JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September Tahun 2025
ISSN 3025-0919 (media online)
Hal 1066-1068

Pengembangan Aplikasi Pengujian Kerentanan Keamanan Web Menggunakan Flask di PT. Aratech Nusantara Indonesia

Desi Kartika[1*], Sasa Mantiri[2*], Wanda Muharram[3], Sonasa Rinusantoro[4]

[1234]University of Pamulang, Jl. Raya Puspitek, Kec. Pamulang, Kota Tangerang Selatan, 15310, Indonesia
Email: [1]desikartika085@gmail.com, [2]sasamantiri2@gmail.com, [3]wandamuharram3@gmail.com, [4]dosen02289@unpam.ac.id

Abstrak− Keamanan sistem informasi menjadi prioritas utama seiring meningkatnya serangan siber terhadap aplikasi web. Penelitian ini bertujuan mengembangkan aplikasi pengujian kerentanan (penetration testing) berbasis web menggunakan framework Flask untuk mendukung kegiatan keamanan web di PT. Aratech Nusantara Indonesia. Metode yang digunakan adalah observasi, wawancara, dan studi pustaka, dilanjutkan dengan pengembangan perangkat lunak iteratif. Aplikasi yang dikembangkan dapat melakukan berbagai pengujian seperti port scanning, deteksi SSL, SQL Injection, XSS, dan Open Redirect, serta menyediakan laporan hasil dalam format PDF. Hasil menunjukkan aplikasi mampu mempercepat proses uji keamanan dan meningkatkan efisiensi tim teknis.

Kata Kunci: Keamanan web, Penetration testing, Flash, SQL Injection, XSS, Aratech

Abstract− *Information system security has become a top priority due to the increasing number of cyberattacks targeting web applications. This study aims to develop a web-based vulnerability testing (penetration testing) application using the Flask framework to support web security activities at PT. Aratech Nusantara Indonesia. The methods used include observation, interviews, and literature studies, followed by iterative software development. The developed application is capable of performing various tests such as port scanning, SSL detection, SQL Injection, XSS, and Open Redirect, and provides test result reports in PDF format. The results show that the application successfully accelerates the security testing process and improves the efficiency of the technical team.*

Keywords*: Web security, Penetration testing, Flask, SQL Injection, XSS, Aratech*

1. PENDAHULUAN

Pada era digital, kerentanan sistem informasi web menjadi sasaran utama serangan siber. Oleh karena itu, pengujian kerentanan web (web penetration testing) menjadi aspek penting dalam menjaga keamanan data dan sistem. PT. Aratech Nusantara Indonesia yang bergerak dalam bidang keamanan TI masih mengandalkan tools manual seperti Kali Linux, yang menuntut keahlian teknis tinggi dan kurang efisien. Penelitian ini merancang aplikasi uji keamanan yang terintegrasi dan lebih mudah digunakan, bertujuan untuk mendeteksi kerentanan umum secara otomatis.

2. METODE PENELITIAN

2.1 Jenis Penelitian

Penelitian ini menggunakan metode Research and Development (R&D), yaitu metode yang bertujuan untuk mengembangkan dan menguji aplikasi baru, dalam hal ini aplikasi PentestWeb untuk pengujian keamanan website secara otomatis.

2.2. Tahapan Penelitian

a. Studi Literatur

Peneliti melakukan studi literatur terkait keamanan aplikasi web, jenis-jenis kerentanan (seperti SQL Injection, XSS, LFI, Directory Traversal, Open Redirect), serta teknologi dan tools yang relevan seperti Flask, sqlmap, nmap, dan requests.

b. Analisis Kebutuhan

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September Tahun 2025
ISSN 3025-0919 (media online)
Hal 1066-1068

Analisis kebutuhan dilakukan untuk menentukan fitur-fitur yang harus ada pada aplikasi, seperti scan otomatis berbagai kerentanan, export hasil ke PDF, dan tampilan antarmuka yang mudah digunakan.

c. Perancangan Sistem

Perancangan sistem dilakukan dengan membuat diagram activity, use case, sequence, dan flowchart untuk menggambarkan alur kerja aplikasi, serta desain antarmuka pengguna (UI).

d. Implementasi

Aplikasi dikembangkan menggunakan bahasa Python dengan framework Flask. Fitur utama yang diimplementasikan meliputi:

1. Scan header keamanan, SSL, port, SQL Injection, XSS, LFI, Directory Traversal, dan Open Redirect.
2. Export hasil scan ke PDF.
3. Antarmuka web responsif dan mudah digunakan.

e. Pengujian (Testing)

Pengujian dilakukan dengan memasukkan berbagai URL target dan memeriksa apakah aplikasi dapat mendeteksi kerentanan yang ada serta menghasilkan laporan PDF yang sesuai. Pengujian juga mencakup validasi input dan penanganan error.

f. Evaluasi

Evaluasi dilakukan dengan membandingkan hasil scan aplikasi dengan tools manual atau tools lain, serta mengumpulkan feedback dari pengguna terkait kemudahan penggunaan dan keakuratan hasil.
Evaluasi dilakukan dengan membandingkan hasil scan aplikasi dengan tools manual atau tools lain, serta mengumpulkan feedback dari pengguna terkait kemudahan penggunaan dan keakuratan hasil.

3. ANALISA DAN PEMBAHASAN

Pada bagian ini berisi hasil dari kegiatan penelitian yang sudah dilakukan

a. Arsitektur Sistem

Peneliti melakukan studi literatur terkait keamanan aplikasi web, jenis-jenis kerentanan (seperti SQL Injection, XSS, LFI, Directory Traversal, Open Redirect), serta teknologi dan tools yang relevan seperti Flask, sqlmap, nmap, dan requests.

b. Fitur Utama

Input Target: URL atau IP address
Jenis Pengujian: port scan, security headers, SSL/TLS, SQLi, XSS, LFI, Directory Traversal, dan Open Redirect

c. Laporan: Hasil uji ditampilkan secara langsung dan dapat diekspor ke PDF menggunakan WeasyPrint.

d. Uji Coba

Pengujian dilakukan terhadap berbagai target URL dengan simulasi serangan umum. Hasil menunjukkan aplikasi mampu mengidentifikasi kerentanan secara cepat, dan laporan PDF dapat dihasilkan secara otomatis.

e. Analisis

Pendekatan modular pada tiap jenis pengujian menjadikan aplikasi mudah dikembangkan. Validasi input dilakukan sebelum scanning untuk menghindari kesalahan. Aplikasi memberikan nilai tambah berupa kecepatan dan kemudahan dokumentasi uji keamanan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September Tahun 2025
ISSN 3025-0919 (media online)
Hal 1066-1068

4. KESIMPULAN

Aplikasi pengujian kerentanan berbasis web berhasil dikembangkan menggunakan Flask dengan fitur utama yang mendukung kegiatan penetration testing internal. Penggunaan tools ini membantu PT. Aratech Nusantara Indonesia dalam meningkatkan efisiensi dan efektivitas proses pengujian keamanan web.

SARAN

1. Pengembangan selanjutnya dapat mencakup:
2. Penyimpanan hasil scan ke database.
3. Implementasi fitur login dan hak akses.
4. Integrasi dengan pipeline CI/CD.
5. Pengujian performa dan dokumentasi teknis lanjutan.

REFERENCES

Grinberg, M. (2018). Flask Web Development (2nd ed.). O'Reilly.

McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley.

Nmap Project. (2023). Nmap Reference Guide.

OWASP Foundation. (2023). OWASP Top 10 Web Application Security Risks.

Stasinopoulos, D. (2012). sqlmap: Automatic SQL Injection and Database Takeover Tool.

WeasyPrint. (2023). HTML to PDF Generator.