

**ANALISIS KEAMANAN SISTEM MENGGUNAKAN METODE  
OWASP (OPEN WEB APPLICATION SECURITY PROJECT)  
(STUDI KASUS: PRAKERIN.SMKKESATRIANPWT.SCH.ID)**



**SKRIPSI**

**FAHRIEL ARYA PRATAMA**

**1903040115**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN SAINS  
UNIVERSITAS MUHAMMADIYAH PURWOKERTO  
OKTOBER 2023**

**ANALISIS KEAMANAN SISTEM MENGGUNAKAN METODE  
OWASP (OPEN WEB APPLICATION SECURITY PROJECT)  
(STUDI KASUS: PRAKERIN.SMKKESATRIANPWT.SCH.ID)**



**SKRIPSI**

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

**FAHRIEL ARYA PRATAMA**

**1903040115**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN SAINS  
UNIVERSITAS MUHAMMADIYAH PURWOKERTO  
OKTOBER 2023**

## HALAMAN PERSETUJUAN

Skripsi ini diajukan oleh:

Nama : Fahriel Arya Pratama

NIM : 1903040115

Program Studi : Teknik Informatika

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Judul : Analisis Keamanan Sistem Menggunakan  
Metode OWASP (*Open Web Application  
Security Project*)  
(Studi Kasus: [prakerin.smkkesatrianpwt.sch.id](http://prakerin.smkkesatrianpwt.sch.id))

telah diterima dan disetujui

Purwokerto, 24 Oktober 2023

PEMBIMBING

Ermadi Satriya Wijaya, S.T., M.Kom

NIK. 2160767

## HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama : Fahriel Arya Pratama  
NIM : 1903040115  
Program Studi : Teknik Informatika  
Fakultas : Teknik dan Sains  
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto  
Judul : Analisis Keamanan Sistem Menggunakan Metode  
OWASP (*Open Web Application Security Project*)  
(Studi Kasus: [prakerin.smkkesatrianpwt.sch.id](http://prakerin.smkkesatrianpwt.sch.id))

telah berhasil dipertahankan di hadapan 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) : Ermadi Satriya Wijaya, S.T., M.Kom.  
Penguji 2 : Mukhlis Prasetyo Aji, S.T., M.Kom.  
Penguji 3 : Harjono, S.T., M.Eng.  
Ditetapkan di : Purwokerto  
Tanggal : 24 Oktober 2023

Mengetahui

Dekan Fakultas Teknik dan Sains

Ir. Teguh Mardiana, S.T., M.T., ASEAN.Eng., ACPE., IPM  
NIK. 2160172



## HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertandatangan dibawah ini:

Nama : Fahriel Arya Pratama  
NIM : 1903040115  
Program Studi : 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 di kutip maupun dirujuk telah saya nyatakan dengan benar serta bukan hasil penjiplakan dari karya orang lain.

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

Purwokerto, 24 Oktober 2023

Yang Membuat Pernyataan



Fahriel Arya Pratama

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIK

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

Nama : Fahriel Arya Pratama  
NIM : 1903040115  
Program Studi : Teknik Informatika  
Fakultas: : Teknik dan Sains  
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto  
Jenis Karya : Skripsi

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

ANALISIS KEAMANAN SISTEM MENGGUNAKAN METODE OWASP  
(OPEN WEB APPLICATION SECURITY PROJECT)  
(STUDI KASUS: PRAKERIN.SMKKESATRIANPWT.SCH.ID)

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

Pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Purwokerto

Pada tanggal : 24 Oktober 2023

Yang Menyatakan,



Fahriel Arya Pratama

## **MOTTO**

" Khoirunnas anfa'uhum linnas "

(Sebaik-baik manusia adalah yang paling bermanfaat bagi manusia lain)



## 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 Dinas Komunikasi dan Informatika Purbalingga.
2. Orang tua serta saudara yang senantiasa memberikan semangat, bimbingan, dan doanya untuk saya sampai saat ini.
3. Bapak Ermadi Satriya Wijaya, S.T., M.Kom 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 laporan 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 Sistem Menggunakan Metode OWASP (Open Web Application Security Project) (Studi Kasus: prakerin.smkkesatrianpwt.sch.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 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,

Fahriel Arya Pratama

## 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
DAFTAR LAMPIRAN.....	xviii
ABSTRAK.....	xix
ABSTRAC.....	xx
BAB I PENDAHULUAN.....	1
A. LATAR BELAKANG.....	1
B. PERUMUSAN 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.....	11

BAB III METODE PENELITIAN.....	17
A. JENIS PENELITIAN.....	17
B. METODE PENGUMPULAN DATA.....	18
C. WAKTU DAN TEMPAT .....	19
D. INSTUMEN PENELITIAN.....	20
E. FLOWCHART.....	22
F. TEKNIK PENGUJIAN.....	23
G. REPORTING.....	31
BAB IV HASIL DAN PEMBAHASAN .....	32
A. HASIL.....	32
1. Information Gathering .....	32
2. Configuration and 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 .....	64
8. Testing for Error Handling.....	76
9. Testing for Weak Cryptography .....	77
10. Business Logic Testing.....	80
11. Client-side Testing .....	84
12. API Testing .....	91
B. PEMBAHASAN .....	93
1. Hasil pengujian Web Security Testing Guide (WSTG) Versi 4.2 .....	93
2. Hasil Pengujian WSTG 4.2 berdasarkan OWASP TOP 10.....	115

3. Analisis .....	119
BAB V KESIMPULAN .....	122
A. KESIMPULAN .....	122
B. SARAN .....	122
DAFTAR PUSTAKA .....	123
LAMPIRAN .....	125



## DAFTAR TABEL

Tabel 1. Tabel perangkat lunak pengujian .....	20
Tabel 2. Information Gathering.....	23
Tabel 3. Configuration and Deployment Management Testing.....	24
Tabel 4. Identity Management Testing .....	25
Tabel 5. Authentication Testing .....	25
Tabel 6. Authorization Testing .....	26
Tabel 7. Session Management Testing.....	27
Tabel 8. Input Validation Testing .....	27
Tabel 9. Testing for Error Handling.....	29
Tabel 10. Testing for Weak Cryptography .....	29
Tabel 11. Business Logic Testing .....	29
Tabel 12. Client-side Testing .....	30
Tabel 13. API Testing .....	31
Tabel 14. Pengujian <i>Web Security Testing Guide</i> (WSTG) Versi 4.2 .....	93
Tabel 15. Pengujian WSTG 4.2 berdasarkan OWASP TOP 10 .....	115

## DAFTAR GAMBAR

Gambar 1. Perbandingan OWASP Top 10 tahun 2017 dan OWASP Top tahun 2021(OWASP, 2021) .....	12
Gambar 2. <i>Flowchart</i> .....	22
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> .....	36
Gambar 6. Hasil menganalisis <i>header HTTP</i> .....	36
Gambar 7. Hasil identifikasi <i>file</i> .....	37
Gambar 8. Hasil pemeriksaan informasi kerentanan <i>server</i> .....	38
Gambar 9. Hasil pengujian peninjauan konten halaman <i>web</i> .....	38
Gambar 10. Hasil identifikasi <i>framwework 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 .....	41
Gambar 14. Pengujian peninjauan cadangan lama .....	42
Gambar 15. Pengujian infrastruktur dan antarmuka admin aplikasi.....	43
Gambar 16. Pengujian metode <i>HTTP</i> .....	43
Gambar 17. Pengujian keamanan transportasi ketat <i>HTTP</i> .....	44
Gambar 18. Hasil <i>identifikasi cross domain policy</i> .....	45
Gambar 19. Pengujian izin <i>file</i> uji.....	45
Gambar 20. Pengujian pengambilalihan <i>subdomain</i> .....	46
Gambar 21. Pengujian penyimpanan <i>cloud</i> .....	47
Gambar 22. Pengujian definisi peran tes.....	48
Gambar 23. Pengujian proses pendaftaran pengguna .....	48
Gambar 24. Pengujian penyediaan akun percobaan .....	49
Gambar 25. Pengujian pencacahan akun dan akun pengguna yang dapat ditebak .....	50
Gambar 26. Menguji kebijakan nama pengguna yang lemah .....	50
Gambar 27. Pengujian kredensial yang diangkut melalui saluran terenkripsi .....	51
Gambar 28. Pengujian kredensial <i>default</i> .....	52

Gambar 29. Pengujian mekanisme penguncian yang lemah.....	52
Gambar 30. Pengujian untuk melewati skema autentikasi.....	53
Gambar 31. Pengujian rentan ingat kata sandi.....	54
Gambar 32. Pengujian kelemahan <i>cache browser</i> .....	54
Gambar 33. Pengujian kebijakan kata sandi lemah .....	55
Gambar 34. Pengujian jawaban pertanyaan keamanan lemah .....	55
Gambar 35. Pengujian untuk perubahan kata sandi yang lemah .....	56
Gambar 36. Pengujian otentikasi yang lemah.....	56
Gambar 37. Pengujian file traversal termasuk direktori .....	57
Gambar 38. Pengujian untuk melewati skema otorisasi .....	58
Gambar 39. Pengujian eskalasi hak istimewa.....	59
Gambar 40. Pengujian referensi objek langsung yang tidak aman .....	59
Gambar 41. Pengujian skema manajemen sesi .....	60
Gambar 42. Pengujian Atribut <i>Cookies</i> .....	61
Gambar 43. Pengujian fiksasi sesi .....	61
Gambar 44. Pengujian variabel sesi .....	62
Gambar 45. Pengujian pemalsuan permintaan lintas situs.....	62
Gambar 46. Pengujian fungsi <i>logout</i> .....	63
Gambar 47. Timeout sesi pengujian.....	63
Gambar 48. Pengujian untuk sesi membingungkan.....	64
Gambar 49. Pengujian pembajakan sesi penyerang.....	64
Gambar 50. Pengujian <i>reflected cross-site scripting</i> .....	65
Gambar 51. Pengujian untuk scripting lintas situs tersimpan.....	66
Gambar 52. Pengujian gangguan kata kerja <i>HTTP</i> .....	66
Gambar 53. Pengujian polusi parameter <i>HTTP</i> .....	67
Gambar 54. Pengujian untuk injeksi <i>SQL</i> .....	68
Gambar 55. Pengujian injeksi protokol akses direktori ringan.....	69
Gambar 56. Pengujian injeksi <i>XML</i> .....	69
Gambar 57. Pengujian <i>injeksi server-side included (SSI)</i> .....	70
Gambar 58. Pengujian untuk injeksi <i>XPath</i> .....	70
Gambar 59. Pengujian injeksi <i>SMTP IMAP</i> .....	71

Gambar 60. Pengujian injeksi kode .....	71
Gambar 61. Pengujian injeksi perintah .....	72
Gambar 62. Pengujian untuk injeksi string format .....	72
Gambar 63. Pengujian kerentanan yang diinkubasi.....	73
Gambar 64. Pengujian penyelundupan pemisahan <i>HTTP</i> .....	73
Gambar 65. Pengujian permintaan masuk <i>HTTP</i> .....	74
Gambar 66. Pengujian injeksi <i>host header</i> .....	74
Gambar 67. Pengujian injeksi template sisi <i>server</i> .....	75
Gambar 68. Pengujian pemalsuan permintaan sisi <i>server</i> .....	76
Gambar 69. Pengujian kesalahan kode .....	76
Gambar 70. Pengujian pelacakan tumpukan.....	77
Gambar 71. Hasil Pengujian keamanan lapisan transport lemah.....	78
Gambar 72. Pengujian <i>padding oracle</i> .....	78
Gambar 73. Pengujian informasi sensitif yang dikirim melalui saluran tidak terenkripsi.....	79
Gambar 74. Pengujian enkripsi lemah .....	79
Gambar 75. Pengujian validasi data logika bisnis .....	80
Gambar 76. Pengujian kemampuan memalsukan permintaan .....	81
Gambar 77. Pengujian pemeriksaan integritas.....	81
Gambar 78. Pengujian pertahanan terhadap penyalahgunaan aplikasi .....	83
Gambar 79. Pengujian unggah uji berkas berbahaya .....	83
Gambar 80. Pengujian pembuatan skrip situs berbasis <i>DOM</i> .....	84
Gambar 81. Pengujian untuk eksekusi <i>JavaScript</i> .....	85
Gambar 82. Pengujian untuk injeksi <i>HTML</i> .....	85
Gambar 83. Pengujian untuk pengalihan <i>URL</i> sisi klien .....	86
Gambar 84. Pengujian untuk injeksi <i>CSS</i> .....	86
Gambar 85. Pengujian manipulasi sumber daya sisi klien.....	87
Gambar 86. Pengujian berbagi sumber daya lintas asal.....	87
Gambar 87. Pengujian flashing lintas situs .....	88
Gambar 88. Hasil pengujian <i>clickjacking</i> .....	89
Gambar 89. Pengujian <i>WebSockets</i> .....	90

Gambar 90. Pengujian pesan <i>web</i> .....	90
Gambar 91. Pengujian penyimpanan <i>browser</i> .....	91
Gambar 92. Penguji penyertaan skrip lintas situs .....	91
Gambar 93. Pengujian <i>GraphQL</i> .....	92



## DAFTAR LAMPIRAN

Lampiran 1. Surat Perizinan Penelitian Dari SMK Kesatrian Purwokerto .....	125
Lampiran 2. Hasil Cek <i>Similarity</i> Laporan Skripsi.....	126
Lampiran 3. Pertimbangan Pembaharuan Website Sistem informasi Praktek Kerja Industri SMK Kesatrian Purwokerto.....	128



## ABSTRAK

Perkembangan teknologi informasi dalam jaringan komputer berkembang sangat pesat dan fleksibel. Internet merupakan jaringan komputer yang lazim digunakan karena kemudahan aksesnya. Hal ini akan beresiko terhadap persebaran informasi yang bersifat private. Seiring dengan pesatnya perkembangan teknologi tersebut, semakin besar pula ancaman dan gangguan terhadap kinerja dalam teknologi tersebut. Maka dari itu, perlu dilakukan pengujian celah keamanan, karena kuat lemahnya sistem keamanan akan berdampak langsung pada keberlangsungan SMK tersebut. Dengan menggunakan metode pengujian WSTG Versi 4.2 dapat menerapkan pengujian secara detail. Dari hasil pengujian disesuaikan dengan OWASP Top 10 yang didalamnya terdapat daftar kerentanan agar dari hasil pengujian telah dilakukan dapat disimpulkan. Berdasarkan hasil pengujian penetration menggunakan metode WSTG (*Web Security Testing Guide*) Versi 4.2, dapat diperoleh hasil bahwa terdapat celah keamanan yang berbahaya berdasarkan OWASP TOP 10 diantaranya yaitu: *Broken Access Control, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures*. Dari hasil analisa kerentanan ini dapat membantu para pengelola dan pengembang sistem untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut.

**Kata kunci:** *Keamanan Sistem, Penetrasi Testing, OWASP*

## ABSTRAC

*The development of information technology in computer networks is growing very rapidly and flexibly. The internet is a computer network that is commonly used because of its ease of access. This will pose a risk to the distribution of private information. Along with the rapid development of this technology, the threats and disruptions to the performance of this technology become greater. Therefore, it is necessary to test security gaps, because the strength and weakness of the security system will have a direct impact on the sustainability of the vocational school. By using the WSTG Version 4.2 testing method you can apply detailed testing. The test results are adjusted to the OWASP Top 10, which contains a list of vulnerabilities so that conclusions can be drawn from the test results that have been carried out. Based on the results of penetration testing using the WSTG method (Web Security Testing Guide) Version 4.2, results can be obtained that there are dangerous security gaps based on the OWASP TOP 10, including: Broken Access Control, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures. The results of this vulnerability analysis can help system managers and developers to be aware of the risks that may occur so they can take action to prevent and overcome these risks.*

**Keywords:** *System Security, Penetration Testing, OWASP*