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

Dengan Hak Bebas Royalti Nonekslusif 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 Muhammadiya 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 kehadirat 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

DAFTAR TABEL

DAFTAR GAMBAR

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*