website Posketanmu menjadi lebih aman dan tahan terhadap serangan siber.

Kata Kunci : Website, Google Penetration Testing, OWASP Top 10 2021

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, atas segala limpahan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan skripsi yang berjudul "PENGUJIAN CELAH KEAMANAN WEBSITE POSKETANMU DENGAN GOOGLE PENETRATION TESTING DAN METODE OWASP TOP 10 2021" ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan Sarjana (S1) di Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur.

Penulis menyadari bahwa dalam penulisan skripsi ini, terdapat keterbatasan. Dengan rendah hati, penulis menerima saran dan kritik yang membangun. Semoga skripsi ini memberikan manfaat bagi semua pihak, termasuk pembaca dan penelitian di masa depan. Meskipun masih jauh dari sempurna, penulis berharap kritik dan saran konstruktif akan membantu perbaikan di masa yang akan datang.

Surabaya, 28 Mei 2024

Penulis

UCAPAN TERIMA KASIH

Penulisan laporan skripsi ini tidak dapat terwujud tanpa bantuan, motivasi, dan dukungan dari berbagai pihak. Oleh karena itu, dengan tulus, penulis ingin 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 dan Dosen Wali penulis.
4. Bapak Achmad Junaidi, S.Kom., M.Kom., selaku Dosen Pembimbing II yang meluangkan waktu, tenaga, serta pikiran untuk membimbing dan mengarahkan penulis selama proses penyelesaian skripsi.
5. Bapak Andreas Nugroho Sihananto, S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan arahan, dukungan, serta saran kepada penulis sehingga penulis dapat menyelesaikan penyusunan skripsi.
6. Seluruh Dosen Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jawa Timur yang telah memberikan ilmunya kepada penulis selama perkuliahan.
7. Kedua orang tua penulis, Mbak hilda, Mas Novan, Fara dan keluarga penulis yang senantiasa untuk mendoakan, dan memberikan dukuan selama proses penulisan skripsi ini.
8. Sahabat – sahabat penulis, Lila, Wiji, Putri, Tataks, Kharisma, Nabila, Firda dan Teman – teman kos. Terimakasih karena selalu ada disamping penulis selama menyelesaikan perjalanan ini.

Penulis hanya bisa berharap, semoga Tuhan Yang Maha Esa senantiasa memberi perlindungan dan membalas semua kebaikan yang telah diberikan.

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI.....	i
SURAT PERNYATAAN ANTI PLAGIAT.....	ii
ABSTRAK.....	iii
KATA PENGANTAR.....	iv
UCAPAN TERIMA KASIH.....	v
DAFTAR ISI.....	vi
DAFTAR TABEL.....	viii
DAFTAR GAMBAR.....	ix
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan Penelitian.....	3
1.4. Manfaat Penelitian.....	4
1.5. Batasan Masalah.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terdahulu.....	5
2.2. Dinas kependudukan dan Pencatatan Sipil Kabupaten Mojokerto.....	7
2.2.1 Visi dan Misi.....	8
2.2.2 Tugas Pokok dan Fungsi.....	8
2.2.3 Struktur Organisasi.....	9
2.3. Website Posketanmu.....	9
2.4. <i>Penetration Testing</i>	10
2.4.1 <i>Reconnaissance dan Information Gathering</i>	13
2.4.2 <i>Google Hacking</i>	14
2.4.3 <i>Vulnerability Scanning</i>	14
2.4.4 <i>Vulnerability Assesment</i>	15
2.4.5 <i>Exploitation</i>	15
2.4.6 <i>Reporting</i>	16
2.5. OWASP TOP 10 2021.....	16
2.6. Alat bantu.....	29
2.6.1 Kali Linux.....	30
2.6.2 Mozilla Firefox.....	30
2.6.3 Whois.....	31
2.6.4 Wappalizer.....	31
2.6.5 Nslookup.....	31
2.6.6 Nmap.....	32
2.6.7 Wireshark.....	32
2.6.8 Bettercap.....	33
2.6.9 Whatweb.....	33
2.6.10 OWASP Zed Attack Proxy (ZAP).....	33
2.6.11 Burp Suite.....	35
BAB III METODOLOGI PENELITIAN.....	37
3.1 Studi Literatur.....	37
3.2 Cara Kerja Sistem.....	38
3.3 Reconnaissance & Information Gathering.....	40

3.4	<i>Vulnerability scanning</i>	43
3.5	<i>Vulnerability Assessment</i>	45
3.6	<i>Exploitation</i>	45
3.7	<i>Reporting</i>	49
BAB IV	HASIL DAN PEMBAHASAN	52
4.1	<i>Information Gathering</i>	52
4.1.1	<i>Nslookup</i>	52
4.1.2	<i>Nmap</i>	53
4.1.3	<i>Whois</i>	53
4.1.4	<i>Informasi arsitektur</i>	55
4.1.5	<i>Google Dorking</i>	57
4.2	<i>Vulnerability Scanning</i>	58
4.2.1	<i>OWASP ZAP</i>	58
4.3	<i>Vulnerability Assessment</i>	59
4.4	<i>Exploitation</i>	61
4.4.1	<i>Content Security Policy (CSP) Header Not Set</i>	61
4.4.2	<i>CDM-001 Cross Domain Misconfiguration</i>	73
4.4.3	<i>BDR-001 Big Redirect Detected (Potential Sensitive Information Leak)</i>	76
4.4.4	<i>Open Redirect</i>	78
4.4.5	<i>CNH-001 Cookie No HttpOnly Flag</i>	90
4.4.6	<i>CWS-001 Cookie Without Secure Flags</i>	94
4.4.7	<i>XJS-001 Cross domain javascript file inclusion</i>	98
4.4.8	<i>SMC-001 Secure Page Include Mix Content</i>	101
4.4.9	<i>STS-001 Strict-Transport-Security Header Not Set</i>	103
4.4.10	<i>TDS-001 Timestamp Disclosure - Unix</i>	107
4.4.11	<i>Cross-Site Scripting</i>	110
4.5	<i>Reporting</i>	114
4.5.1	<i>Hasil</i>	114
4.5.2	<i>Rekomendasi Perbaikan</i>	116
BAB V	PENUTUP.....	119
5.1	<i>Kesimpulan</i>	119
5.2	<i>Saran</i>	120
DAFTAR	PUSTAKA	120
Lampiran	122
Lampiran	Surat.....	122

DAFTAR TABEL

Tabel 3. 1. Daftar alat serta rencana penggunaan	40
Tabel 3. 2. Eksploitasi kerentanan	46
Tabel 3. 3. <i>Tools</i> yang digunakan untuk <i>eksploitasi</i>	46
Tabel 3. 4. Rencana pengujian	48
Tabel 3. 5. Kerentanan website dan dampaknya	50
Tabel 4. 1. Hasil pemindaian dengan <i>google dorking</i>	57
Tabel 4. 2. Hasil <i>vulnerability assesment</i>	60
Tabel 4. 3. Pengujian serangan XSS	113
Tabel 4. 4. Hasil <i>information gathering</i>	114
Tabel 4. 5. Hasil pengujian	115
Tabel 4. 6. Rekomendasi perbaikan	116

DAFTAR GAMBAR

Gambar 1. 0. Dispendukcapil Kab. Mojokerto	7
Gambar 2. 0. Website Posketanmu	10
Gambar 2. 1. Daftar OWASP TOP 10 edisi 2021	17
Gambar 2. 2. Kali Linux	30
Gambar 2. 3. Nmap pada kali linux.....	32
Gambar 2. 4. OWASP ZAP	34
Gambar 2. 5. Aplikasi Burp Suite	36
Gambar 3. 1. Metodologi penelitian.....	37
Gambar 3. 2. Use Case website Posketanmu.....	39
Gambar 3. 3. Gambar scanning dengan ZAP	44
Gambar 4. 1. Hasil scan nslookup	52
Gambar 4. 2. Hasil scan nmap.....	53
Gambar 4. 3. Hasil scan Whois	54
Gambar 4. 4. Scan lanjutan whois	55
Gambar 4. 5. Hasil scan web dengan wappalyzer	56
Gambar 4. 6. Hasil scan whatweb	57
Gambar 4. 7. Hasil pemindaian ZAP.....	59
Gambar 4. 8. Kerentanan <i>content-security-policy header not set</i>	61
Gambar 4. 9. Halaman yang terindikasi kerentanan <i>CSP header not set</i>	62
Gambar 4. 10. Implementasi CSP pada website id.pinterest.com.....	62
Gambar 4. 11. <i>Output</i> consol web id.pinterest.com.....	63
Gambar 4. 12. Respon <i>header</i> halaman /help	63
Gambar 4. 13. <i>Output</i> konsol browser halaman /help	64
Gambar 4. 14. Respon <i>header</i> halaman /login	64
Gambar 4.15. Output konsol browser halaman /login	65
Gambar 4. 16. Respon <i>header</i> halaman /mojokertoku	65
Gambar 4. 17. Output konsol browser halaman mojokertoku	66
Gambar 4. 18. Respon <i>header</i> halaman /dashboard-akta.....	66
Gambar 4. 19. Output konsol browser halaman akta.....	67
Gambar 4. 20. Respon <i>header</i> halaman /tambah pengajuan	67
Gambar 4. 21. Output konsol halaman /tambah-pengajuan.....	68
Gambar 4. 22. Respon <i>header</i> halaman /tambah-pengajuan.....	68
Gambar 4. 23. Output konsol browser /halaman /pengajuan-akta	69
Gambar 4. 24. Respon <i>header</i> halaman /pengajuan	69
Gambar 4. 25. Output konsol browser /halaman/pengajuan	70
Gambar 4. 26. Respon <i>header</i> halaman /profil.....	70
Gambar 4. 27. Output konsol halaman /profil	71
Gambar 4. 28. Respon <i>header</i> halaman pindah-masuk/register.....	71
Gambar 4. 29. Output konsol browser pindah-masuk/register	72
Gambar 4. 30. Respon <i>header</i> halaman /register.....	72
Gambar 4. 31. Output konsol browser halaman /register	73
Gambar 4. 32. Halaman yang terindikasi rentan <i>cross domain missconfiguration</i>	73
Gambar 4. 33. <i>Request</i> dan <i>response</i> halaman /mojokertoku	74
Gambar 4. 34. Menambahkan 'origin' pada <i>header request</i>	75
Gambar 4. 35. <i>Respon header</i> halaman dashboard-akta/pengajuan.....	75
Gambar 4. 36. Hasil scanning Zap dgn URL yg terindikasi rentan <i>big redirect</i>	76
Gambar 4. 37. <i>Request Post</i> halaman /login-action pengguna.....	77
Gambar 4. 38. Pengubahan <i>Referer</i> dengan Http://attacker.com/	77
Gambar 4. 39. Hasil pengubahan <i>referer</i> dengan HTTP	78
Gambar 4.40. <i>Respon header</i> halaman /mojokertoku.....	78

Gambar 4. 41. Request dan response halaman login petugas	79
Gambar 4. 42. Permintaan GET halaman /login-action-petugas	80
Gambar 4. 43. Respon browser saat berhasil <i>redirect</i>	80
Gambar 4. 44. POST /login-action halaman pengguna	81
Gambar 4. 45. Menambahkan ' <i>referer</i> ' pada method POST	82
Gambar 4. 46. Halaman login pengguna berhasil <i>redirect</i>	82
Gambar 4. 47. GET halaman /dashboard KIA	83
Gambar 4. 48. Hasil perubahan <i>referer</i>	83
Gambar 4. 49. Get halaman /dashboard-akta.....	84
Gambar 4. 50. Hasil perubahan <i>referer</i> halaman dashboard KIA	85
Gambar 4. 51. <i>Request</i> Get halaman e-KTP	86
Gambar 4. 52. Hasil perubahan <i>referrer</i> halaman E-KTP	86
Gambar 4. 53. <i>Request</i> GET halaman /dashboard-kk.....	87
Gambar 4. 54. Hasil perubahan <i>referer</i> halaman /dashboard-kk.....	88
Gambar 4. 55. <i>Request</i> GET halaman /pindah-keluar	89
Gambar 4. 56. Hasil perubahan <i>referer</i> halaman /mojokertoku/pindah-keluar	89
Gambar 4. 57. Gambar hasil <i>scanning</i> kerentanan <i>cookie no httpOnly flag</i>	90
Gambar 4. 58. <i>Request</i> GET halaman /mojokertoku	91
Gambar 4. 59. <i>Response</i> halaman /mojokertoku	91
Gambar 4. 60. <i>Request</i> GET /logout halaman posketanmu	92
Gambar 4. 61. Mencoba <i>Login</i> kembali dengan cookie awal	93
Gambar 4. 62. Output konsol browser saat ingin mengambil sesi cookie	93
Gambar 4. 63. Hasil <i>scanning</i> kerentanan <i>cookie without secure flag dengan ZAP</i>	94
Gambar 4. 64. <i>Response</i> halaman /mojokertoku	95
Gambar 4. 65. Wireshark saat monitoring lalu lintas web posketanmu	96
Gambar 4. 66. Cookie editor untuk XSRF token <i>login</i> website posketanmu.....	96
Gambar 4. 67. Cookie editor untuk laravel session <i>login</i> website posketanmu	97
Gambar 4. 68. Respon website setelah <i>cookie</i> berhasil di edit	98
Gambar 4. 69. Hasil <i>scanning</i> ZAP pada halaman yg terindikasi rentan <i>Cross Domain Javascript</i>	99
Gambar 4. 70. Kode Javascript yg terindikasi rentan	99
Gambar 4. 71. Penyisipan <i>payload</i> XSS pada <i>function success</i>	100
Gambar 4. 72. Penyisipan <i>payload</i> XSS pada <i>function notify error</i>	100
Gambar 4. 73. Output konsol saat menginputkan <i>documen.domain</i>	100
Gambar 4. 74. Halaman website yg terindikasi rentan	101
Gambar 4. 75. File <i>img source</i> yg terindikasi rentan	102
Gambar 4. 76. Hasil inspeksi URL yang teridikasi rentan.....	102
Gambar 4. 77. Hasil <i>scanning</i> ZAP pada kerentanan <i>Strict-Transport-Security Header</i> not set.....	103
Gambar 4. 78. Implementasi HSTS pada website Cloudflare	104
Gambar 4. 79. Respon <i>header</i> web posketanmu	105
Gambar 4. 80. Detail security web Posketanmu.....	105
Gambar 4. 81. Bettercap untuk melacak data sensitive pada website Posketanmu.....	105
Gambar 4. 82. Wireshark untuk memantau lalu lintas HTTP pada website Posketanmu	106
Gambar 4. 83. Hasil <i>scanning</i> ZAP pada halaman web yang terindikasi rentan <i>timestamp disclosure</i>	107
Gambar 4. 84. Tampilan URL yg terindikasi rentan <i>Timestamp Disclosure</i>	108
Gambar 4. 85. Respon <i>header</i> URL yg terindikasi rentan <i>Timestamp Disclosure</i>	109
Gambar 4. 86. Respon <i>header</i> website posketanmu	109
Gambar 4. 87. Serangan XSS pada web posketanmu	110
Gambar 4. 88. <i>Request</i> POST halaman /post-akta.....	111
Gambar 4. 89. Penyisipan <i>payload</i> XSS pada parameter pengajuan	111
Gambar 4. 90. Respon <i>header</i> setelah penyisipan <i>payload</i> XSS	112

Gambar 4. 91. Respon UI website saat berhasil disisipkan *payload* XSS 112