**Journal of Science and Social Research** ISSN 2615 – 4307 (Print)
August 2025, VIII (3): 5360– 5367 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

# PERANCANGAN SISTEM *OPEN SOURCE* UNTUK PENETRATION TESTING PADA WEBSITE PORTAL AKADEMIK

**Alif Al Farizi[1], Yusuf Ramadhan Nasution[2], Muhamad Alda[3]**
**Universitas Islam Negeri Sumatera Utara, Medan**
email: [1]alifalfarizi72@gmail.com, [2]ramadhannst@uinsu.ac.id,
[3]muhamadalda@uinsu.ac.id

***Abstract:*** *One technique for locating security flaws in information systems is penetration testing. This research aims to design and implement an open-source system that integrates several penetration testing tools to assess the security of the PortalSIA UINSU website. The tools used include Paramspider, Dalfox, Cyberfox, Sqlmap, and Penblood. The system is designed to perform parameter scanning, exploitation, and automatic reporting of test results in a structured manner. The results show that out of five tested URLs, most did not reveal significant vulnerabilities, except for some connectivity issues during the SQL injection testing stage. This system can be utilized as a tool to efficiently detect and analyze potential vulnerabilities in target websites.*

***Keyword:*** *Penetration Testing, Open Source, Website Security*

**Abstrak:** Salah satu teknik untuk menemukan kelemahan keamanan dalam sistem informasi adalah pengujian penetrasi. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem sumber terbuka yang mengintegrasikan beberapa alat pengujian penetrasi untuk menilai keamanan situs web PortalSIA UINSU. Alat yang digunakan meliputi Paramspider, Dalfox, Cyberfox, Sqlmap, dan Penblood. Sistem ini dirancang untuk melakukan pemindaian parameter, eksploitasi, dan pelaporan otomatis hasil pengujian secara terstruktur. Hasil penelitian menunjukkan bahwa dari lima URL yang diuji, sebagian besar tidak mengungkapkan kerentanan yang signifikan, kecuali beberapa masalah konektivitas selama tahap pengujian injeksi SQL. Sistem ini dapat digunakan sebagai alat untuk mendeteksi dan menganalisis potensi kerentanan secara efisien di situs web target.

**Kata kunci:** Pengujian Penetrasi, *Open Source*, Keamanan Situs Web

## PENDAHULUAN

Keamanan ialah salah satu dari masalah utama sistem informasi. Pertumbuhan konektivitas dari sebuah komputer melalui internet, Meningkatnya ekstensibilitas sistem, dan pertumbuhan ukuran yang tidak terkendali dari ukuran dan kompleksitas sistem telah membuat keamanan perangkat lunak sebuah masalah yang lebih besar sekarang dari pada di masa lalu (Aulia et al., 2023; Mallaboyev et al., 2022). Upaya untuk memecahkan masalah keamanan dan mematuhi peraturan keamanan yang berlaku, pakar keamanan telah mengembangkan berbagai metode jaminan keamanan yang mencakup bukti kebenaran desain. Uji penetrasi adalah metode komprehensif untuk menguji dasar komputasi yang lengkap, terpadu, operasional, dan terpercaya yang terdiri dari perangkat keras, perangkat lunak dan manusia (Wijaya et al., 2024) .Proses ini melibatkan analisis aktif sistem yang buruk atau tidak tepat, kelemahan perangkat keras dan perangkat lunak dan kelemahan operasional dalam proses atau penanggulangan teknis (Rayner et al., 2024). Ada tiga metode penetrasi yaitu *Black Box, Grey Box,* dan *White Box* (Putra Utama et al., n.d.).

*Black box* ialah metode yang mana seorang pentester yang berperan

sebagai pentester yang harus mengeksploitkan sistem untuk mencari celah keamanan yang dapat diretas, dan pentester tidak di bekali informasi apapun tentang targetnya dan harus menganalisa sendiri (Ahmad, 2021). *Grey box* yang mana pentester memiliki akses dan informasi hanya sebagai sebatas pengguna dan metode ini lebih efisien dibandingkan *black box* karena sudah memiliki beberapa informasi dan pentester dapat langsung menguji keamanan targetnya (Lana Rahardian, 2022) (Linggih Jaelani & Khoirunnisa, 2023). Sedangkan *White box* memiliki akses penuh dan pentester hanya harus meneliti dan memilah milah semua data yang diterima dan mengalokasikan celah pada tiap titik yang dianggap berpotensi di hack (Kanade et al., 2024). Sering ditemukan sebuah kesalahan sistem di *website* PortalSIA UINSU seperti identitas atau foto mahasiswa yang berubah dengan sendirinya.

## METODE

### Metode Pengumpulan Data

Didalam penelitian ini penulis menggunakan beberapa metode pengumpulan data sebagai berikut (Nawassyarif et al., 2020):

1. Observasi

Observasi merupakan teknik pengumpulan data yang dilakukan dengan cara mengamati objek penelitian secara langsung. Observasi pada penelitian ini dilakukan dengan cara *login* sebagai pengguna web dan mengumpulkan sebuah informasi yang bisa digunakan untuk proses selanjutnya (Firmansyah et al., 2022) (Studi Sistem Informasi Universitas Trilogi Jakarta Jl TMP Kalibata No et al., 2021).

2. Wawancara

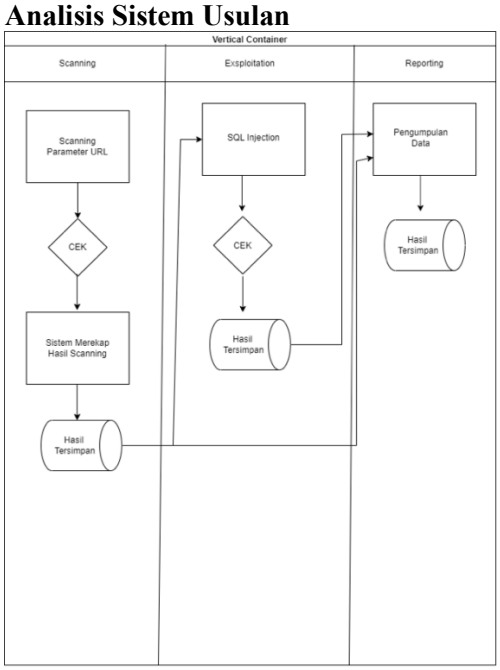
Wawancara adalah salah satu teknik pengumpulan data dengan melakukan komunikasi secara langsung terhadap narasumber yang telah dipilih dan ahli dibidang ini dan dapat membantu dalam merancang pembuatan script pentrasi testing (Setiawan et al., 2025). Peneliti yang di pilih ialah kepala Pustipada Universitas Islam Negeri Sumatera Utara (Rahardja et al., 2021).

3. Studi Pustaka

Data yang diperoleh dengan memanfaatkan berbagai sumber seperti jurnal, karya ilmiah, halaman *website* dan penelitian yang pernah dilakukan sebelumnya. Studi pustaka digunakan untuk mendapat informasi pendukung yang berkaitan dengan *Penetration Testing* dan *Bug Hunter* (Andharsaputri et al., 2021).

## HASIL DAN PEMBAHASAN

### Analisis Sistem Usulan




**Gambar 1 Analisis Sistem Usulan**

Keterangan Analisis Sistem Usulan:

***Scanning***

Pada tahap ini merupakan tahapan dalam proses *Information Gathering* atau pengumpulan Informasi terkait *website* target pengujian (Costaner & Musfawati, 2020). Tahapan ini bertujuan untuk mengumpulkan informasi dengan *website* target seperti Parameter URL yang mungkin memiliki parameter tersembunyi dan tidak tertaut yang secara khusus berguna saat mencari kerentanan

terkait *Web Cache Poisoning*. Untuk hasil pengujian akan otomatis tersimpan disebuah file terpisah dengan nama file yang sesuai tanggal pengujian. Ditahap *scanning* ini penguji menggunakan tools yg khusus seperti paramspider dan dalfox. Penguji merancang kedua tools lebih sederhana untuk digunakan (Gustiyono et al., 2024).

**Exploitasi**

Untuk tahap *Exploitation* penguji menggunakan *tools Cyberfox* yang mana penguji akan membuka secara otomatis. Untuk pengujian exploitasi disini penguji akan menguji parameter url yang sudah diuji sebelumnya, dan penguji akan menambahkan beberapa text (Burhani & Priyawati, 2024).

***Reporting***

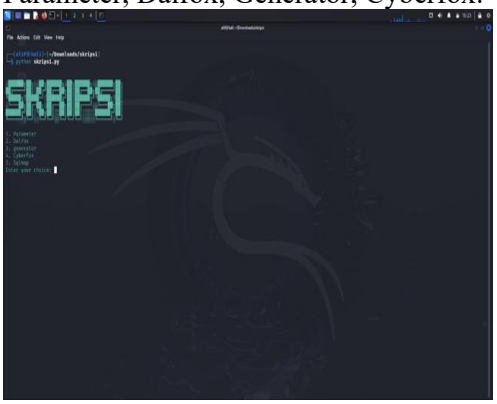
Ditahap ini penguji akan mengumpulkan dan melaporkan hasil pengujian kerentanan dan kemudian diberikan keterangan atas hasil dan temuan dari pengujian yang dilakukan.

**Implementasi Sistem**

Berikut ini dijelaskan tentang tampilan hasil dari perancangan sistem yang dibangun dapat dilihat sebagai berikut:

**Tampilan Utama**

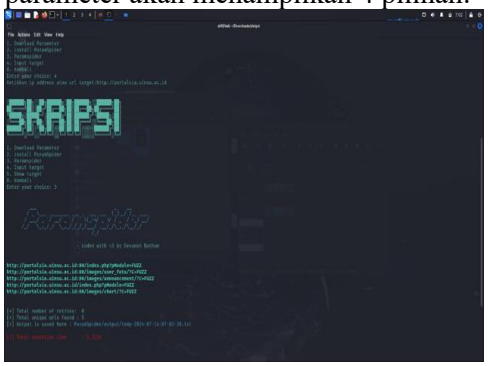
Tampilan Utama/ pertama yang akan tampil saat penguji menjalankan system ini, ditampilan ini terdapat 4 pilihan untuk memulai penetrasi yaitu Parameter, Dalfox, Generator, Cyberfox:




**Gambar 2 Tampilan Utama**

**Tampilan Parameter**

Jika penguji memilih 1 (satu) atau parameter akan menampilkan 4 pilihan:

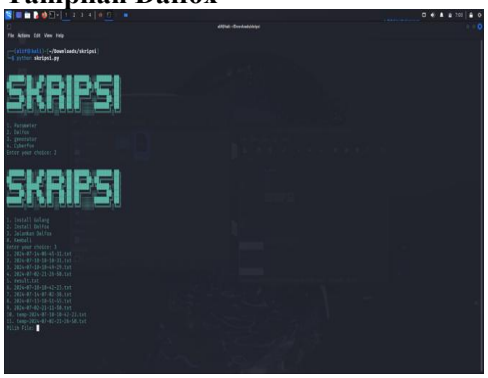



**Gambar 3 Tampilan Hasil Parameter**

Pada gambar diatas dapat dilihat hasil dari uji coba parameter pada url target dan hasil akan otomatis disimpan pada folder output yang sudah disediakan. Disini penguji mendapatkan 5 url yaitu:

1. http://portalsia.uinsu.ac.id:80/index.php?pModule=FUZZ
2. http://portalsia.uinsu.ac.id:80/images/user_foto/?C=FUZZ
3. http://portalsia.uinsu.ac.id:80/images/announcement/?C=FUZZ
4. http://portalsia.uinsu.ac.id/index.php?pModule=FUZZ
5. http://portalsia.uinsu.ac.id:80/images/chart/?C=FUZZ

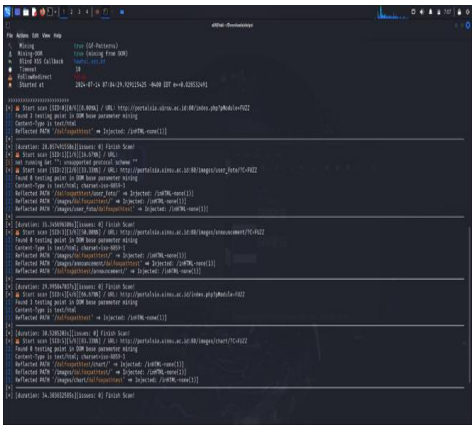
**Tampilan Dalfox**




**Gambar 4 Tampilan Dalfox**

Selanjutnya sistem akan otomatis menguji file tersebut, terlihat pada gambar dibawah adalah proses pengujian pada file yang diuji dan terlihat ada 5 Url yang diuji.

**Journal of Science and Social Research** ISSN 2615 – 4307 (Print)
August 2024, VII (3): 268 – 275 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



**Gambar 5 Tampilan Hasil Uji Coba Dalfox**

Dari hasil uji coba 5 url diatas ialah:

1. http://portalsia.uinsu.ac.id:80/index.php?pModule=FUZZ ditemukan 3 titik pengujian dalam penambang parameter, dan memantulkan 1 jalur dan menyuntikkan 1 dalfoxpathtest, dan tidak ditemukan sebuah masalah.
2. http://portalsia.uinsu.ac.id:80/images/user_foto/?C=FUZZ ditemukan 0 titik pengujian dalam penambang parameter, dan memantulkan 3 jalur untuk menyuntikkan 1 dalfoxpathtest, dan tidak ditemukan sebuah masalah.
3. http://portalsia.uinsu.ac.id:80/images/announcement/?C=FUZZ ditemukan 0 titik pengujian dalam penambang parameter, dan memantulkan 3 jalur untuk menyuntikkan 1 dalfoxpathtest, dan tidak ditemukan sebuah masalah.
4. http://portalsia.uinsu.ac.id:80/images/chart/?C=FUZZ ditemukan 0 titik pengujian dalam penambang parameter, dan memantulkan 3 jalur untuk menyuntikkan 1 dalfoxpathtest, dan tidak ditemukan sebuah masalah.
5. http://portalsia.uinsu.ac.id/index.php?pModule=FUZZ ditemukan 3 titik pengujian dalam penambang parameter, dan tidak ditemukan sebuah masalah.

**Tampilan *Generator*/*Penblood***


**Gambar 6 Tampilan *Penblood***

***Scanning***

Untuk menggunakan tools ini cara kerjanya sama seperti yang sebelumnya penguji bisa langsung pilih ingin mencoba yang mana dan untuk pilihan pertama yaitu scaning ada beberapa yang bisa dicoba penguji, dapat dilihat pada gambar dibawah.


**Gambar 7 Tampilan Dari *Scanning***

Dan disini penguji akan mencoba 1 tools yaitu Who is yang mana penguji akan melihat beberapa informasi tehadap url yang diuji, sebelum menjalankan penguji harus input URL terlebih dahulu dengan cara input 95 atau set target dan setelah itu penguji dapat menjalankan tools *Who Is*, dan hasil pengujian akan ditampilkan dan disimpan pada folder *output.*

***Generator***

Pada tools ini terdapat empat pilihan yaitu *Deface Page Generator, Password Generator, PLDT Wifi Password Calculator* dan *Text To Hash*, dapat dilihat pada gambar dibawah.


**Gambar 8 Tampilan *Generator***

Tampilan *Cyber Fox*

**Journal of Science and Social Research** ISSN 2615 – 4307 (Print)
August 2024, VII (3): 268 – 275 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

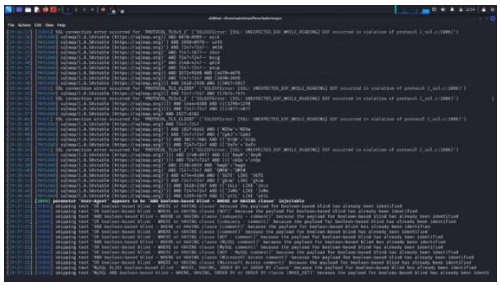
Pada tampilan Cyberfox terdapat 3 pilihan yaitu *Download Cyberfox*, *Install Cyberfox* dan Jalankan *Cyberfox*, *Cyberfox* ialah sebuah hackbar yang funsinya untuk melakukan serangan pada Url yang sudah diuji sebelumnya dan di *Cyberfox* penguji bisa menambahkan beberapa *Injection* yang bisa membantu penguji untuk menguji *website* target, dapat dilihat pada gambar dibawah.


**Gambar 9 Tampilan *Cyberfox***

**Tampilan Sqlmap**

Pada tampilan Sqlmap terdapat 2 pilihan yaitu Sqlmap, *Input Target, Sqlmap* ialah sebuah *tools* yang funsinya untuk melakukan serangan pada Url yang sudah diuji sebelumnya, dapat dilihat pada gambar dibawah penguji melakukan pengujian pada link http://portalsia.uinsu.ac.id:80/images/user foto/?C=.


**Gambar 10 Tampilan *SqlMap***



**Gambar 11 Tampilan Hasil *SqlMap***

## SIMPULAN

Berdasarkan hasil yang didapat dari peneltian yang dilakukan dalam penyusunan skripsi ini serta mengacu pada tujuan penelitian, maka dapat disimpulkan:

1. Untuk proses parameter penguji mendapatkan 5 url.
2. Pada pengujian dalfox atau *injected* XSS 5 url tidak memiliki masalah.
3. Untuk *scan* data di *penblood* penguji dapat beberapa informasi terkait *website* Portalsia UINSU.
4. Untuk hasil dari sqlmap yang mana beberapa kali sistem mendapatkan masalah untuk terhubung ke parameter. Dan parameter *host* tidak dapat di *injected* karena titik injeksi palsu atau tidak dapat di eksploitasi
5. Sistem yang dibangun dapat membantu bukan hanya untuk *website* Portalsia Uinsu.
6. Sistem yang dibangun dapat memberikan informasi dan menguji tentang kerentanan pada *website* target.

## DAFTAR PUSTAKA

Ahmad, P. A. (2021). Cyber Security Is More than Just a Question of Information Technology. *Journal of Image Processing and Intelligent Remote Sensing*, *12*, 1–7. https://doi.org/10.55529/jipirs12.1.7

Andharsaputri, R. L., Syahputra, E., & Prianto, W. (2021). Implementasi Rapid Application Development Pada Sistem Informasi Pengadaan Barang Dan Jasa. *JOISIE Journal Of Information System And Informatics Engineering*, *5*(1), 12.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi Dan*

*Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Burhani, L. F., & Priyawati, D. (2024). Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (PTES). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(1), 307–319. https://doi.org/10.29100/jipi.v9i1.4455

Costaner, L., & Musfawati, dan. (2020). 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)*, *5*(1), 45–55.

Firmansyah, D., Pasim Sukabumi, S., & Al Fath Sukabumi, S. (2022). Teknik Pengambilan Sampel Umum dalam Metodologi Penelitian: Literature Review. *Jurnal Ilmiah Pendidikan Holistik (JIPH)*, *1*(2), 85–114. https://doi.org/10.55927

Gustiyono, A., Alwi, E. I., & Abdullah, S. M. (2024). Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing. *CyberSecurity Dan Forensik Digital*, *7*(1), 25–33.

Kanade, A., Ranganthan, C. S., Jyothi Babu, A., Ramachandran, G., Kusuma, A. K., Anand, M., & Lokeswar Reddy, D. V. (2024). Analysis of wireless network security in internet of things and its applications. *Indian Journal of Engineering*, *21*(55). https://doi.org/10.54905/disssi.v21i55.e1ije1675

Lana Rahardian, R. (2022). Analisis Keamanan Web New Kuta Golf Menggunakan Metode Vulnerability Assessments Dan Perhitungan Security Metriks. *Jurnal Informatika Dan Teknologi Komputer*, *2*(3), 256–265.

Linggih Jaelani, W., & Khoirunnisa, F. (2023). Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan Website Pada Instansi (REDACTED). *NARATIF: Jurnal Ilmiah Nasional Riset Aplikasi Dan Teknik Informatika*, *05*(1), 1–8.

Mallaboyev, N. M., Qozaqova Munojat Sharifjanovna, Qosimov Muxammadjon, & Chimberdiyev Shukurullo. (2022). Information Security Issues. *International Congress on Multidisciplinary Studies in Education and Applied Sciences*.

Nawassyarif, M. Julkarnain, & Kiki Rizki Ananda. (2020). Sistem Informasi Pengolahan Data Ternak Unit Pelaksana Teknis Produksi Dan Kesehatan Hewan Berbasis Web. *Jurnal JINTEKS*, *2*(1), 32–39.

Putra Utama, F., Muhamad, R., & Nurhadi, H. (n.d.). Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method. *CommIT Journal*, *18*(1), 2024.

Rahardja, U., Handayani, I., & Elinda, B. D. (2021). Viewboard Jadwal Persiapan Sidang Pada Sistem PESSTA+ Menggunakan YII Framework di Perguruan Tinggi. *CSRID (Computer Science Research and Its Development Journal)*, *10*(3), 171. https://doi.org/10.22303/csrid.10.3.2018.171-179

Rayner, O. :, Chanarly, A., Munir, A., & Surasa, H. (2024). Analisis Keamanan Aplikasi Rememberme! Menggunakan Metode Vulnerability Assessment. *Jurnal KHARISMA Tech*, *19*(2), 27–35. https://jurnal.kharisma.ac.id/kharismatech

Setiawan, H. B., Sukamto, R. A., & Hambali, Y. A. (2025). Rancang Bangun Visual Novel Game Sebagai

Media Pengenalan Interview Kerja. *SIMKOM*, *10*(1), 87–100. https://doi.org/10.51717/simkom.v10i1.732

Studi Sistem Informasi Universitas Trilogi Jakarta Jl TMP Kalibata No, P., Tiga Kec Pancoran, D., Kunci, K., Kost, R., & Informasi, S. (2021). RANCANG BANGUN SISTEM INFORMASI SEWA RUMAH KOST (E-KOST) BERBASIS WEBSITE CHALIDAZIA NIZAR. *Jurnal Sistem Informasi Dan Sains Teknologi*, *3*(1).

Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web Application Penetration Testing on Udayana University's OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). *International Journal of Information Technology and Computer Science*, *16*(2), 45–56. https://doi.org/10.5815/ijitcs.2024.02.04