

TUGAS AKHIR

**ANALISIS KEAMANAN APLIKASI BERBASIS WEB
MENGUNAKAN METODE *PENETRATION TESTING*
Studi Kasus: *E-commerce Assakinahmart***



MUHAMMAD YUWAN SAFRINACIKIT
2010651102

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2025

**ANALISIS KEAMANAN APLIKASI BERBASIS WEB
MENGUNAKAN METODE *PENETRATION TESTING*
Studi Kasus: *E-commerce Assakinahmart***

Disusun sebagai salah satu syarat untuk kelulusan
Strata Satu (S-1) Prodi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember



MUHAMMAD YUWAN SAFRI NACIKIT
2010651102

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2025

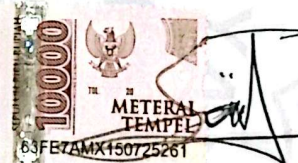
SURAT PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Yuwan Safri Nacikit
Nomor Induk Mahasiswa : 2010651102
Program Studi : S-1 Teknik Informatika
Perguruan Tinggi : Universitas Muhammadiyah Jember

Menyatakan dengan sesungguhnya karya ilmiah berupa tugas akhir yang berjudul **“ANALISIS KEAMANAN APLIKASI BERBASIS WEB MENGGUNAKAN METODE *PENETRATION TESTING* Studi Kasus: *E-commerce Assakinahmart*”** adalah benar merupakan karya sendiri. Hal-hal yang bukan karya saya, dalam penelitian tersebut diberi tanda sitasi dan ditunjukkan dalam daftar pustaka. Apabila di kemudian hari terbukti pernyataan saya tidak benar dan ditemukan pelanggaran atas karya Tugas Akhir ini, saya bersedia menerima sanksi akademik berupa pencabutan Tugas Akhir dan gelar yang saya peroleh dari Tugas Akhir tersebut.

Jember, 17 Januari 2025



Muhammad Yuwan Safri Nacikit
NIM. 2010651102

LEMBAR PERSETUJUAN TUGAS AKHIR
ANALISIS KEAMANAN APLIKASI BERBASIS WEB
MENGGUNAKAN METODE *PENETRATION TESTING*
Studi kasus: *E-commerce Assakinahmart*

Oleh:
MUHAMMAD YUWAN SAFRI NACIKIT


2010651102

Telah disetujui bahwa Laporan Tugas Akhir ini diajukan pada sidang
Tugas Akhir sebagai salah satu syarat kelulusan dan mendapatkan gelar
Sarjana Komputer (S.Kom)

Di
Universitas Muhammadiyah Jember

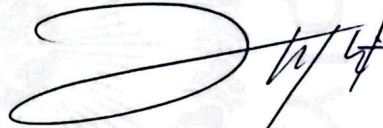
Disetujui oleh,

Pembimbing I



Miftahur Rahman S.Kom., M.Kom
NIDN. 0724039201

Pembimbing II



Ari Eko Wardoyo S.T., M.Kom
NIDN. 0014027501

LEMBAR HALAMAN PENGESAHAN

**ANALISIS KEAMANAN APLIKASI BERBASIS WEB
MENGUNAKAN METODE *PENETRATION TESTING*
Studi Kasus: *E-commerce Assakinahmart***

Oleh:

MUHAMMAD YUWAN SAFRI NACIKIT
2010651102

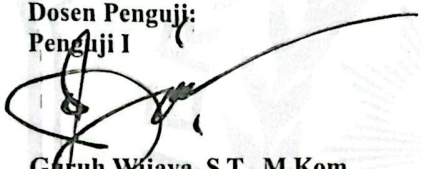
Telah mempertanggungjawabkan Laporan Tugas Akhirnya pada sidang Tugas Akhir 17 Januari 2025 sebagai salah satu syarat kelulusan dan mendapatkan gelar Sarjana Komputer (S.Kom)

Di

Universitas Muhammadiyah Jember

Disetujui oleh,

Dosen Penguji:
Penguji I


Guruh Wijaya, S.T., M.Kom
NIDN. 0729017601

Dosen Penguji:
Penguji II

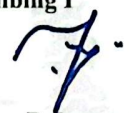

Habibatul Azizah Al Faruq, M.Pd
NIDN. 0718128901

Mengesahkan,
Dekan Fakultas Teknik

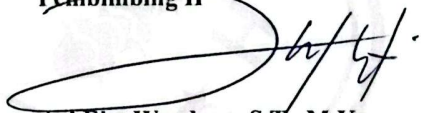


Dr. I. Muhtar, S.T., M.T., IPM.
NIDN. 0610067301

Dosen Pembimbing:
Pembimbing I


Miftahur Rahman, S.Kom., M.Kom
NIDN. 0724039201

Dosen Pembimbing:
Pembimbing II


Ari Eko Wardoyo, S.T., M.Kom.
NIDN. 0014027501

Mengetahui,
Ketua Program Studi
Teknik Informatika



Rosita Yanuarti, S.Kom., M.Cs
NIDN. 0629018601

MOTTO

“no system is save”

“aim for the impossible”

“have fun in cyberspace and meatspace”

(MRX)

“Semua orang berhak belajar IT, Tapi tidak semua orang mampu bertahan”



PERSEMBAHAN

Puji syukur kepada Allah S.W.T atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir ini. Atas segala upaya, bimbingan, dan arahan dari semua pihak, penulis mengucapkan terimakasih sebesar-besarnya kepada:

1. Allah SWT berkat segala ridho, rahmat dan hidayah-Nya penulis dapat menyelesaikan segala urusan dalam menyusun laporan Tugas Akhir dan diberikan kesempatan mendapatkan gelar Sarjana Komputer.
2. Bapak Dr. Ir. Muhtar, S.T., M.T., IPM selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember.
3. Ibu Rosita Yanuarti, S.Kom., M.Cs selaku Kepala Program Studi Teknik Informatika di Universitas Muhammadiyah Jember.
4. Bapak Miftahur Rahman S.Kom., M.Kom selaku dosen pembimbing 1, dan Bapak Ari Eko Wardoyo S.T., M.kom selaku dosen pembimbing 2 tugas akhir yang telah memberikan bimbingan, dan arahan dengan penuh kesabaran dari awal hingga akhir sehingga tugas akhir ini dapat terselesaikan.
5. Bapak Guruh Wijaya, S.T., M.Kom selaku dosen penguji 1, dan Ibu Habibatul Azizah Al Faruq, M.Pd selaku dosen penguji 2 yang telah memberikan saran dan masukan yang membangun dalam penelitian ini.
6. Bapak dan Ibu Dosen Program Studi Teknik Informatika Universitas Muhammadiyah Jember, atas ilmu dan pengetahuan yang telah diberikan.
7. Kedua orang tua saya yang selalu memberikan dukungan dan doa hingga tugas akhir ini selesai.
8. Sahabat saya Owner SIBERMUDA.IDN Rama Ahmad Ramdani dan Rekan-rekan seperjuangan yang telah membantu dalam pelaksanaan tugas akhir ini.
9. Temanku Dina Adelia Rahmawati yang selalu saya repotkan dalam tugas akhir ini.

ABSTRAK

Nacikit, Muhammad Yuwan Safri. 2025. Analisis Keamanan Aplikasi Berbasis Web Menggunakan Metode *Penetration Testing* Studi Kasus *Ecommerce* Assakinahmart. Tugas Akhir. Program Sarjana. Program Studi Teknik Informatika. Universitas Muhammadiyah Jember.

Pembimbing: (1) Miftahur Rahman, S.Kom., M.Kom.; (2) Ari Eko Wardoyo, S.T., M.Kom.

Keamanan aplikasi berbasis *web* merupakan aspek krusial dalam memastikan integritas dan kerahasiaan data, terutama pada *platform e-commerce* yang rentan terhadap serangan *cyber*. Penelitian ini bertujuan untuk menganalisis tingkat keamanan aplikasi *web e-commerce* Assakinahmart menggunakan metode *penetration testing*. Metode ini melibatkan simulasi serangan yang mungkin dilakukan oleh pihak tidak bertanggung jawab untuk mengidentifikasi kerentanan dalam sistem. Studi ini meliputi pengujian terhadap berbagai aspek, termasuk autentikasi pengguna, manajemen sesi, enkripsi data, serta perlindungan terhadap serangan *Sql Injection* dan *Cross-Site Scripting (XSS)*. Hasil penelitian ini menunjukkan bahwa *assakinahmart.com* telah memenuhi standar keamanan yang tinggi dan aman dari ancaman yang termasuk dalam *OWASP TOP 10-2021*. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan kesadaran dan tindakan preventif terhadap potensi ancaman keamanan pada aplikasi *web*.

Kata Kunci: Keamanan *web*, *Penetration testing*, *E-commerce*, Kerentanan aplikasi, Assakinahmart.

ABSTRACT

Nacikit, Muhammad Yuwan Safri. 2025. *Web Based Application Security Analysis Using Penetration Testing Method Assakinahmart E-commerce Case Study. Thesis. Degree program. Informatics Engineering Study Program. Muhammadiyah University of Jember.*

Advisors: (1) Miftahur Rahman, S.Kom., M.Kom.; (2) Ari Eko Wardoyo, S.T., M.Kom.

Web application security is a crucial aspect in ensuring the integrity and confidentiality of data, especially on e-commerce platforms that are vulnerable to cyber attacks. This research aims to analyze the security level of the E-Commerce Assakinah Mart web application using the penetration testing method. This method involves simulating attacks that may be carried out by unauthorized parties to identify vulnerabilities in the system. The study includes testing various aspects, such as user authentication, session management, data encryption, as well as protection against Sql Injection and Cross-Site Scripting (XSS) attacks. The results of this study indicate that aisyyiah.rebrainstudio.com has met high security standards and is secure from threats included in the OWASP Top 10-2021. Therefore, this research is expected to contribute to increasing awareness and preventive measures against potential security threats in web applications.

Keywords: *Web Security, Penetration Testing, E-commerce, Application Vulnerabilities, Assakinahmart.*

DAFTAR ISI

SURAT PERNYATAAN	ii
LEMBAR PERSETUJUAN TUGAS AKHIR	iii
LEMBAR HALAMAN PENGESAHAN	iv
MOTTO	v
PERSEMBAHAN	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan masalah	2
1.3. Tujuan Penelitian	3
1.4. Batasan Penelitian	3
1.5. Manfaat Penelitian	3
BAB II TINJAUAN PUSTAKA	4
2.1. Aplikasi Web	4
2.2. Assakinah	5
2.3. <i>E-Commerce</i>	6
2.4. Keamanan Aplikasi Web	7
2.5. <i>Penetration Testing</i>	9
2.6. Jenis-Jenis <i>Penetration Testing</i>	10
2.7. Tahapan-Tahapan <i>Penetration Testing</i>	12
2.8. Penelitian Terdahulu	13
2.9. <i>Nmap</i>	13
2.10. <i>Dirsearch</i>	14
2.11. <i>Burp Suite</i>	14
2.12. <i>Sqlmap</i>	14
2.13. <i>PentestTools</i>	15
2.14. <i>OWASP</i>	15
2.15. <i>CVE dan CWE</i>	16
BAB III METODOLOGI PENELITIAN	17
3.1. Tahapan Penelitian	17
3.2. Identifikasi Masalah	18
3.3. Studi Literatur	18
3.3.1 <i>Website</i>	18
3.3.2 <i>Penetration Testing (Pentesting)</i>	18
3.3.3 <i>Vulnerability</i>	19
3.4. Pengumpulan Data (<i>Information Gathering</i>)	19
3.5. Analisa Celah Keamanan	20
3.6. <i>Exploitation</i>	21
3.7. <i>Reporting</i>	22
BAB IV HASIL DAN PEMBAHASAN	23
4.1. Hasil Analisis Keamanan berdasarkan <i>OWASP TOP 2021</i>	23
4.1.1 Pengumpulan Data (<i>Information Gathering</i>)	25

4.1.2	Analisa Teknologi	27
4.1.3	Analisa Celah Keamanan (<i>Scanning</i>)	28
4.1.3.1	<i>Scanning Directory</i>	28
4.1.3.2	<i>Broken Access Control</i>	30
4.1.3.3	<i>Vulnerable and Outdated Components</i>	31
4.1.3.4	Security Misconfiguration	32
4.1.4	<i>Exploitation</i>	33
4.1.4.1	<i>Injection</i>	33
4.1.4.2	<i>Identification and Authentication Failures</i>	34
4.1.4.3	<i>Business Logic Vulnerability</i>	38
4.1.5	<i>Reporting</i>	42
BAB V KESIMPULAN DAN SARAN		47
5.1.	Kesimpulan	47
5.2.	Saran	48
DAFTAR PUSTAKA		49



DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	13
Tabel 2. 2 Perbedaan <i>CVE</i> dan <i>CWE</i>	16
Tabel 3. 1 <i>Information Gathering</i>	19
Tabel 3. 2 Pengujian Jaringan	20
Tabel 3. 3 <i>Reporting</i>	22
Tabel 4. 1 Tabel Keamanan berdasarkan <i>Owasp</i> top 10.....	24
Tabel 4. 2 <i>Report Business Logic Vulnerability</i>	44
Tabel 4. 3 Temuan Kerentanan	45



DAFTAR GAMBAR

Gambar 2. 1 <i>OWASP TOP 10 2021</i>	15
Gambar 3. 1 <i>Flowchart Penelitian</i>	17
Gambar 3. 2 <i>Nmap Scanning</i>	20
Gambar 3. 3 <i>File Robots.txt</i>	21
Gambar 3. 4 <i>Scanning Xspear</i>	22
Gambar 4. 1 <i>Ping Domain</i>	25
Gambar 4. 2 <i>Scanning Domain</i>	26
Gambar 4. 3 <i>Scanning Ip dengan Nmap</i>	26
Gambar 4. 4 <i>Wappalyzer</i>	28
Gambar 4. 5 <i>Scanning Directory</i>	29
Gambar 4. 6 <i>Halaman Dashboard</i>	30
Gambar 4. 7 <i>Scanning Ip Server</i>	31
Gambar 4. 8 <i>Scanning dengan Tool Shcheck</i>	32
Gambar 4. 9 <i>Sqlmap Parameter</i>	34
Gambar 4. 10 <i>Tool Burp Suite</i>	35
Gambar 4. 11 <i>Login Assakinahmart</i>	35
Gambar 4. 12 <i>Login 1</i>	36
Gambar 4. 13 <i>Login 2</i>	36
Gambar 4. 14 <i>Login 3</i>	37
Gambar 4. 15 <i>Exploit Username dan Password</i>	37
Gambar 4. 16 <i>Temuan User dan Password</i>	38
Gambar 4. 17 <i>Response Success to Login</i>	38
Gambar 4. 18 <i>Halaman Utama</i>	39
Gambar 4. 19 <i>Checkout Barang</i>	39
Gambar 4. 20 <i>Cart produk</i>	40
Gambar 4. 21 <i>Post /api/order</i>	40
Gambar 4. 22 <i>Halaman Repeater</i>	41
Gambar 4. 23 <i>Total Bayar</i>	41
Gambar 4. 24 <i>Perhitungan kerentanan menggunakan CVSS</i>	42