

**ANALISIS KEAMANAN WEBSITE DENGAN METODE OWASP (OPEN
WEB APPLICATION SECURITY PROJECT) (STUDI KASUS:
fts.ump.ac.id)**



SKRIPSI

MOCHAMAD DEDE NURSIDI

1903040161

**TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
JANUARI 2024**

**ANALISIS KEAMANAN WEBSITE DENGAN METODE OWASP (OPEN
WEB APPLICATION SECURITY PROJECT) (STUDI KASUS:
fts.ump.ac.id)**



SKRIPSI

**Diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana
Komputer**

MOCHAMAD DEDE NURSIDI

1903040161

**TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
JANUARI 2024**

HALAMAN PERSETUJUAN

Skripsi ini diajukan oleh :

Nama : Mochamad Dede Nursidi
NIM : 1903040161
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto
Judul : Analisis Keamanan Website Dengan Metode OWASP (*Open Web Application Security Project*)
(Studi Kasus: fts.ump.ac.id)

telah diterima dan disetujui
Purwokerto, 9 Januari 2024

Pembimbing



Harjono, S.T., M.Eng.

NIK.2160389

HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama : Mochamad Dede Nursidi
NIM : 1903040161
Jurusan : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto
Judul : Analisis Keamanan Website Dengan Metode
OWASP (*Open Web Application Security Project*)
(Studi Kasus: fts.ump.ac.id)

telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

DEWAN PENGUJI

Penguji 1 (Pembimbing) : Harjono, S.T., M.Eng.
Penguji 2 : Mukhlis Prasetyo Aji S.T., M.Kom.
Penguji 3 : Agung Purwo Wicaksono S.T., M.Kom.
Ditetapkan di : Purwokerto
Tanggal : 9 Januari 2025

Mengetahui,

Dekan Fakultas Teknik dan Sains,



Dr. T. Ir. Iskahar, S.T., M.T.

NIK. 2160207

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertanda tangan dibawah ini:

Nama : Mochamad Dede Nursidi
NIM : 1903040161
Jurusan : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah hasil karya saya dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar dan bukan hasil dari penjiplakan dari karya orang lain.

Demikian pernyataan ini saya buat dan apabila kelak dikemudian hari terbukti ada unsur penjiplakan, saya bersedia mempertanggungjawabkan sesuai dengan ketentuan yang berlaku.

Purwokerto, 9 Januari 2024

Yang membuat menyatakan



M. Dede Nursidi

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademika Universitas Muhammadiyah Purwokerto dan demi pengembangan ilmu pengetahuan, saya yang bertanda tangan dibawah ini:

Nama : Mochamad Dede Nursidi
NIM : 1903040161
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto
Jenis Karya : Skripsi

Menyetujui untuk memberikan Hak Bebas Royalti Noneksklusif (Non-exclusive Royalti-Free Right) kepada Universitas Muhammadiyah Purwokerto atas karya saya yang berjudul:

ANALISIS KEMAMAN WEBSITE DENGAN METODE OWASP (OPEN
WEB APPLICATION SECURITY PROJECT) (STUDI KASUS:
FTS.UMP.AC.ID)

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Muhammadiyah Purwokerto berhak menyimpan, mengalihmedia/ mengalihinformatkan, mengelola dalam bentuk pangkalan data, merawat, dan mempublikasikan skripsi saya dengan tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sadar dan sebenar-benarnya.

Dibuat di: Purwokerto

Pada tanggal : 9 Januari

Yang menyatakan,



M. Dede Nursidi

MOTTO

Setiap lembar yang ditulis adalah langkah menuju masa depan, setiap rintangan yang dihadapi adalah bukti ketangguhan, dan setiap doa yang dipanjatkan adalah kekuatan tak terlihat. Tetap semangat membangun mimpi dengan kerja keras dan ketangguhan hati.



HALAMAN PERSEMBAHAN

Dengan segala kerendahan hati, serta rasa syukur terhadap Allah SWT yang memberikan rahmat dan nikmat-Nya, maka saya persembahkan Laporan Skripsi ini kepada:

1. Allah SWT yang senantiasa melimpahkan nikmat dan kasih sayang-Nya, sehingga dapat melaksanakan Penelitian Skripsi di Universitas Muhammadiyah Purwokerto.
2. Orang tua serta saudara yang senantiasa memberikan semangat, bimbingan, dan doanya untuk saya sampai saat ini.
3. Bapak Harjono, S.T., M.Eng selaku Dosen Pembimbing Skripsi yang telah membimbing dan mengarahkan penyusun selama rangkaian penelitian skripsi.
4. Kepada semua teman seperjuangan angkatan 2019 Teknik Informatika yang sudah memberikan banyak pengalaman dalam kehidupan saya.
5. Serta semua pihak yang tidak dapat disebutkan satu per satu yang telah membantu penyusunan menyelesaikan skripsi ini.

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT yang telah memberikan rahmat dan karunia- Nya, sehingga penyusun dapat menyelesaikan Laporan Skripsi dengan judul “Analisis Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) (Studi Kasus: fts.ump.ac.id)”. Penelitian Skripsi ini merupakan salah satu persyaratan kurikulum untuk menyelesaikan pendidikan sarjana pada Program Studi Teknik Informatika Fakultas Teknik dan Sains Universitas Muhammadiyah Purwokerto.

Pelaksanaan Skripsi ini dimaksudkan agar mahasiswa memperoleh pengalaman, wawasan di dunia kerja, sekaligus mempelajari ilmu baru dan mengerti kehidupan di dunia kerja. Dengan mengikuti Skripsi ini diharapkan dapat memotivasi untuk belajar lebih giat karena telah melihat kenyataan yang ada di lapangan, dimana mahasiswa dituntut untuk selalu belajar dan meningkatkan kualitas pribadi.

Laporan ini jauh dari kata sempurna dan masih banyak kekurangan mengingat keterbatasan pengalaman dan kemampuan, oleh karena itu kritik dan saran yang membangun sangat diharapkan demi hasil yang lebih baik di masa mendatang. Akhirnya, besar harapan agar kehadiran laporan skripsi ini dapat memberikan manfaat yang berarti untuk para pembaca.

Penyusun,

M. Dede Nursidi

DAFTAR ISI

HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN ORISINALITAS.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIK	vi
MOTTO	vii
HALAMAN PERSEMBAHAN	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
ABSTRAK	xvii
ABSTRAC.....	xviii
BAB I PENDAHULUAN	1
A. LATAR BELAKANG	1
B. RUMUSAN MASALAH.....	3
C. BATASAN MASALAH.....	3
D. TUJUAN PENELITIAN.....	4
E. MANFAAT PENELITIAN	4
BAB II TINJAUAN PUSTAKA	5
A. PENELITIAN TERDAHULU.....	5
B. LANDASAN TEORI.....	12
1. Website.....	12
2. Vulnerability.....	12
3. OWASP WSTG (Web Security Testing Guide)	12

4.	OWASP ZAP.....	16
5.	Penetration Testing.....	16
6.	Keamanan Informasi.....	17
BAB III METODE PENELITIAN		18
A.	JENIS PENELITIAN	18
B.	URAIAN.....	19
1.	Studi Literatur	19
2.	Pengumpulan Data.....	19
3.	Penetrasi dengan referensi OWASP WSTG v4.2.....	22
4.	Analisis Dan Laporan	31
BAB IV HASIL DAN PEMBAHASAN.....		32
A.	HASIL.....	32
1.	Information Gathering	32
2.	Configurasi dan Deploy Management Testing.....	39
3.	Identity Management Testing.....	47
4.	Authentication Testing	51
5.	Authorization Testing.....	57
6.	Session Management Testing.....	59
7.	Input Validation Testing	63
8.	Testing for Error Handling	71
9.	Testing for Weak Cryptography.....	73
10.	Business Logic Testing.....	76
11.	Client-side Testing	80
12.	API Testing.....	86
B.	PEMBAHASAN	87
1.	Hasil Pengujian Web Security Testing Guide (WSTG) versi 4.2	87

2. Hasil Pengujian WSTG 4.2 Berdasarkan OWASP TOP 10	110
3. Analisis	114
BAB V KESIMPULAN DAN SARAN	116
A. KESIMPULAN.....	116
B. SARAN.....	116
DAFTAR PUSTAKA	117



DAFTAR TABEL

Table 1. Penelitian terdahulu	5
Table 2. Kebutuhan Perangkat Lunak.....	20
Table 3. <i>Information gathering</i>	23
Table 4. <i>Configuration and Deployment Management Testing</i>	24
Table 5. <i>Identity Management Testing</i>	25
Table 6. Authentication Testing	25
Table 7. <i>Authorization Testing</i>	26
Table 8. <i>Session Management Testing</i>	27
Table 9. <i>Input Validation Testing</i>	27
Table 10. <i>Testing For Error Handling</i>	29
Table 11. <i>Testing For Weak Cryptography</i>	29
Table 12. <i>Bussines logic test</i>	29
Table 13. <i>Client-Side Testing</i>	30
Table 14. <i>API Testing</i>	31
Table 15. Pengujian Web Security Testing Guide (WSTG) v4.2	87
Table 16. Pengujian WSTG 4.2 Berdasarkan OWASP TOP 10	110

DAFTAR GAMBAR

Gambar 1. Perbandingan OWASP Top 10 Tahun 2017 dan 2021	13
Gambar 2. Langkah-langkah Penelitian	18
Gambar 3. Pengujian <i>ip address</i> dan <i>ip server</i>	33
Gambar 4. Hasil pengujian <i>port</i> pintu terbuka pada <i>server</i>	34
Gambar 5. Hasil mengidentifikasi <i>server</i>	35
Gambar 6. Hasil menganalisis <i>header</i> HTTP.....	36
Gambar 7. Hasil identifikasi file.....	37
Gambar 8. Hasil pemeriksaan informasi kerentanan <i>server</i>	37
Gambar 9. Hasil pengujian peninjauan halaman web	38
Gambar 10. Hasil identifikasi <i>metode web</i>	39
Gambar 11. Hasil identifikasi konfigurasi infrastruktur jaringan.....	40
Gambar 12. Pengujian konfigurasi platform aplikasi.....	41
Gambar 13. Pengujian penanganan ekstensi untuk informasi sensitive.....	42
Gambar 14. Pengujian peninjauan cadangan lama.....	42
Gambar 15. Pengujian infrastruktur dan antarmuka admin aplikasi	43
Gambar 16. Pengujian metode HTTP	44
Gambar 17. Pengujian keamanan transportasi ketat HTTP.....	44
Gambar 18. Hasil identifikasi cross domain.....	45
Gambar 19. Pengujian pengambilalihan subdomain	46
Gambar 20. Pengujian penyimpanan <i>cloud</i>	47
Gambar 21. Pengujian definisi peran tes	48
Gambar 22. Pengujian proses pendaftaran pengguna.....	48
Gambar 23. Pengujian penyediaan akun percobaan.....	49
Gambar 24. Pengujian pencacahan akun dan akun pengguna yang dapat ditebak.....	50
Gambar 25. Menguji kebijakan pengguna yang lemah	50
Gambar 26. Pengujian kredensial yang terangkut melalui saluran tereksripsi.....	51
Gambar 27. Pengujian kredensial default.....	52
Gambar 28. Pengujian mekanisme penguncian yang lemah	52
Gambar 29. Pengujian untuk melewati skema autentikasi	53
Gambar 30. Pengujian rentan ingat kata sandi	54

Gambar 31. Pengujian kelemahan <i>cache browser</i>	54
Gambar 32. Pengujian kebijakan kata sandi lemah.....	55
Gambar 33. Pengujian jawaban pertanyaan keamanan lemah	55
Gambar 34. Pengujian untuk perubahan kata sandi yang lemah.....	56
Gambar 35. Pengujian otentikasi yang lemah	56
Gambar 36. Pengujian <i>file</i> traversal termasuk direktori.....	57
Gambar 37. Pengujian untuk melewati skema otorisasi.....	58
Gambar 38. Pengujian eskalasi hak istimewa	58
Gambar 39. Pengujian referensi objek langsung yang tidak aman.....	59
Gambar 40. Pengujian skema manajemen sesi.....	60
Gambar 41. Pengujian <i>Attribute Cookies</i>	60
Gambar 42. Pengujian fiksasi sesi.....	61
Gambar 43. Pengujian pemalsuan permintaan lintas situs	62
Gambar 44. Pengujian pembajakan sesi penyerang	62
Gambar 45. Pengujian <i>reflected cross-site scripting</i>	63
Gambar 47. Pengujian gangguan kata kerja HTTP.....	64
Gambar 48. Pengujian polusi parameter HTTP.....	65
Gambar 49. Pengujian untuk sql injeksi.....	65
Gambar 50. Pengujian injeksi protokol akses direktori ringan	66
Gambar 51. Pengujian injeksi XML.....	67
Gambar 55. Pengujian injeksi kode.....	67
Gambar 56. Pengujian injeksi perintah	68
Gambar 57. Pengujian untuk injeksi string format.....	68
Gambar 58. Pengujian kerentanan yang diinkubasi	69
Gambar 60. Pengujian permintaan masuk HTTP	69
Gambar 61. Pengujian injeksi <i>host header</i>	70
Gambar 62. Pengujian injeksi template sisi server.....	70
Gambar 63. Pengujian pemalsuan permintaan sisi server	71
Gambar 64. Pengujian kesalahan kode.....	72
Gambar 65. Pengujian pelacakan tumpukan	72
Gambar 66. Hasil pengujian keamanan transport lemah.....	73
Gambar 67. Pengujian padding oracle.....	74

Gambar 68. Pengujian informasi sensitive dikirim saluran tidak terenkripsi.....	75
Gambar 69. Pengujian enkripsi lemah.....	75
Gambar 70. Pengujian validasi data logika bisnis.....	76
Gambar 71. Pengujian kemampuan memalsukan permintaan.....	77
Gambar 72. Pengujian pemeriksaan integritas	77
Gambar 73. Pengujian pertahanan terhadap penyalahgunaan aplikasi.....	79
Gambar 74. Pengujian unggah uji berkas berbahaya	79
Gambar 75. Pengujian pembuatan skrip situs berbasis DOM.....	80
Gambar 77. Pengujian untuk injeksi <i>HTML</i>	81
Gambar 79. Pengujian untuk injeksi <i>CSS</i>	81
Gambar 80. Pengujian manipulasi sumber daya sisi klien.....	82
Gambar 81. Pengujian berbagi sumber daya lintas asal.....	82
Gambar 83. Pengujian <i>clickjacking</i>	83
Gambar 84. Pengujian <i>WebSocket</i>	84
Gambar 85. Pengujian pesan web.....	84
Gambar 86. Pengujian penyimpanan browser.....	85
Gambar 87. Pengujian penyertaan skrip lintas situs.....	85
Gambar 88. Pengujian <i>GrapQL</i>	86

ABSTRAK

Dalam era digital saat ini, website sering digunakan untuk mengelola berbagai jenis data, mulai dari informasi pribadi pengguna, transaksi keuangan, hingga data sensitif perusahaan. Oleh karena itu, memastikan keamanan data menjadi aspek penting dalam pengembangan dan pengelolaan aplikasi berbasis website. Dengan demikian, keamanan website merupakan aspek penting yang harus diperhatikan. Maka, perlu dilakukan pengujian terhadap celah keamanan, karena kekuatan sistem keamanan berpengaruh langsung terhadap keberlanjutan sebuah website. Metode pengujian OWASP WSTG Versi 4.2 memungkinkan pengujian secara detail, dengan hasil yang disesuaikan pada OWASP Top 10—sebuah daftar kerentanan yang digunakan sebagai acuan dalam penilaian. Berdasarkan pengujian penetrasi didalam website fts.ump.ac.id menggunakan metode WSTG (Web Security Testing Guide) Versi 4.2, ditemukan celah keamanan berbahaya sesuai OWASP TOP 10, di antaranya: *Broken Access Control*, *Insecure Design*, *Security Misconfiguration*, dan *Vulnerable and Outdated Components*. Hasil analisis kerentanan ini diharapkan dapat membantu pengelola dan pengembang sistem menyadari potensi risiko sehingga dapat mengambil tindakan pencegahan serius yang dapat membayakan website fts.ump.ac.id.

Kata Kunci: *Keamanan, Website, OWASP, WSTG*

ABSTRAC

In today's digital era, websites are often used to manage various types of data, ranging from users' personal information and financial transactions to sensitive corporate data. Therefore, ensuring data security through websites has become a crucial aspect of web application development and management. For this reason, website security is an essential aspect that must be prioritized. Security testing is necessary to identify vulnerabilities, as the strength of a security system directly impacts the sustainability of a website. The OWASP WSTG Version 4.2 testing methodology enables detailed assessments with results aligned to the OWASP Top 10—a list of vulnerabilities used as a benchmark for evaluation. Based on penetration testing conducted on the website fts.ump.ac.id using the WSTG (Web Security Testing Guide) Version 4.2 method, critical security vulnerabilities were identified according to the OWASP Top 10, including Broken Access Control, Insecure Design, Security Misconfiguration, and Vulnerable and Outdated Components. The findings from this vulnerability analysis are expected to help system administrators and developers recognize potential risks and take serious preventive measures to safeguard the website fts.ump.ac.id from harm.

Key Words: *Security, Website, OWASP, WSTG*