Jurnal Tera
Volume 5, Issue 2, September 2025
Page 49-58

E-ISSN : 2776-9666
P-ISSN : 2776-1789

PENERAPAN BURPSUITE UNTUK MENGIDENTIFIKASI SERANGAN PADA JARINGAN WIRELESS

Eka Novitasari[1], Tamsir Ariyadi[2], Dwi Pertiwiningsih[3]
[1,2,3)] Universitas Bina Darma, Sumatra Selatan, Indonesia

Corresponding author

E-mail : tamsirariyadi@binadarma.ac.id, novitasarie739@gmail.com, dwipertiwiningsih69@gmail.com

Diterima : 25-12-2025
Direvisi : 05-01-2026
Dipublikasi : 20-01-2026

Kata Kunci: Burpsuite, Jaringan Wireless,analisis kerentanan

Abstrak: BurpSuite adalah sebuah platfrom untuk pengujian keamanan pada aplikasi web yang terdiri dari berbagai macam alat yang bekerja sama untuk mendeteksi dan mengeksploitasi pada kerentanannya.Selain itu,Keamanan jaringan wireless merupakan aspek penting dalam perlindungan data dan menjaga kerahasiaan.Macam-macam serangan jaringan wireless seperti *session hijacking*,*man-in-the-middle*,dan *hijacking attack,parameter tampering*.Tujuan Penelitian ini untuk mengetahui sejauh mana BurpSuite digunakan sebagai alat evaluasi keamanan pada jaringan serta panduan untuk melakukan analisis resiko keamanan.Penelitian ini diharapkan dapat memberikan pemahaman lebih luas bahwa Burpsuite merupakan alat yang sangat efektif dalam membantu proses identifikasi serangan serta mendukung untuk peningkatan keamanan jaringan wireless melalui proses analisis yang sistematis.

Abstrak: BurpSuite is a platform for security testing on web applications that consists of a wide variety of tools that work together to detect and exploit vulnerabilities. In addition, wireless network security is an important aspect of data protection and maintaining confidentiality. Various wireless network attacks such as session hijacking, man-in-the-middle, and hijacking attack, parameter tampering. The purpose of this study is to find out the extent to which BurpSuite is used as a security evaluation tool on the network as well as a guide to conduct security risk analysis. This research is expected to provide a broader understanding that Burpsuite is a very effective tool in assisting in the process of identifying attacks and supporting the improvement of wireless network security through a systematic analysis process.

1.PENDAHULUAN

Pada Era Modern sekarang jaringan wireless bukanlah hal yang baru,hampir diseluruh tempat seperti Perusahaan,Rumah,Kampus,dan area publik.Banyak terdapat jaringan Wireless untuk memperlancar suatu koneksi internet dan informasi di tempat tersebut.Dalam jaringan Wireless sudah banyak data yang sudah berlalu lalang melalui kabel jaringan,baik dalam paket data yang mengandung sebuah informasi penting yang bersifat sangat pribadi,alamat dari suatu situs,dan lainnya..Secara umum jaringan yang telah terhubung pada keamanan menunjukan sangat rendah dan tidak selalu aman sehingga dapat diretas oleh para hacker.

Sekarang ini sudah ada beberapa teknik dalam penyerangan terhadap sistem keamanan yang mencoba masuk menyerang seperti mencuri password,merusak sistem,mencuri database,dan mengirimkan paket data yang berjumlah besar terhadap server,serangan keamanan tersebut berupa serangan *Man-In-The-Middle,*.serangan *session hijacking,serangan Parameter Tampering* dan serangan *hijacking attack.*

Dalam mengurangi resiko tersebut,diperlukannya upaya untuk pengujian keamanan jaringan melalui metode penetration testing.Salah satu tools yang banyak sekali digunakan dalam proses pengujian tersebut adalah Burpsuite.Burpsuite merupakan aplikasi intercepting proxy yang memilikki kemampuan-kemampuan untuk menganalisis trafik,mengidentifikasi pada celah kemanan,dan mensimulasikan serangan suatu sistem ataupun jaringan.Penerapan Burpsuite ini tidak hanya digunakan pada aplikasi berbasis web,namun dapat dimanfaatkan untuk mendeteksi aktivitas serangan pada jaringan wireless yang melalui analisis trafik data melewati jaringan tersebut.

Sebab itu,penelitian ini dilakukan untuk menerapkan Burpsuite sebagai alat bantu untuk mengidentifikasi potensi serangan pada jaringan wireless,serta memberikan gambaran terhadap tingkat-tingkat resiko keamanan dan kebutuhan terhadap peningkatan pada perlindungan jaringan.

2. KAJIAN PUSTAKA

2.1 Jaringan Wireless

Jaringan wireless adalah teknologi jaringan yang memungkinkan suatu perangkat saling terhubung tanpa menggunakan kabel,melainkan melalui gelombang elektromagnetik.Jaringan

Wireless juga banyak digunakan seperti perusahaan,kampus,rumah,dan area publik.Teknologi ini memungkinkan pengguna dapat mengakses jaringan internet untuk memperlancar suatu koneksi internet dan arus informasi pada tempat tersebut.Namun,jaringan wireless yang bersifat transmisi terbuka dapat menyebabkan jaringan ini sangat rentan terhadap serangan,sehingga diperlukannya pengelolaan keamanan yang baik untuk melindungi pencurian data serta hacker.

2.2 Burpsuite

Burpsuite merupakan salah satu tools penetration testing yang banyak sekali digunakan untuk menganalisis dan menguji suatu keamanan aplikasi web serta lalu lintas pada jaringan.Burpsuite juga memiliki fitur-fitur seperti *intercepting proxy*,*scanner*,*repeater*,dan *intruder*.Dalam jaringan wireless,Burpsuite dapat dimanfaatkan untuk mengidentifikasi serangan,mengidentifikasi aktivitas yang mencurigakan,menguji kerentanan komunikasi,dan mensimulasikan serangan yang berbasis web yang berjalan diatas jaringan wireless.

3. METODE PENELITIAN

Penelitian ini dilakukan dengan memulai beberapa tahap proses yang dimulai dengan instalasi burpsuite pada sistem operasi Kali Linux.Menjalankan Burpsuite,mengkonfigurasi proxy,dan menghubungkan browser ke Burpsuite,Menangkap trafik jaringan pada wireless,menganalisis request,response,session,dan melakukan simulasi serangan serta mengidentifikasi potensi keamanan.

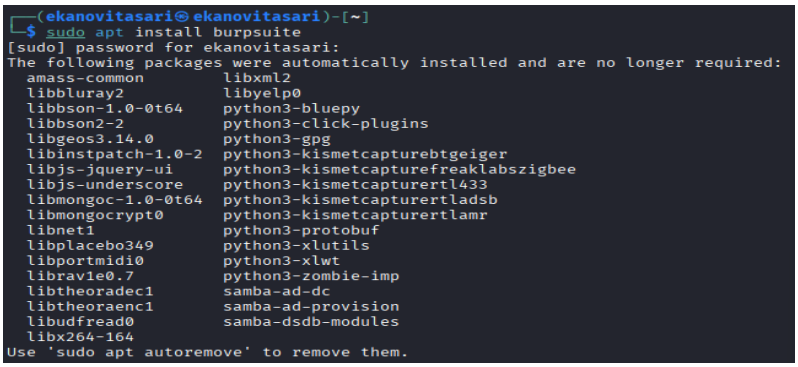
3.IMPLEMENTASI

3.1 Instalasi Burpsuite pada kali linux

3.1.1 Proses instalasi Burpsuite

Pada tahap pertama ini dilakukan proses instalasi Burpsuite pada kali linux,dengan menggunakan mesin VirtualBox.Setelah terinstal Burpsuite,kemudian klik pada menu pencarian di sana akan muncul Burpsuitenya.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

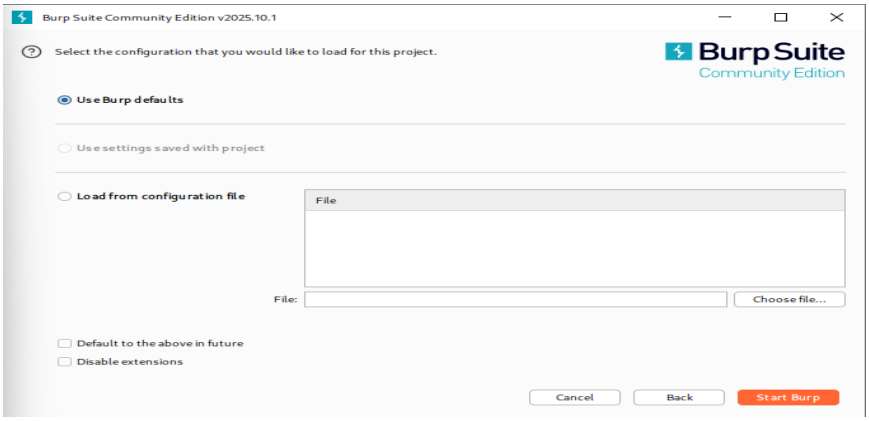


Gambar 1.proses penginstalan Burpsuite

3.2.1 Tampilan awal Burpsuite

Gambar 2,menunjukkan tampilan awal pada aplikasi BurpSuite *Community Edition* yang dijalankan pada sistem operasi Kali Linux. Pada tahap ini, BurpSuite belum dikonfigurasi sebagai proxy dan belum menangkap lalu lintas jaringan.

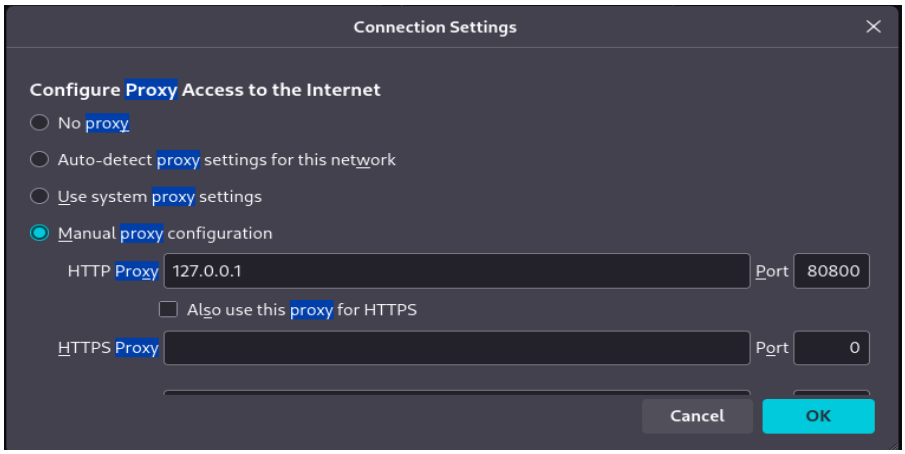
.



Gambar 2. Tampilan awal Burpsuite

3.3.1 Konfigurasi Proxy pada Burpsuite

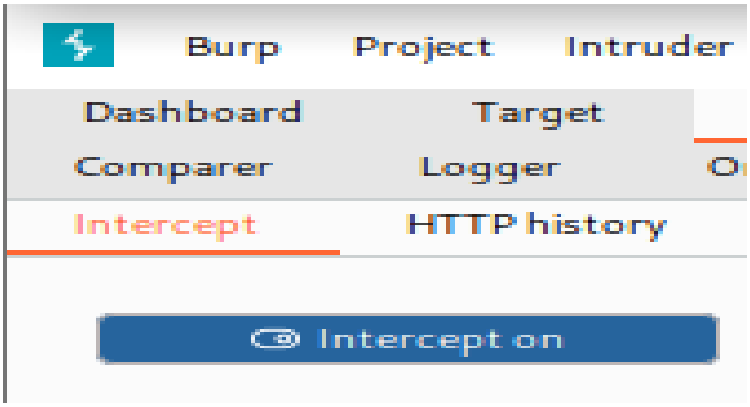
Gambar 3,memperlihatkan konfigurasi proxy pada BurpSuite menggunakan alamat ip **127.0.0.1** dan port **8080**. Konfigurasi ini bertujuan agar BurpSuite dapat berfungsi sebagai *intercepting proxy* untuk menangkap lalu lintas jaringan wireless



Gambar 3. Konfigurasi Proxy

3.4.1 Aktivasi Intercept Proxy

Gambar 4,menampilkan fitur Intercept On pada Burpsuite.Saat fitur ini di aktifkan,maka setiap permintaan (*request*) dari client akan ditahan terlebih dahulu oleh Burpsuite sebelum diteruskan ke server.

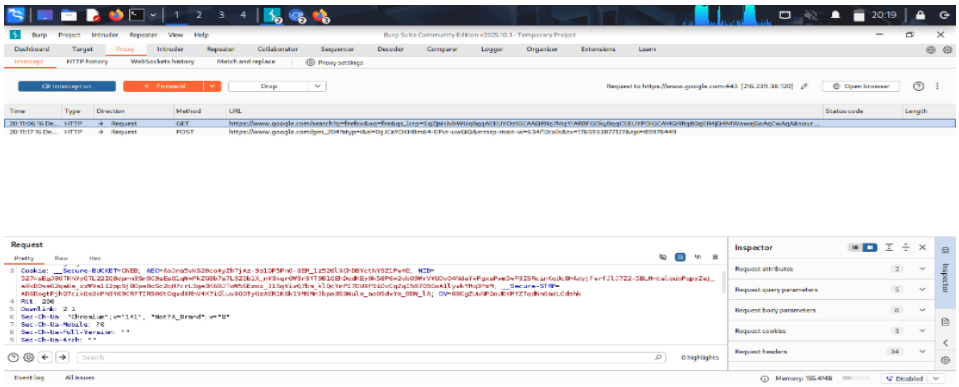


Gambar 4. Mengaktifkan Intercept proxy

3.5.1 Penangkapan Request HTTP

Gambar 5,memperlihatkan request **HTTP** yang berhasil ditangkap oleh BurpSuite saat client mengakses suatu website misalnya "**Firefox**" melalui jaringan wireless. Informasi seperti *method*, *URL*, dan parameter yang dapat dianalisis

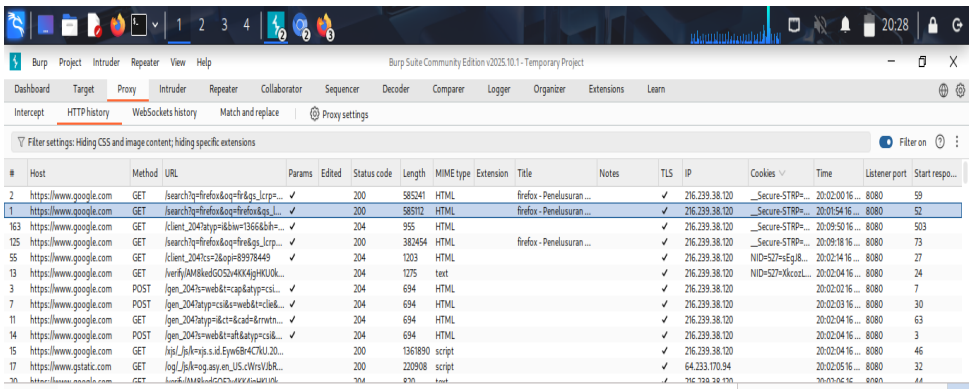
.



Gambar 5. Request yang berhasil ditangkap oleh Burpsuite

3.6.1 Analisis session dan cookie

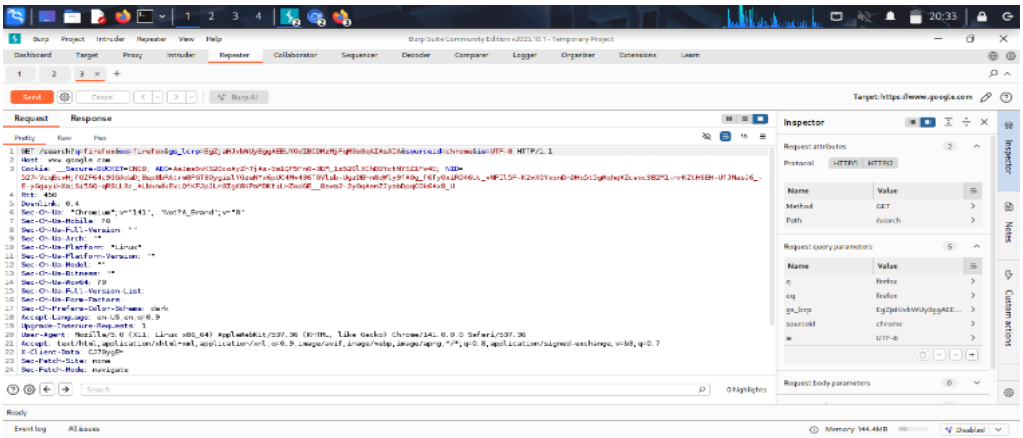
Gambar 6, menunjukkan analisis pada session dan cookie pada menu **HTTP History**. Informasi cookie yang tertangkap dapat digunakan untuk mengidentifikasi potensi *serangan session hijacking*.



Gambar 6. Menunjukan hasil analisis session dan cookie pada menu **HTTP History**

3.7.1 Modifikasi request menggunakan Repeater

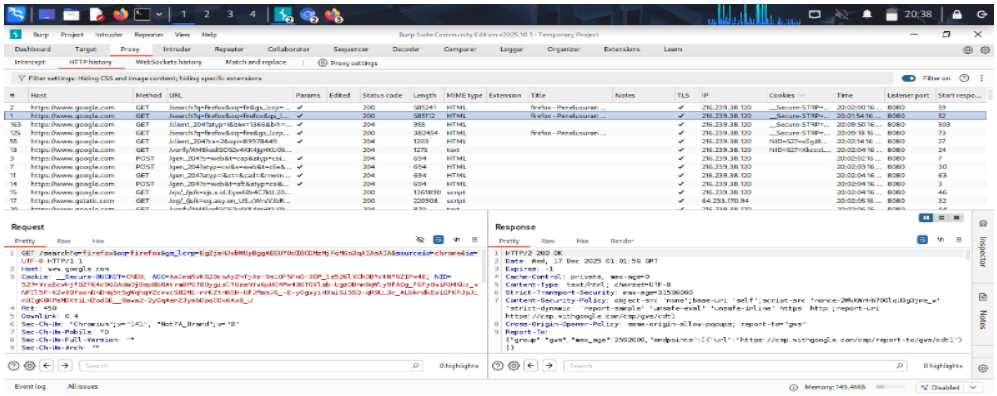
Gambar 7,menampilkan proses tahap pengujian dengan fitur Repeater, di mana request dimodifikasi dan dikirim ulang ke server untuk menguji kerentanan seperti *parameter tampering* dan *replay attack.*



Gambar 7. Proses pengujian dengan fitur Repeater

3.8.1 Modifikasi request menggunakan Repeater

Gambar 8, menunjukkan hasil akhir pengujian, di mana BurpSuite berhasil mengidentifikasi lalu lintas mencurigakan dan potensi serangan pada jaringan wireless berdasarkan analisis data yang ditangkap.



Gambar 8. Menunjukan hasil akhir pengujian,dimana Burpsuite berhasil mengidentifikasi lalu lintas yang mencurigakan dan potensi serangan pada jaringan wireless

3.9.1 Ringkasan Dari Instalasi Burpsuite untuk mengidentifikasi serangan

Tahap akhir dilakukannya analisis terhadap efektivitas BurpSuite dalam mengidentifikasi serangan pada jaringan wireless.Membuktikan bahwa Jaringan wireless sangat rentan terhadap serangan,Hasil dari pengujian yang telah dilakukan,digunakan untuk memberikan rekomendasi untuk peningkatan keamanan jaringan wireless.

4. HASIL DAN PEMBAHASAN

4.1 Hasil dari Pengujian

Dari hasil pengujian telah dilakukan terhadap jaringan wireless yang menggunakan Burpsuite pada sistem operasi Kali Linux yang dimana pengujian ini fokus pada lalu lintas data (*traffic*) yang melewati jaringan wireless,menganalisis *request* dan *response HTTP*,serta mengindentifikasinya potensi serangan yang dapat terjadi selama proses komunikasi data berlangsung.Berdasarkan tahap pengujian yang telah dilakukan,bahwa Burpsuite telah berhasil menangkap berbagai informasi penting seperti *request HTTP*, *session*, dan *cookie*,yang dikirmkan melalui jaringan wireless.Informasi ini menjadi dasar dalam mengidentifikasi potensi kerentanan pada keamanan,khususnya pada serangan-serangan yang berbasis web yang berjalan di atas jaringan wireless.

4.2 Identifikasi serangan pada jaringan wireless

Hasil pengujian menunjukan bahwa jaringan wireless memiliki tingkat kerentanan yang sangat tinggi terhadap beberapa jenis serangan,Terutama pada komunikasi data yang tidak menggunakan enkripsi

yang kuat.Sehingga Burpsuite mampu menampilkan sangat detail terhadap komunikasi client-server secara jelas,sehingga aktivitas yang mencurigakan dapat terdeteksi.Jenis-jenis serangan yang teridentifikasi antara lain serangan *session hijacking*,*parameter tampering*,dan *main-in-the-middle*.Serangan ini muncul karena lemahnya pengamanan session dan penggunaan terhadap protokol **HTTP** tanpa perlindungan tambahan.

Tabel

Tabel dibawah ini merangkum adanya tahapan dan proses dari hasil pengujian terhadap kerentanan dan serangan-serangan yang terjadi pada jaringan wireless menggunakan Burpsuite

Tabel 1. Hasil pengujian kemanan jaringan pada Burpsuite

No	Tahap Pengujian	Fitur Burpsuite	Hasil
1	Konfigurasi Proxy	Proxy Listener	Burpsuite berhasil menangkap lalu lintas pada jarinngan
2	Intercept request	Intercept Proxy	Request **HTTP**,Tertahan sebelum ke server
3	Analisis Traffic	HTTP History	Data Request dan response sudah dapat diananlisis
4	Analisis Session	Cookie Analyzer	Cookie dan session ID telah berhasil di identifikasi
5	Modifikasi request	Repeater	Request dapat dimodifikasi dan dikirim ulang ke server

Tabel 2. Hasil mengidentifikasi terhadap jenis serangan

No	Jenis Serangan	Temuan Terhadap serangan	Dampak terhadap serangan
1	Session Hijacking	Cookie session terlihat sangat jelas	Dampaknya dapat pengambil ahlian akun
2	Main-In-the-Middle	Request dapat di intercept	Dampaknya Kebocoran data yang sensitif
3	Parameter Tampering	Parameter request dapat diubah	Dampaknya dapat Memanipulasi data
4	Replay Attack	Request dapat dikirm ulang	Dampaknya penyalahgunaan transaksi data

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dari penelitian telah disimpulkannya bahwa Burpsuite terbukti sangat efektif sebagai alat bantu pengujian keamanan jaringan wireless,khususnya dalam menganalisis lalu lintas data yang melewati jaringan tersebut.Melalui fitur-fitur seperti *proxy listener*,*intercept proxy*,*HTTP History*,dan *repeater*,Burpsuite mampu menangkap,menahan,serta memodifikasi request dan response antara clien-server secara detail.Jaringan wireless juga memiliki tingkat kerentanan yang sangat tinggi,terutama ketika komunikasi data masih menggunakan protokol **HTTP** tanpa ekripsi yang kuat.Dari hasil pengujian yang telah berhasil menangkap suatu informasi sensitif seperti session ID dan cookie,yang bisa berpotensi disalahgunakan oleh pihak-pihak yang tidak berwenang.Terutama serangan-serangan yang telah diidentifikasi oleh Burpsuite seperti *session hijacking*,*main-in-the-middle*,*parameter tampering*,dan *replay attack*.Serangan-serangan ini muncul akibat lemahnya pengamanan,kurangnya validasi prameter,serta tidak adanya perlindungan tambahan pada proses komunikasi data.Maka,proses analisis menggunakan Burpsuite dapat memberikan gambaran yang jelas mengenai alur komunikasi client-server,sehingga semua aktivitas yang mencurigakan dapat terdeteksi sejak dini.Informasi dari hasil pengujian ini sangat membantu untuk melakukan evaluasi tingkat resiko keamanan pada jaringan wireless.Penelitian ini juga telah membuktikan bahwa penerapan Burpsuite sangat mendukung untuk peningkatan keamanan pada jaringan wireless,terutama sebagai alat evaluasi awal dalam penetration testing dan analisis kerentanan secara sistematis.

Dari Penelitian ini,bahwa pengelolaan jaringan wireless sangat disarankan untuk menerapkan enkripsi yang sangat kuat,seperti penggunaan protokol **HTTP** secara menyeluruh dan penerapan yang standar aagar kemanan jaringan dapat lebih aman,berguna untuk meminimalkan risiko penyadapan dan pencurian data.Dalam pengujian keamanan jaringan sebaiknya dilakukannya secara berkala,tidak hanya menggunakan Burpsuite,tetapi bisa dikombinasikan dengan tools penetration testing lainnya agar hasil evaluasi terhadap keamanan menjadi lebih komprehensif.Dan untuk pengamanan terhadap session ID dan cookie perlu ditingkatkan,dengan menerapkan mekanisme *secure cookie*,*HTPPOnly*,serta pengelolaan terhadap session yang lebih baik untuk mencegah adanya serangan session hijacking.

DAFTAR PUSTAKA

Akbar, M. H. (2024). *EVALUASI KEAMANAN JARINGAN (Wi-Fi) TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS DI PT. PELABUHAN INDONESIA (PERSERO) REGIONAL 2 TELUK BAYUR* (Doctoral dissertation, Universitas Putra Indonesia YPTK Padang).

Sistematika penulisan jurnal

Hanafi, M. A. (2024). *ANALISA KEAMANAN JARINGAN WIRELESS UNIMMA MENGGUNAKAN METODE PENETRATION TESTING* (Doctoral dissertation, Skripsi, Universitas Muhammadiyah Magelang).

Huzaini, F. T. (2024). *ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI* (Doctoral dissertation, Sekolah Tinggi Teknologi Terpadu Nurul Fikri).

IRAWAN, D. S. (2022). *PENGUJIAN KEMANAN SISTEM INFORMASI BERBASIS WEB BERDASARKAN DOKUMEN OWASP WSTG V4. 2(Studi Kasus: Sistem Informatics Expo Universitas Islam Indonesia).*

PortSwigger. (2022). *BURPSUITE DOCUMENTATION & USER GUIDE. PORTSWIGGER WEB SECURITY*

Kurniawan, R. (2021). *Analisis keamanan fasilitas jaringan (wifi) terhadap serangan packet sniffing pada protocol http dan https (Doctoral dissertation, Universitas Islam Riau).*

Rachman, R. (2021). *Analisis Keamanan Jaringan Wireless LAN (WLAN) Dengan Metode Penetration Testing Pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru (Doctoral dissertation, Universitas Islam Riau).*

Arini, A., Arsalan, M. L., & Sukmana, H. T. (2024). *Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: Pt. Akurat. Co). Cyber Security Dan Forensik Digital, 6(2), 30-38.*

Nugraha, A. D., Husaini, H., & Anwar, A. (2022). *Analisis Keamanan Data Dalam Jaringan Terhadap Kegiatan Sniffing Menggunakan Serangan Man In The Midle Attack. Jurnal Teknologi Rekayasa Informasi dan Komputer, 5(2).*

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). *Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. Techno. com, 22(2), 418-429.*