DETEKSI KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP
(STUDI KASUS : WEBSITE SATU DATA KABUPATEN MALANG)

LAPORAN TUGAS AKHIR

Diajukan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Riris Fitri Ramadhani

(201910370311245)

Bidang Minat

(Sistem Keamanan Jaringan)

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2023

LEMBAR PERSETUJUAN

Deteksi Kerentanan Keamanan Website Menggunakan Metode OWASP (Studi Kasus : Website Satu Data Kabupaten Malang)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Informatika Universitas Muhammadiyah Malang

Menyetujui,

Malang, *30 Oktober 2023*

Dosen Pembimbing 1	Dosen Pembimbing 2
Ir Denar Regata Akbi S.Kom., M.Kom.	**Zamah Sari ST., MT.**
NIP. 10816120591PNS.	**NIP. 10814100555PNS.**

LEMBAR PENGESAHAN

Deteksi Kerentanan Keamanan Website Menggunakan Metode OWASP (Studi Kasus : Website Satu Data Kabupaten Malang)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

RIRIS FITRI RAMADHANI

201910370311245

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 30 Oktober 2023

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Didih Rizki Chandranegara S.kom., M.Kom	**Wildan Suharso S.Kom., M.Kom**
NIP. 180302101992PNS.	**NIP. 10817030596PNS.**

Mengetahui,

Ketua Jurusan Informatika

Ir. Galih Wasis Wicaksono S.kom. M.Cs.

NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : RIRIS FITRI RAMADHANI

NIM : 201910370311245

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Deteksi Kerentanan Keamanan Website Menggunakan Metode OWASP (Studi Kasus : Website Satu Data Kabupaten Malang)"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkansumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka sayasiap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Malang, 30 Oktober 2023
Yang Membuat Pernyataan

Ir Denar Regata Akbi S.Kom., M.Kom.

RIRIS FITRI RAMADHANI

ABSTRAK

Semakin cepat teknologi berkembang, semakin cepat pula perkembangan teknologi digital, khususnya kejahatan yang dapat terjadi pada suatu website. Kejahatan pada website merupakan peretasan untuk mendapatkan data dan informasi yang tidak disadari oleh target. Pengujian keamanan website perlu dilakukan agar kerentanan dapat terdeteksi dan memahami risiko yang ada. Untuk memeriksa kerentanan keamanan website dapat menggunakan metode OWASP (*Open Web Application Security Project*), dengan adanya OWASP sebagai standar keamanan untuk meningkatkan keamanan website dan juga dapat membantu pengelola atau pengembang sistem dalam mencegah dan memperbaiki kerentanan yang ditemukan. Kerentanan pada website juga diperlukan sebuah sistem penilaian untuk mengevaluasi sistem keamanan yaitu CVSS (*Common Vulnerable Scoring System*). Hal ini dapat memberikan hasil untuk perbaikan selanjutnya dan dapat diimplementasikan oleh pengembang sistem. Penelitian ini mencoba mendeteksi kerentanan keamanan website Satu Data Kabupaten Malang menggunakan metode OWASP untuk memperoleh informasi dari hasil pengujian kerentanan dan juga dapat menilai kerentanan keamanan pada website Satu Data Kabupaten Malang untuk mencegah terjadinya serangan.

Kata Kunci : *OWASP, Website Security, Vulnerability, Penetration Testing, CVSS*

ABSTRACT

The faster technology develops, the faster the development of digital technology, especially crimes that can occur on a website. Crime on the website is hacking to get data and information that the target is not aware of. Website security testing needs to be done so that vulnerabilities can be detected and understand the risks that exist. To check for website security vulnerabilities, you can use the OWASP (Open Web Application Security Project) method, with the presence of OWASP as a security standard to improve website security and can also help system managers or developers in preventing and fixing vulnerabilities found. Vulnerabilities on the website also require a rating system to evaluate the security system, namely CVSS (Common Vulnerable Scoring System). This can provide results for subsequent improvements and can be implemented by system developers. This study tries to detect security vulnerabilities of the One Data Malang Regency website using the OWASP method to obtain information from the results of vulnerability testing and can also assess security vulnerabilities on the One Data Malang Regency website to prevent attacks.

Keywords **:** *OWASP, Website Security, Vulnerability, Penetration Testing, CVSS*

LEMBAR PERSEMBAHAN

Alhamdulillah, dengan mengucapkan puji dan syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga peneliti dapat menyelesaikan skripsi ini. Terwujudnya skripsi ini tidak lepas dari bantuan berbagai pihak berupa bimbingan, petunjuk dan dukungan serta bantuan dalam penyelesaian skripsi ini. Pada kesempatan ini peneliti ingin menyampaikan ucapan terima kasih sebesar-besarnya kepada :

1. Orang tua tercinta, Ayah dan Ibu peneliti yang selalu memberikan kasih sayang, dukungan, doa, dan motivasi dalam menyelesaikan pendidikan sarjana serta atas kesabarannya yang luar biasa dalam setiap langkah hidup peneliti, yang merupakan anugerah terindah dalam hidup. Peneliti berharap dapat menjadi anak yang dapat dibanggakan.
2. Kedua kakak peneliti, Bima dan Alfi serta keponakan tersayang Fayyola. Berkat bantuan, petunjuk, dan semangat dari mereka peneliti dapat menyelesaikan skripsi ini.
3. Kedua dosen pembimbing peneliti, bapak Ir Denar Regata Akbi, S.Kom, M.Kom dan bapak Zamah Sari, S.T, M.T., yang telah menyediakan waktu dan tenaga untuk memberikan bimbingan, pengarahan serta nasehat yang berharga kepada peneliti dalam penyusunan skripsi ini.
4. Ibu Evi Dwi Wahyuni, S.Kom, M.Kom., selaku dosen wali peneliti yang telah membimbing dan mengajarkan ilmu-ilmu selama perkuliahan.
5. Seluruh dosen dan staff program studi Informatika fakultas Teknik Universitas Muhammadiyah Malang yang telah memberikan ilmu-ilmu yang berharga dan bantuan dalam pengumpulan data dalam perkuliahan maupun penyusunan skripsi ini.
6. Bapak Suryadi selaku Kepala Bidang website Satu Data Kabupaten Malang yang telah membantu dan menyediakan waktu kepada peneliti.

7. Sahabat-sahabat terbaik peneliti, Anisa dan Puput yang telah menaungi keresahan peneliti dalam suka maupun duka dan menjadi tempat sambat yang paling sering peneliti kunjungi.
8. Seluruh teman terbaik kelas E Informatika angkatan 2019 yang telah membantu dan saling bahu-membahu serta dukungan selama perkuliahan. Terutama untuk "Power Rangers" yang selalu memberikan semangat dan saran yang luar biasa dalam penyusunan skripsi ini.

Malang, 08 November 2023

Riris Fitri Ramadhani

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT. Atas limpahan rahmat dan hidayah-Nya, sehingga peneliti dapat menyelesaikan tugas akhir sebagai salah satu untuk memenuhi syarat dalam penyusunan skripsi di Jurusan Informatika Fakultas Teknik Universitas Muhammadiyah Malang. Dalam kesempatan ini, peneliti membuat skripsi yang berjudul: "**DETEKSI KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (STUDI KASUS: WEBSITE SATU DATA KABUPATEN MALANG)".**

Skripsi ini bertujuan untuk melengkapi tugas akhir yang merupakan salah satu syarat guna memperoleh gelar sarjana starta 1. Dengan segala keterbatasan pengetahuan dan pengalaman yang dimiliki, peneliti menyadari bahwa penyusunan skripsi ini masih jauh dari sempurna. Oleh karena itu, peneliti mengucapkan terima kasih atas segala bantuan, doa, dan dukungan dari berbagai pihak semoga segala kebaikan dan pertolongan semuanya mendapat berkah dari Allah SWT.

Akhir kata, peneliti mempunyai harapan besar pada skripsi ini dan mengharapkan saran yang membangun agar dapat memberikan manfaat kepada semua pembacanya.

Malang, 08 November 2023

Riris Fitri Ramadhani

.

DAFTAR ISI

LEMBAR PERSETUJUAN ii
LEMBAR PENGESAHAN iii
LEMBAR PERNYATAAN iv
ABSTRAK v
ABSTRACT vi
LEMBAR PERSEMBAHAN vii
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
DAFTAR LAMPIRAN xiv
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
BAB II 4
TINJAUAN PUSTAKA 4
2.1 Penelitian Terdahulu 4
2.2 Kerentanan *Website* 5
2.3 *Website* Satu Data Kabupaten Malang 6
2.4 *OWASP* (*Open Web Application Security Project*) 7
2.5 *OWASP TOP 10* 2021 8
2.6 CVSS (*Common Vulnerability Scoring System*) 10
BAB III 14
METODE PENELITIAN 14
3.1 Alur Penelitian 14

3.2 *Reconnaissance* 15
3.3 *Scanning* 15
3.4 *Exploitation* 15
3.5 *Reporting* 16
3.6 CVSS (*Common Vulnerability Scoring System*) 16
BAB IV 18
HASIL DAN PEMBAHASAN 18
4.1 *Reconnaissance* 18
4.2 *Scanning* 20
4.3 *Exploitation* 21
4.4 *Reporting* 26
4.4.1 Alert Detail 30
4.5 Perhitungan CVSS (*Common Vulnerability Scoring System*) 33
4.5.1 Perhitungan Clickjacking Attack 33
4.5.2 Perhitungan XSS Attack 35
4.5.3 Perhitungan CRSF Attack 37
BAB V 40
KESIMPULAN 40
5.1 Kesimpulan 40
5.2 Saran 40
DAFTAR PUSTAKA 42
LAMPIRAN 44

DAFTAR GAMBAR

Gambar 1. CVSS Metric 10
Gambar 2. CVSS Score 12
Gambar 3. Base Score Formula 13
Gambar 4. Alur Penelitian 14
Gambar 5. Hasil pengujian menggunakan nikto 19
Gambar 6. Halaman login disusupi 22
Gambar 7. Data yang dicuri 22
Gambar 8. Payloads 23
Gambar 9. Hasil injeksi Payloads 23
Gambar 10. Hasil pengujian SQL Injection 24
Gambar 11. Halaman Ubah Password yang disusupi 25
Gambar 12. Mengubah password pada akun pengguna 25
Gambar 13. Login dengan password yang diubah 26
Gambar 14. Penyerang berhasil login 26
Gambar 15. Base Score Clickjacking Attack 35
Gambar 16. Base Score XSS Attack 37
Gambar 17. Base Score CRSF Attack 39

DAFTAR TABEL

Tabel 1. Penelitian Terdahulu 4
Tabel 2. Tools tahap Reconaissannce 7
Tabel 3. Tools tahap Scanning 7
Tabel 4. Exploitability Metrics 11
Tabel 5. Impact Metrics 12
Tabel 6. Hasil Kerentanan OWASP Top 10 16
Tabel 7. Hasil CVSS Score 17
Tabel 8. Scanning Port menggunakan nmap 18
Tabel 9. DNS Enumeration menggunakan netcraft 19
Tabel 10. Scanning website menggunakan acunetix 20
Tabel 11. Scanning website menggunakan dirsearch 21
Tabel 12. Hasil kerentanan OWASP Top 10 27
Tabel 13. Alerts Detail 30
Tabel 14. Hasil perhitungan Clickjacking Attack 33
Tabel 15. Hasil perhitungan XSS Attack 35
Tabel 16. Hasil perhitungan CRSF Attack 37

DAFTAR LAMPIRAN

Lampiran 1. Surat Permohonan Data Tugas Akhir 44

DAFTAR PUSTAKA

[1] I. P. A. Eka Pratama and A. A. B. A. Wiradarma, "Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company)," *International Journal of Computer Network and Information Security*, vol. 11, no. 7, pp. 8–12, Jul. 2019, doi: 10.5815/ijcnis.2019.07.02.

[2] K. Nisa, M. A. Putra, R. A. Siregar, and M. D. Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," vol. 3, no. 4, pp. 308–316, 2022.

[3] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *Jurnal Informasi dan Teknologi*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[4] Y. Thurfah Afifa Rosaliah and B. Hananto, *Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx*. 2021.

[5] R. Ashar, "Jurnal Informasi dan Teknologi Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," vol. 4, pp. 187–194, 2022, doi: 10.37034/jsisfotek.v4i4.233.

[6] B. Harahap, "Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta," *Jurnal Informatika dan Teknologi Pendidikan*, vol. 1, no. 2, pp. 80–86, Dec. 2021, doi: 10.25008/jitp.v1i2.15.

[7] A. Rochman, R. R. Salam, and S. A. Maulana, "ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DANOPEN WEB APPLICATION SECURITY PROJECT (OWASP)DI RUMAH SAKIT XYZ," vol. 2, no. 4, p. 6, 2021, doi: https://doi.org/10.36418/jist.v2i4.124.

[8] J. Pendidikan and D. Konseling, "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment."

[9] Dewi Aryanti, Nurholis, and J. N. Utamajaya, "ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA," vol. 26, no. 2, pp. 173–180, 2021, doi: https://doi.org/10.54543/fusion.v1i03.53.

[10] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal of Computer Engineering, System and Science)*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[11] S. Hidayatulloh and D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP).” [Online]. Available: http://jurnal.itg.ac.id/

[12] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, “Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP,” *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 21, no. 2, p. 80, 2022, doi: 10.53513/jis.v21i2.6119.

[13] G. Guntoro, L. Costaner, and M. Musfawati, “Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning),” *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[14] D. Priyawati, S. Rokhmah, and I. C. Utomo, “Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP,” 2022. [Online]. Available: https://ijcis.net/index.php/ijcis/index

[15] I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, and I. Km. W. Yuda Arimika, “Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project),” *Simkom*, vol. 7, no. 1, pp. 23–27, 2022, doi: 10.51717/simkom.v7i1.63.

[16] R. R. Daniswara, G. Made, A. Sasmita, P. Agus, and E. Pratama, “Testing for Information Gathering Using OWASP Testing Guide v4 (Case Study : Udayana University SIMAK-NG Application),” 2020.

[17] L. Allodi, S. Banescu, H. Femmer, and K. Beckers, “Identifying relevant information cues for vulnerability assessment using CVSS,” in *CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, Association for Computing Machinery, Inc, Mar. 2018, pp. 119–126. doi: 10.1145/3176258.3176340.

[18] M. Aziz, “Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz,” *Jecsit*, vol. 1, no. 1, pp. 101–109, 2021.

[19] D. D. Cahyani *et al.*, “ANALISIS KERENTANAN WEBSITE SMP NEGERI 3 SEMARAPURA MENGGUNAKAN METODE PENGUJIAN RATE LIMITING DAN OWASP,” *INSERT: Information System and Emerging Technology Journal*, vol. 2, no. 2, 2021.

[20] FIRST, “Common Vulnerability Scoring System version 3.1 Specification Document Revision 1,” pp. 1–24, 2019, [Online]. Available: https://www.first.org/cvss/

UNIVERSITAS
MUHAMMADIYAH
MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Riris Fitri Ramadhani**

NIM : **201910370311245**

Judul TA : **Deteksi Kerentanan Keamanan Website Menggunakan Metode OWASP (Studi Kasus : Website Satu Data Kabupaten Malang)**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	8 %
2.	Bab 2 – Daftar Pustaka	25 %	15 %
3.	Bab 3 – Analisis dan Perancangan	25 %	14 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	13 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	4 %
6.	Makalah Tugas Akhir	20%	10 %

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

UNIVERSITAS MUHAMMADIYAH MALANG
IF
FAKULTAS TEKNIK

(.....)