Jurnal Pendidikan dan Konseling
Volume 4 Nomor 4 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Penetration Testing pada *Website* Universitas Singaperbangsa Karawang *Menggunakan Open Web Application Security Project* (OWASP)

Muhammad Rafi Ramdani[1], Nono Heryana[2], Agung Susilo Yuda Irawan[3]
[1,2,3] Teknik Informatika, Ilmu Komputer, Universitas Singaperbangsa Karawang
Email: muhammad.rafi18168@student.unsika.ac.id[1], nono@unsika.ac.id[2], agung@unsika.ac.id[3]

Abstrak

Universitas Singaperbangsa adalah perguruan tinggi yang memanfaatkan *website* dalam melakukan kegiatan perkuliahannya. Banyak resiko yang akan terjadi apabila *webserver* yang digunakan oleh *website* Universitas Singaperbangsa tidak memiliki keamanan yang baik, banyak ancaman dari pihak yang tidak bertanggung jawab yang bisa memanfaatkan celah keamanan. Tujuan penelitian ini adalah melakukan identifikasi masalah kerentanan yang terdapat dalam *website* Universitas Singaperbangsa dan melakukan pengujian serta analisis untuk mengetahui kondisi kerentanan website tersebut menggunakan *Open Web Application Security Project* (OWASP). Metode penelitian yang digunakan sebagai parameter keamanan website adalah *OWASP Top*-10 2021. Pengujian dilakukan pada alamat *domain* journal.unsika.ac.id dengan melakukan proses *scanning vulnerability analysis* menggunakan *tools OWASP ZAP*, ditemukan 3 celah dengan tingkat risiko *high*, 5 celah dengan tingkat risiko *medium*, 8 celah dengan tingkat risiko *low*, dan 3 celah dengan tingkat risiko *informational*. Hasil pengujian pada *penetration testing* berhasil pada celah keamanan, *X-Frame-Options Header Not Set, Application Error Disclosure, Broken Access Control*. Berdasarkan 10 daftar kerentanan *OWASP Top*-10 2021, *website* Universitas Singaperbangsa Karawang dengan alamat *domain* journal.unsika.ac.id tidak memiliki celah keamanan yang berisiko tinggi, hanya memiliki kerentanan pada celah *broken access control* yang termasuk pada daftar *OWASP* dan celah tersebut hanya menampilkan direktori pada *website* yang tidak terlalu sensitif yang hanya menampilkan informasi berupa *plugins* yang digunakan pada *website*.
Kata kunci : *Website*, *Penetration Testing, Vulnerability Analysis, Owasp Zap*

Abstract

Singaperbangsa University is a university that utilizes the website in conducting its lecture activities. Many risks will occur if the webserver used by the Singaperbangsa University website does not have good security, there are many threats from irresponsible parties who can take advantage of security holes. The purpose of this study is to identify the vulnerability problems contained in the website of the University of Singaperbangsa and conduct testing and analysis to determine the condition of the vulnerability of the website using the Open Web Application Security Project (OWASP). The research method used as a website security parameter is OWASP Top-10 2021. The test was carried out at the journal.unsika.ac.id domain address by carrying out a scanning vulnerability analysis process using OWASP ZAP tools, found 3 gaps with a high risk level, 5 gaps with a high level of risk. medium risk, 8 loopholes with low risk level, and 3 loopholes with informational risk level. The test results on penetration testing were successful on security holes, X-Frame-Options Header Not Set, Application Error Disclosure, Broken Access Control. Based on the list of 10 OWASP Top-10 vulnerabilities 2021, the Universitas Singaperbangsa Karawang website with the domain address journal.unsika.ac.id does not have a high-risk security vulnerability, only has a vulnerability in the broken access control loophole

which is included in the OWASP list and the vulnerability only displays a directory on a website that is not too sensitive that only displays information in the form of plugins used on the website.
Keywords: *Website, Penetration Testing, Vulnerability Analysis, Owasp Zap*

PENDAHULUAN

Dalam perkembangan Teknologi Informasi (TI), telah menyebabkan perubahan dan dampak besar pada manusia dalam kehidupan sehari - hari. Perkembangan TI yang semakin cepat dan terus mengalami perubahan telah menjadikan era teknologi yang lebih cepat dari yang pernah dibayangkan sebelumnya. Saat ini komputer tidak hanya berfungsi sebagai pengolahan data saja, tetapi telah menjadi senjata utama bagi perusahaan untuk berkompetisi sebagai yang terbaik (Stiawan, 2005).

Banyak kasus kejahatan pada dunia komputer, khususnya pada jaringan internet dalam menghadapi serangan *virus. Worm, Dos, Web Deface,* bahkan sampai dengan masalah pencurian kartu kredit. Dari laporan digital yang telah dibuat oleh *We Are Social* (HootSuite), penggunaan internet di Indonesia kini pada awal tahun 2021 telah mencapai 202,6 juta jiwa. Jumlah pengguna internet di Indonesia saat ini 274,9 juta jiwa, artinya *penetrasi* internet di Indonesia telah mencapai 73,7% pada awal tahun 2021 (Ramadhan, 2020).

Universitas Singaperbangsa Karawang merupakan perguruan tinggi yang sudah memanfaatkan teknologi *website* dalam melakukan proses seperti pengolahan data dan informasi. Seluruh informasi yang berkaitan dengan kampus telah dimuat pada *website*. Banyak resiko yang akan terjadi jika *website* yang telah digunakan oleh Universitas Singaperbangsa tidak memiliki standar keamanan yang baik, banyak ancaman dari pihak luar yang tidak bertanggung jawab yang bisa memanfaatkan celah keamanan dan merugikan Universitas Singaperbangsa Karawang.

Keamanan perangkat lunak memainkan peran penting dalam banyak aspek keamanan siber. Untuk melindungi *web server* dari serangan pihak yang tidak bertanggung jawab, sebaiknya pengujian *web server* harus dilakukan dengan melakukan selftest pada sistem *web server* itu sendiri menggunakan metode *penetration testing*.

Menurut Mulyadi, pengujian penetrasi adalah prosedur dan teknik untuk menilai keamanan suatu sistem komputer atau jaringan dengan menjalankan simulasi serangan untuk mengetahui dimana sistem rentan dan menutup atau memperbaiki celah tersebut. Pengujian *penetrasi* dilakukan sebagai tindakan pencegahan untuk mencegah peretasan pada sistem (Mulyadi, 2018).

Penelitian sebelumnya dilakukan oleh (Yudiana et al., 2021) mengenai Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis *Website* Pada STMIK ROSMA Dengan Menggunakan *OWASP TOP* 10. Pengujian yang dilakukan pada penelitian ini menunjukan bahwa sistem informasi e-office memiliki 13 kerentanan berdasarkan *OWASP Top* 10 2017, sistem informasi e-office memiliki 4 kerentanan yaitu *Sensitive Data Exposure, Security Misconfiguration, Cross Site Scripting, dan Insecure Deseralization.*

Penelitian sebelumnya dilakukan oleh (Sahren et al., 2019) mengenai *Penetration Testing* Untuk Deteksi *Vulnerability* Sistem Informasi Kampus. Pada pengujian ini telah ditemukan beberapa celah keamanan pada sistem informasi kampus yang bisa saja nantinya digunakan untuk memanipulasi file lokal, mengganggu kinerja dari *server* itu sendiri dengan teknik *DoS*, melakukan *clickjacking* serta *CSRF/Cross-site request forgery*.

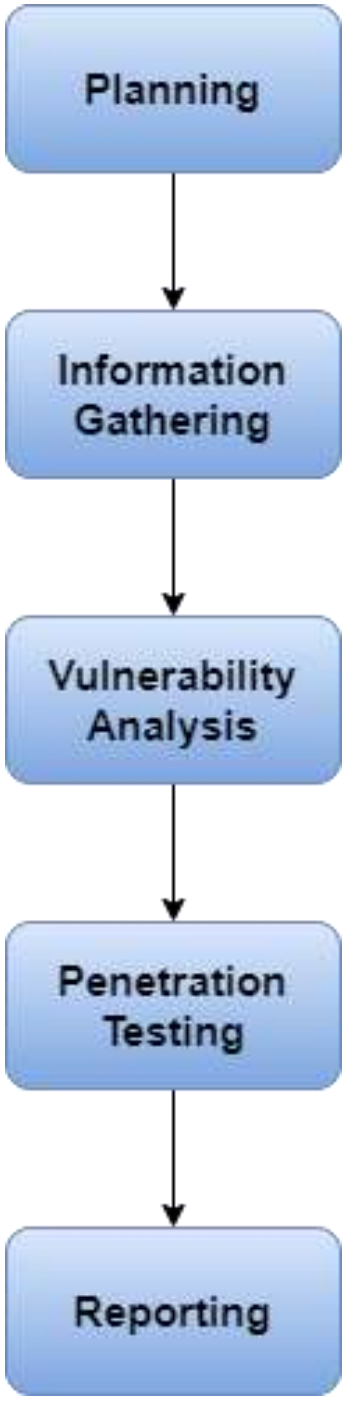
Pengujian penetrasi pada website dapat dilakukan dengan berbagai cara. Salah satunya adalah dengan menggunakan parameter keamanan yang dibuat oleh OWASP. OWASP adalah komunitas terbuka yang memungkinkan organisasi atau administrator sistem untuk mengembangkan dan memelihara aplikasi terpercaya (Cerullo, 2009).

Penelitian ini bertujuan untuk menganalisis dan melakukan pengujian keamanan website Universitas Singaperbangsa Karawang menggunakan metode Penetration Testing dengan parameter keamanan dari *OWASP TOP* 10. Versi OWASP menggunakan *OWASP* 2021, dan pemindaian kerentanan website yang digunakan adalah *OWASP ZAP, Nmap, Nikto* dan *Whatweb*. Hasil dari penelitian diharapkan menjadi informasi

sekaligus evaluasi bagi Perguruan Tinggi Universitas Singaperbangsa Karawang dalam menjaga dan mengembangkan website Universitas Singaperbangsa Karawang.

METODE

Metode Penetration Testing akan digunakan untuk melakukan pengujian pada website Universitas Singaperbangsa Karawang dengan menggunakan tahapan dari metode *Penetration Testing*.



Adapun rancangan dari alur penelitian akan dijelaskan sebagai berikut :

1. *Planning*
   Pada tahap Planning, akan dirancangan ruang lingkup dari penelitian Penetration Testing. Menentukan ruang lingkup dan tujuan pengujian, termasuk sistem yang akan diuji dan metode pengujian yang akan digunakan.
2. *Information Gathering*
   Pada tahap ini dikumpulkan semua informasi tentang website Universitas Singaperbangsa Karawang. Kemudian dilakukan scanning untuk 23 mengumpulkan informasi mengenai domain, server, ip address, host, dan firewall.
3. *Vulnerability Analysis*
   Pada tahap ini mencari celah keamanan yang bisa dilakukan dengan cara manual atau dengan otomatis tergantung tools yang akan digunakan.
4. *Penetration Testing*
   Setelah menemukan kerentanan. Langkah selanjutnya adalah mengeksploitasinya, dengan kata lain, lakukan eksperimen serangan. Penentuan target dan pemilihan tools yang tepat. Pada tahap ini biasanya menggunakan serangan web application, seperti cross-site scripting, SQL Injection untuk menemukan kerentanan pada target.
5. *Reporting*
   Pada tahap akhir akan dibuat laporan. Laporan tersebut mencakup langkahlangkah yang diambil, kerentanan keamanan yang terdeteksi dengan menggunakan parameter keamanan OWASP Top 10-2021.

HASIL DAN PEMBAHASAN

Proses yang dilakukan untuk menemukan celah keamanan pada website meliputi planning, information gathering, vulnerability analysis, penetration testing dan reporting. Pada proses vulnerability analysis menggunakan tools OWASP ZAP (Zed Attack Proxy) dalam menemukan celah keamanan pada website journal.unsika.ac.id. Sehingga pada proses penetration testing dilakukan dengan berdasarkan kerentanan yang ditemukan pada tahap vulnerability analysis. Hasil dari penelitian ini yaitu reporting atau hasil yang ditemukan pada saat pengujian penetration testing berdasarkan kerentanan yang dimiliki OWASP TOP 10-2021.

Planning

Dalam melakukan penetration testing, planning merupakan tahapan awal untuk melakukan pengujian. Penentuan objek dan ruang lingkup yang akan diuji dalam melakukan proses penetration testing merupakan bagian dari tahapan planning. Objek yang akan di uji adalah website Universitas Singaperbangsa Karawang dengan nama domain journal.unsika.ac.id.

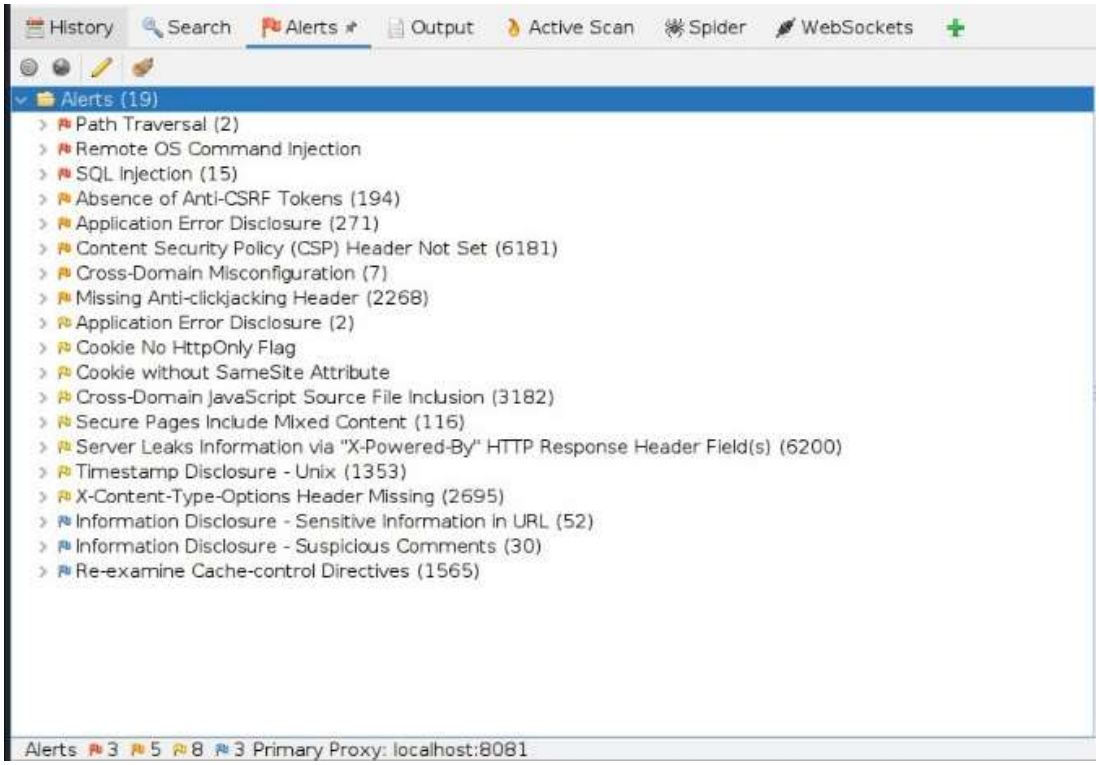
Gambar 1. *website* journal.unsika.ac.id

Informatin Gathering

Setelah melakukan planning atau menentukan scope pengujian, langkah selanjutnya adalah melakukan information Gathering, maksudnya adalah dengan mengumpulkan informasi sebanyak mungkin dari website yang akan di uji, untuk mengumpulkan informasi pada website, dapat menggunakan beberapa tools untuk membantu jalannya pengujian.

Vulnerability Analysis

Tahap ke tiga melakukan proses vulnerability analysis pada domain journal.unsika.ac.id. Pada proses ini bertujuan untuk menemukan kelemahan yang ada dalam sistem menggunakan *tools OWASP ZAP*.



Gambar 2. **Hasil Pengujian OWASP ZAP**

Penetration Testing

Hasil dari vulnerability analysis menampilkan informasi celah keamanan pada website journal.unsika.ac.id. Berdasarkan hasil kerentanan yang ditemukan maka akan dilakukan pengujian pada beberapa celah yang lebih spesifik yaitu :

1. Cross-site Request Forgery (CSRF)
2. Cross-site Scripting (XSS)
3. X-Frame-Options Header Not Set
4. SQL Injection
5. Path Traversal
6. Remote OS Command Injection
7. Broken Access Control
8. Application Error Disclosure

Pada tahap ini akan dilakukan pengujian celah kerentanan yang telah ditemukan pada tahapan-tahapan selebelumnya terhadap aplikasi berbasis *website* yaitu journal.unsika.ac.id. Pada tahap ini melakukan uji validasi kerentanan yang ditemukan oleh vulnerability scanner pada tahap vulnerability analysis.

Reporti

No	Jenis Ancaman	Hasil Pengujian	Rekomendasi
1	*Cross-site Request Forgery* (CSRF)	Tidak berhasil	-
2	*Cross-site Scripting* (XSS)	Tidak berhasil	-
3	*X-Frame-Options Header Not Set*	Berhasil, menggunakan *iframe* pada halaman *web* lain.	Menggunakan Content-Security-Policy: frame-ancestors 'none'; yang dapat mencegah domain apapun membuat *framing*.
4	*Sql Injection*	Tidak berhasil	-
5	*Broken Access Control*	Berhasil, hanya ditemukan informasi yang tidak terlalu sensitif	-
6	*Application Error Disclosure*	Berhasil, ditemukan *error* pada *url* https://journal.unsika.ac.id/api/v1/users/	Verifikasi bahwa halaman ini menampilkan pesan kesalahan atau peringatan dan konfigurasi. Gunakan pesan kesalahan kepada pengguna.
7	*Path Tranversal*	Tidak berhasil.	-
8	*Remote OS Command Injection*	Tidak berhasil.	-

Gambar 3. Hasil Pengujian *Penetration Testing*

Hasil pengujian berhasil pada celah keamanan berikut, *X-Frame-Options Header Not Set* yaitu dengan membuat *iframe* pada halaman *web* lain, *Application Error Disclosure* pada url https://journal.unsika.ac.id/api/v1/users/ halaman ini berisi pesan kesalahan atau peringatan *error* yang mungkin mengungkapkan informasi sensitif, dan pada celah *Broken Access Control* yang Ditemukan 20 *url* yang bisa dilewati tanpa adanya proses *autorisasi*, namun hanya menampilkan informasi yang tidak terlalu sensitif, hanya informasi berupa *plugins* yang digunakan pada *website*.

Hasil pengujian berdasarkan parameter OWASP Top 10-2021

No	Nama Kerentanan	Celah Keamanan	Hasil Pengujian
1	A01:2021-*Broken Access Control*	*Path Traversal, Cross-Site Request Forgery (CSRF), Exposure of Information Through Directory Listing*	Celah keamanan yang berhasil di uji adalah *Exposure of Information Through Directory Listing*, pengujian mendapatkan hasil dari direktori yang terbuka yang menampilkan informasi yang tidak terlalu sensitif, hanya berupa *plugins* yang digunakan pada *website*.
2	A02:2021-Crytographic Failures	Tidak Ditemukan	-
3	A03:2021-Injection	*SQL Injection, Cross-site Scripting, Remote OS Command Injection*	Tidak Berhasil,
4	A04:2021-Insecure Design	Tidak Ditemukan	-
5	A05:2021-Security Misconfiguration	Tidak Ditemukan	-
6	A06:2021-Vulnerable and Outdated Components	Tidak Ditemukan	-
7	A07:2021-Identification and Authentication Failures	Tidak Ditemukan	-
8	A08:2021-Software and Data Integrity Failures	Tidak Ditemukan	-
9	A09:2021-Security Logging and Monitoring Failures	Tidak Ditemukan	-
10	A10:2021-Server-Side Request Forgery	Tidak Ditemukan	-

Gambar 4. Daftar Kerentanan *OWASP* dan Hasil Pengujian

Website journal.unsika.ac.id memiliki 8 kerentanan berdasarkan hasil dari scanning menggunakan tools *OWASP ZAP*. Dari 8 kerentanan ini dilakukan pengujian pada tahap *penetration testing* dan 3 dari 6 kerentanan tersebut berhasil ditemukan celah keamanannya.

Pada Gambar 8. merupakan pengujian dari daftar 10 kerentanan yang dimiliki *OWASP* yaitu *OWASP TOP* 10-2021 dan hasil pengujian pada tahap *penetration testing*. Berdasarkan dari hasil pengujian yang dilakukan 1 dari 8 kerentanan tersebut termasuk ke dalam daftar *OWASP TOP* 10 yaitu pada kerentanan *broken access control*. Namun hasil yang ditemukan pada celah broken access control merupakan informasi tampilan yang tidak terlalu sensitive, hanya berupa *plugins* yang digunakan pada *website*.

SIMPULAN

1. Pengujian dilakukan pada domain journal.unsika.ac.id dengan melakukan proses scanning vulnerability analysis untuk menemukan kerentanan pada website menggunakan tools OWASP-ZAP. Ditemukan 3 kerentanan dengan tingkat risiko high, 5 kerentanan dengan tingkat risiko medium, 8 kerentanan dengan tingkat risiko low, dan 3 kerentanan dengan tingkat risiko informational.
2. Berdasarkan hasil dari proses vulnerability analysis, dilakukan proses pengujian celah keamanan antara lain, *Cross-site Request Forgery (CSRF), Cross-site Scripting (XSS), X-Frame-Options Header Not Set, Sql Injection, Path Tranversal, Remote OS Command Injection, Broken Access Control, Application Error Disclosure*. Hasil pengujian berhasil pada celah keamanan berikut, X-Frame-Options Header Not Set yaitu dengan membuat iframe pada halaman web lain, Application Error Disclosure pada url https://journal.unsika.ac.id/api/v1/users/ halaman ini berisi pesan kesalahan atau peringatan error yang mungkin mengungkapkan informasi sensitif, dan pada celah Broken Access Control yang Ditemukan 20 url yang bisa dilewati tanpa adanya proses *autorisasi*, namun hanya menampilkan informasi yang tidak terlalu sensitif, hanya informasi berupa plugins yang digunakan pada *website*.
3. Berdasarkan parameter kerentanan yang dimiliki *OWASP Top* 10-2021, *website* Universitas Singaperbangsa Karawang tidak memiliki celah keamanan yang berisiko tinggi, hanya memiliki kerentanan pada celah *Broken Access Control* yang hanya menampilkan informasi yang tidak terlalu sensitif hanya berupa plugins yang digunakan pada *website*.

DAFTAR PUSTAKA

Aliefyan, A. (2020). Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web. *ResearchGate*, *July*.

Anherr. (2016). *Information Gathering dengan WhatWeb di Kali Linux*. Anher323.Blogspot.Com.

Cerullo, F. E. (2009). OWASP TOP 10 2009. *Iberic Web Application Security Conference*, 19.

Mulyadi. (2018). *Bagaimana Melakukan "Penetration Test"?* Www.Kompasiana.Com.

Ramadhan, B. (2020). *Data Internet di Indonesia dan Perilakunya Tahun 2020*. Teknoia.Com.

Sahren, Ashari Dalimuthe, R., & Amin, M. (2019). *Prosiding Seminar Nasional Riset Information Science (SENARIS) Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus*. *September*, 994–1001.

Stiawan, D. (2005). *Sistem Keamanan Komputer*. Elex Media Komputindo.

Tarigan, B. V., Kusyanti, A., & Yahya, W. (2017). Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(3), 206–214.

Yudiana, Y., Elanda, A., & Buana, R. L. (2021). 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)*, *6*(2), 185. https://doi.org/10.24114/cess.v6i2.24777

ZAKARIA, M. (2022). *Pengertian NMAP Beserta Fungsi dan Cara Kerjanya yang Perlu Diketahui*.