STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 4 No. 1, Februari 2025, 16 - 21
e-ISSN: 2828-5344 | DOI: 10.55123

TEKNIK PENGUJIAN PENETRASI HTTP MENGGUNAKAN TOOLS BURP SUITE PADA KALI LINUX

[1)] Vanisa Dwi Agustina, [2)] Tamsir Ariyadi, [3)]Tari Syah Putra, [4)]Ahmad Lega

[1,2,3,4)] Prodi Teknik Komputer, Universitas Bina Darma Palembang
Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Palembang

[1,2,3,4)] vanisadwiagustinaa@gmail.com, tamsirariyadi@binadarma.ac.id, tari.saputra08@gmail.com, ahmadlega123@gmail.com

INFO ARTIKEL

Riwayat Artikel :
Diterima : 12 Januari 2025
Disetujui : 2 Februari 2025

Kata Kunci :
Pengujian keamanan web, Burp Suite, Penetrasi aplikasi web, Analisis kerentanan, Serangan siber.

ABSTRAK

Burp Suite adalah alat yang digunakan untuk melakukan pengujian keamanan pada aplikasi web, dengan kemampuan untuk mengidentifikasi dan mengeksploitasi kerentanannya. Alat ini menyediakan berbagai fitur seperti Intercepting Proxy, Scanner, Intruder, dan Repeater, yang memungkinkan pengguna untuk menganalisis lalu lintas HTTP/HTTPS, mencari kerentanan otomatis, serta menguji ketahanan aplikasi terhadap input berbahaya. Burp Suite banyak digunakan oleh para profesional keamanan untuk memastikan bahwa aplikasi web yang diuji bebas dari celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Penelitian ini bertujuan untuk menjelaskan fungsi, penggunaan, serta potensi Burp Suite dalam pengujian keamanan aplikasi web, serta memberikan saran penggunaan yang efektif untuk hasil yang maksimal.

ARTICLE INFO

Article History :
Received : Jan 12, 2025
Accepted : Feb 2, 2025

Keywords*:*
Web security testing, Burp Suite, Web application penetration, Vulnerability analysis, Cyber attack.

ABSTRACT

Burp Suite is a tool used for security testing on web applications, with the capability to identify and exploit vulnerabilities. This tool provides various features such as Intercepting Proxy, Scanner, Intruder, and Repeater, which allow users to analyze HTTP/HTTPS traffic, automatically search for vulnerabilities, and test the application's resilience against malicious inputs. Burp Suite is widely used by security professionals to ensure that web applications being tested are free from exploitable flaws. This study aims to explain the functions, usage, and potential of Burp Suite in web application security testing, as well as provide recommendations for effective use to achieve optimal results..

1. PENDAHULUAN

Aplikasi web telah menjadi bagian penting dari kehidupan sehari-hari, digunakan oleh individu maupun organisasi untuk berbagai tujuan, seperti berkomunikasi, melakukan transaksi bisnis, dan mengelola data pribadi. Seiring dengan peningkatan teknologi dan penggunaan aplikasi web, muncul masalah keamanan yang signifikan. Karena kerentanannya yang terkadang tidak terdeteksi atau diabaikan, aplikasi web sering menjadi sasaran utama serangan siber. Seiring dengan peningkatan teknologi dan penggunaan aplikasi web, muncul masalah keamanan yang signifikan. Karena kerentanannya yang terkadang tidak terdeteksi atau diabaikan, aplikasi web sering menjadi sasaran utama serangan siber. Salah satu masalah terbesar dalam menjaga keamanan aplikasi web adalah mendeteksi dan menangani bug keamanan yang dapat digunakan oleh pihak yang tidak bertanggung jawab.

Dengan teknik serangan yang semakin canggih yang digunakan oleh peretas, ancaman terhadap aplikasi web telah meningkat dalam beberapa tahun terakhir. Kekuatannya dalam aplikasi web dapat digunakan untuk berbagai tujuan, seperti pencurian data dan manipulasi data, hingga serangan yang lebih kompleks, seperti menyebarkan malware melalui celah keamanan atau melakukan serangan terhadap sistem yang lebih besar. Oleh karena itu, sangat penting untuk menemukan dan mengatasi kemungkinan kerusakan sebelum digunakan oleh orang yang tidak bertanggung jawab. Dalam hal ini, pengujian keamanan harus dilakukan untuk memastikan bahwa aplikasi web tetap aman untuk digunakan.

Burp Suite adalah platform pengujian keamanan aplikasi web yang sangat disukai oleh profesional keamanan siber. Banyak alat dan teknik telah dikembangkan untuk menemukan masalah keamanan aplikasi web. Berbagai fitur yang ditawarkan oleh program ini memungkinkan pengujian dan analisis aplikasi web secara menyeluruh untuk menemukan potensi kerentanannya dan menawarkan solusi untuk memperbaikinya. Burp Suite memiliki fitur utama seperti Intercepting Proxy, Scanner, Intruder, dan Repeater. Semuanya memiliki kemampuan untuk mengatur dan menganalisis lalu lintas HTTP/HTTPS antara pengguna dan server. Alat ini memungkinkan pengujian keamanan dilakukan secara menyeluruh dan efektif untuk menemukan masalah keamanan yang mungkin terlewatkan oleh pengujian lainnya.

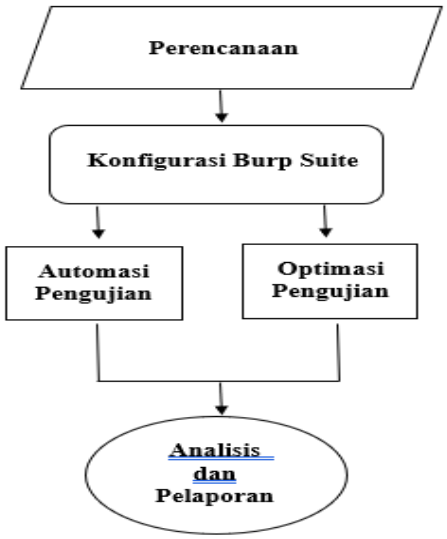
Karena banyaknya kerentanannya yang tidak terdeteksi, aplikasi web sering menjadi sasaran serangan, menurut penelitian sebelumnya. Aplikasi web rentan terhadap berbagai serangan, seperti SQL Injection, XSS, dan CSRF, yang sering digunakan oleh peretas, menurut laporan OWASP (Open Web Application Security Project) (OWASP, 2022). PortSwigger (2023) menyatakan bahwa Burp Suite adalah alat yang sangat baik untuk menemukan celah ini dan menggunakannya. Salah satu fitur canggih Burp Suite adalah Intercepting Proxy, yang memungkinkan pengguna untuk menganalisis dan mengubah permintaan HTTP/HTTPS, dan Scanner, yang dapat secara otomatis mengidentifikasi kerentanannya di aplikasi web. Burp Suite sangat efektif dalam mendeteksi kerentanan aplikasi berbasis web seperti SQL Injection dan XSS, menurut penelitian sebelumnya oleh Smith et al. (2020).

Menurut penelitian Sharma & Gupta (2022), penggunaan alat seperti Burp Suite sangat penting untuk menguji aplikasi web modern yang menggunakan teknologi seperti AJAX dan API. Penggunaan Burp Suite dalam pengujian keamanan aplikasi web sangat penting untuk memastikan bahwa aplikasi yang diuji aman dari ancaman yang ada karena kerentanannya telah terbukti dapat dideteksi oleh alat lain.

2. METODE

Metode sistematis dan berbasis alat otomatisasi digunakan dalam penelitian ini untuk menilai keamanan aplikasi web yang menggunakan fitur yang ada di Burp Suite. Metode ini melibatkan serangkaian tahapan terstruktur, mulai dari perencanaan hingga penyusunan rekomendasi keamanan. Penelitian ini bertujuan untuk menemukan kerentanan

keamanan yang dapat membahayakan aplikasi web secara efektif dan tepat dengan menggunakan kombinasi pengujian otomatis dan manual.



Gambar 1 . Diagram Alur Metodologi

Berikut untuk penjelasan lebih lanjut tentang Diagram Alur Metodologi keamanan web menggunakan Burp Suite:

1. Perencanaan (Planning)

Proses ini dimulai dengan tahapan perencanaan. Pada titik ini, lingkup pengujian telah didefinisikan dengan jelas. Komponen seperti endpoint sensitif, formulir input, dan API aplikasi dipilih oleh tim penguji untuk diuji. Tujuan pengujian juga dijelaskan. Misalnya, mereka bertujuan untuk mengidentifikasi kerentanan umum seperti SQL Injection atau Cross-Site Scripting (XSS), atau untuk mengevaluasi seberapa baik mekanisme autentikasi yang digunakan. Sehingga pengujian dapat dilakukan secara legal dan etis, perencanaan juga diperlukan untuk mendapatkan izin dari pemilik sistem.

2. Konfigurasi Burp Suite

Setelah tahap perencanaan selesai, dilanjutkan dengan tahapan konfigurasi Burp Suite. Pada saat ini, Burp Suite disiapkan untuk memenuhi kebutuhan pengujian. Pengaturan dilakukan untuk memastikan Burp Suite dapat melacak lalu lintas antara browser dan server. Ini memungkinkan analisis setiap permintaan dan respons aplikasi.

Ruang lingkup endpoint yang akan diuji dan penyesuaian fitur otomatis seperti sensitivitas pemindaian adalah konfigurasi tambahan. Jika diperlukan, Burp Extender dapat digunakan untuk menambahkan ekstensi tambahan yang sesuai dengan kebutuhan pengujian tertentu.

3. Automasi Pengujian

Automasi Pengujian adalah langkah berikutnya, yang menggunakan kemampuan otomatis Burp Suite untuk menemukan kerentanan umum. Fitur seperti Burp Scanner melakukan pemindaian menyeluruh pada aplikasi web untuk menemukan kerentanan keamanan seperti SQL Injection dan Cross-Site Scripting (XSS), antara lain.

4. Optimasi Pengujian

Setelah itu, optimalisasi pengujian dilakukan untuk memastikan bahwa hasil pengujian lebih akurat dan relevan. Pada tahap ini, hasil pemindaian otomatis ditinjau untuk menghilangkan false positives dan menemukan kemungkinan kesalahan yang memerlukan pengujian lebih lanjut. Pembuatan payload khusus untuk menguji skenario tertentu juga dapat menjadi bagian dari proses optimasi.

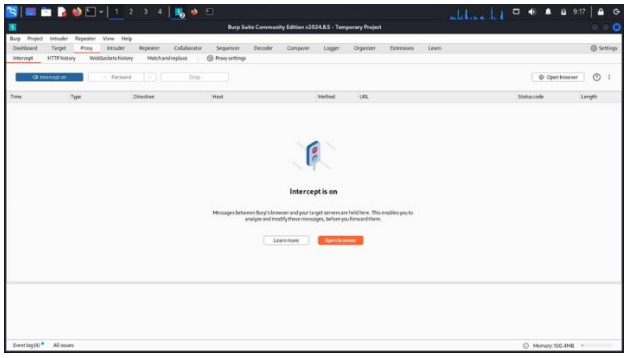
5. Analisis dan Pelaporan

Analisis dan pembuatan saran adalah tahap akhir dari pendekatan ini. Pada titik ini, hasil pengujian dinilai untuk mengevaluasi tingkat risiko setiap kerentanan. Analisis ini bertujuan untuk menentukan konsekuensi yang mungkin disebabkan oleh kerentanan terhadap aplikasi dan pengguna serta kemungkinan eksploitasi oleh pihak yang tidak bertanggung jawab.

Laporan dibuat berdasarkan hasil analisis dan mencakup saran yang jelas dan khusus untuk mengatasi masalah. Sehingga perbaikan dapat segera dilakukan, laporan ini dibuat untuk dipahami oleh tim pengembang dan pemangku kepentingan.

3. HASIL DAN PEMBAHASAN

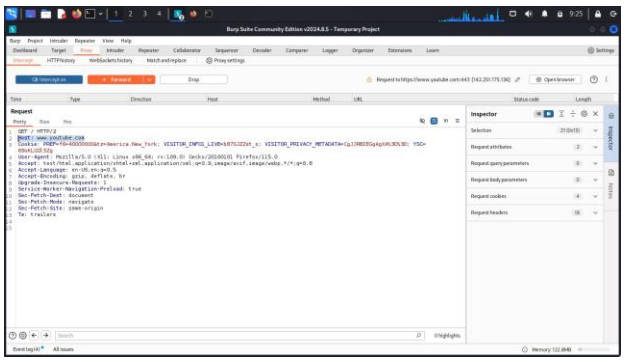
1. Pada Burpsuite, nyalakan interceptnya.



Gambar 2. Menyalakan Intercept

Pengguna akan dibawa ke antarmuka awal Burp Suite setelah penginstalan berhasil. Untuk memulai pengujian cepat, pilih opsi Temporary Project dan klik tombol Next untuk melanjutkan ke pengaturan berikutnya. Setelah memilih pengaturan default, klik Start Burp untuk memulai aplikasi.

2. Setelah itu coba buka kembali Firefox dan coba search situs web apa saja. Disini saya mencoba membuka situs web Youtube. Setelah membuka Youtube pada Firefox, buka kembali Burpsuite maka tampilannya akan seperti gambar dibawah ini.

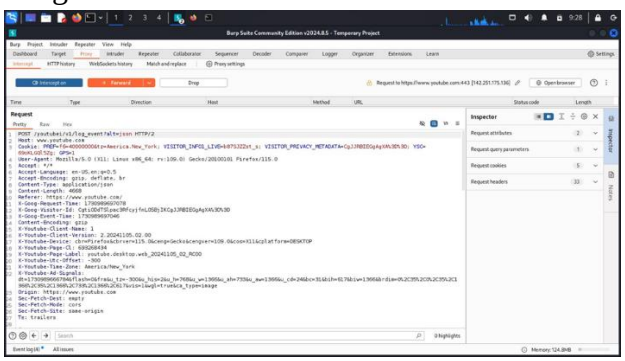


Gambar 3. Membuka Kembali Firefox

Tab Proxy Burp Suite dapat menangkap dan merekam semua permintaan HTTP dan tanggapan yang melewati proxy Burp Suite.

a. Anda harus memastikan bahwa browser yang Anda gunakan telah dikonfigurasi untuk menggunakan proxy Burp Suite, biasanya pada port 8080. Anda dapat memeriksa atau mengubah pengaturan ini di tab Proxy > Options.
b. Setelah membuka situs web atau mengirimkan data melalui formulir browser, Burp Suite akan mengumpulkan dan menyimpan semua permintaan HTTP.
c. Di HTTP History, Anda dapat melihat daftar permintaan yang muncul, yang mengandung informasi seperti URL, metode HTTP, status tanggapan, dan waktu pengambilan.

3. Coba buka kembali Youtube dan buka Burpsuite, maka datanya akan keluar seperti gambar dibawah ini.



Gambar 4. Data Pada Web YouTube

Burp Suite memberikan detail permintaan HTTP yang lengkap untuk analisis lanjutan setelah permintaan HTTP berhasil ditangkap. Analisis ini mencakup header, parameter, dan body permintaan.

4. PENUTUP

4.1. Kesimpulan

Burp Suite adalah salah satu alat yang sangat berguna dan berguna untuk pengujian keamanan aplikasi web. Berbagai fiturnya, seperti Intercepting Proxy, Scanner, Intruder, dan Repeater, memungkinkan profesional keamanan untuk menganalisis dan menemukan kerentanan dalam aplikasi web. Alat ini tidak hanya digunakan untuk menemukan celah keamanan, tetapi juga membantu proses eksploitasi dan mitigasi risiko dengan lebih efisien dan terorganisir. Penggunaan Burp Suite menjadi standar bagi penetration tester dan ethical hacker untuk menguji dan memperbaiki aplikasi web agar lebih aman seiring dengan meningkatnya ancaman terhadap aplikasi web.

Meskipun Burp Suite memiliki banyak fitur, pengguna baru mungkin kesulitan memanfaatkan semua fiturnya karena mereka

perlu memahami teknik pengujian keamanan dan aplikasi web.

4.2. Saran

1. Pelatihan dan Pembelajaran Lanjutan

Para penguji penetrasi atau profesional keamanan harus mendapatkan pelatihan yang memadai untuk memanfaatkan Burp Suite secara optimal. Pelatihan dan pelatihan yang ditawarkan oleh platform seperti PortSwigger akan sangat membantu dalam memahami berbagai fitur dan teknik yang dapat digunakan untuk menemukan dan mengatasi kerentanannya di aplikasi web.

2. Penerapan secara Teratur

Pengujian berkala sangat penting untuk menjaga aplikasi web aman dan aman dari ancaman yang terus berkembang. Pengujian aplikasi web harus dilakukan secara teratur dengan menggunakan alat seperti Burp Suite untuk menemukan masalah keamanan yang muncul seiring dengan pembaruan atau perubahan dalam aplikasi

3. Integrasi dengan Alat Lain

Meskipun Burp Suite adalah alat yang sangat kuat, disarankan untuk menggunakannya bersama dengan alat pengujian keamanan seperti OWASP ZAP atau Nessus untuk mendapatkan gambaran yang lebih baik tentang kemungkinan kerentanan dalam aplikasi web.

4. Peningkatan Penggunaan Fitur Lanjutan

Untuk memenuhi kebutuhan pengujian aplikasi tertentu, pengguna Burp Suite harus mengeksplorasi fitur tambahan seperti Burp Suite Enterprise dan Burp Collaborator.

5. Kesadaran dan Kepatuhan terhadap Etika Pengujian

Selalu ingat untuk melakukan pengujian keamanan dengan izin yang tepat dan mematuhi hukum serta etika yang berlaku. Pengujian penetrasi harus dilakukan hanya pada aplikasi yang telah memperoleh persetujuan atau di bawah pengawasan profesional yang berlisensi.

5. DAFTAR PUSTAKA

Ardiantoro, C. and Puspitasari, N.F. (2024) ‘Analisis Kerentanan Website Xyz Repository Management Project’, *Jurnal Elektrosista*, 11(2).

Aziz Khozindani, A., Muhyidin, Y. and Sunandar, M.A. (2023) ‘Perbandingan Kinerja Tools Wireshark Dan Burpsuite Untuk Penyerangan Website Dengan Metode Sniffing’, *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(3), pp. 2026–2031. Available at: https://doi.org/10.36040/jati.v7i3.7013.

Indera, R., Budiono, A. and Hediyanto, U.Y.K.S. (2023) ‘Vulnerability Assessment Pada Situs Web KPPM FRI Dengan Burp Suite dan Intruder’, *e-Proceeding of Engineering*, 10(2), pp. 1623–1630.

Kondraciuk, A., Bartos, A. and Pańczyk, B. (2022) ‘Comparative analysis of the effectiveness of OWASP ZAP, Burp Suite, Nikto and Skipfish in testing the security of web applications’, *Journal of Computer Sciences Institute*, 24(April), pp. 176–180. Available at: https://doi.org/10.35784/jcsi.2929.

Mainka, C. *et al.* (2015) ‘Automatic recognition, processing and attacking of single sign-on protocols with burp suite’, *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, 251, pp. 117–131.

Ni Putu Ana Rainita *et al.* (2023) ‘Analisis Perbandingan Vulnerability Scanning Pada Website Dvwa Menggunakan Owasp Nikto Dan Burpsuite’, *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, 3(2), pp. 89–97. Available at: https://doi.org/10.55606/jitek.v3i2.908.

Pormes, R. *et al.* (2024) ‘ANALISIS KEAMANAN WEBSITE E-LEARNING POLITEKNIK BHAKTI SEMESTA BERBASIS VULNERABILITY ASSESSMENT’, 12(02).

Sampul, H. (2024) ‘Analisis kinerja burp suite comunnity edition dan owasp- zap dalam mendeteksi vulnerability sql injectio dan cross-site scripting (xss) pada website dvwa’.

Subari, A. *et al.* (2021) ‘Pemanfaatan Metode Wavs (Web Application Security Scanners) Menggunakan Burp Suite Tools Dalam Audit Teknis Keamanan Sistem Informasi Surat Tugas Sekolah Vokasi Undip’, *Gema Teknologi*, 21(4), pp. 125–130. Available at: http://st2.vokasi.undip.ac.id.

Yum Thurfah Afifa Rosaliah, J.J.B.H. (2021) ‘Pengujian Celah Keamanan Website

Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM', *Senamika*, 2(September), pp. 752–761.