Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-10

Ananlisis Vulnerabilitas dan Pengujian Terhadap Google Gruyere

Dhia Suhaila*, Muhammad Karim Bachtiar, Tedi Kurniawan

Sekolah Vokasi, IPB University

Abstrak: Perkembangan masyarakat saat ini semakin didorong dan didukung oleh pertumbuhan teknologi komunikasi melalui pengujian keamanan dengan aplikasi web Google Gruyere. Berbagai kerentanan umum, seperti *Cross-Site Scripting* (XSS), *Client State Manipulation*, *Cross-Site Request Forgery* (CSRF), dan *Path Traversal*, diidentifikasi dan dianalisis. Metode penelitian meliputi identifikasi masalah, tinjauan pustaka, dan eksperimen dengan menggunakan alat pengujian penetrasi. Hasil penelitian menunjukkan bahwa pengujian keamanan yang komprehensif sangat penting untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam suatu sistem. Pengujian penetrasi membantu mengembangkan strategi keamanan yang lebih baik dengan mengidentifikasi kerentanan secara cepat dan akurat dan memungkinkan organisasi untuk melawan potensi ancaman keamanan sebelum dapat dieksploitasi. Menerapkan langkah-langkah keamanan yang tepat seperti sanitasi masukan, penggunaan token CSRF, dan validasi masukan dapat mengurangi risiko serangan siber dan melindungi data pengguna. Kesadaran akan ancaman dan tindakan pencegahan yang tepat sangat penting untuk meningkatkan keamanan siber aplikasi web.

Kata kunci: *Client State Manipulation, Cross-Site Request, Cross-Site Scripting, Cross-Site Scripting*, Keamanan Siber, Path Traversal, Pengujian Penetrasi.

DOI: https://doi.org/10.47134/pjise.v1i3.2574
*Correspondence: Dhia Suhaila
Email: suhailadhia@apps.ipb.ac.id

Received: 28-04-2024
Accepted: 30-05-2024
Published: 31-06-2024

Abstract: *The development of today's society is increasingly driven and supported by the growth of communication technology through security testing with Google Gruyere web applications. Various common vulnerabilities, such as Cross-Site Scripting (XSS), Client State Manipulation, Cross-Site Request Forgery (CSRF), and Path Traversal, were identified and analyzed. The research method includes problem identification, literature review, and experimentation using penetration testing tools. The results showed that comprehensive security testing is essential to maintain the integrity, confidentiality, and availability of information in a system. Penetration testing helps develop better security strategies by identifying vulnerabilities quickly and accurately and enables organizations to counter potential security threats before they can be exploited. Implementing proper security measures such as input sanitization, use of CSRF tokens, and input validation can reduce the risk of cyberattacks and protect user data. Awareness of threats and proper precautions are essential to improving web application cybersecurity.*

Keywords: *Client State Manipulation, Cross-Site Request, Cross-Site Scripting, Cross-Site Scripting, Cybersecurity, Path Traversal, Penetration testing.*

Pendahuluan

Perkembangan masyarakat saat ini semakin didorong dan didukung oleh pertumbuhan teknologi telekomunikasi. Hubungan antar bangsa yang semakin mengglobal, dan munculnya tatanan dunia baru. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia di seluruh dunia. Selain itu, dengan berkembangnya teknologi informasi, dunia menjadi tanpa batas dan perubahan sosial besar-besaran terjadi dengan cepat (Daeng *et al.*, 2023). Informasi dapat mempunyai dampak positif dan negatif. Penggunaan teknologi informasi khususnya internet menawarkan banyak peluang, namun penting juga untuk dicatat bahwa internet memungkinkan dilakukannya kejahatan yang murni bersifat sectarian seperti pencurian, penipuan, intimidasi, dan lain-lain (Ariyaningsih *et al.* 2023).

Keamanan siber pada dasarnya berkaitan erat dengan kehidupan sosial sehari-hari. Keamanan siber secara umum dipahami sebagai ancaman terhadap pelaku digital dari serangan siber juga dikenal sebagai ancaman siber terhadap teknologi digital, seperti, phishing, malware dan serangan kata sandi (Susan dan Rachman 2021). Kejahatan siber merupakan bentuk kejahatan baru yang semakin meningkat seiring dengan berkembangnya teknologi informasi. Kejahatan dunia maya melibatkan komputer dalam pelaksanaannya. Kejahatan yang berkaitan dengan privasi, integritas dan keberadaan data. Sistem TI memerlukan perhatian khusus karena memiliki karakteristik yang berbeda dengan kejahatan biasa (Ramadhani, 2023).

Keamanan siber atau pertahanan merupakan bagian dari metode atau mekanisme yang diterapkan dan digunakan untuk melindungi kerahasiaan data, integritas, ketersediaan informasi dan meminimalkan gangguan (Makbull Rizki, 2022). Keamanan siber mengacu pada alat, kebijakan, konsep keamanan dan langkah-langkah keamanan yang dapat digunakan untuk melindungi lingkungan siber organisasi dan aset penggunanya. Kumpulan Aset organisasi mencakup perangkat komputasi yang terhubung, manusia, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan keseluruhan informasi yang dikirimkan dan disimpan di dunia maya. Secara umum, tujuan keamanan siber adalah ketersediaan, integritas yang mencakup keaslian dan kepastian data dan kerahasiaan. Memahami perilaku individu dalam menghadapi ancaman siber adalah bagian dari pengelolaan keamanan siber dan memitigasi serangan tersebut. Jika pengguna tidak menerapkan perilaku aman, komputer menjadi sangat rentan terhadap serangan cyber (Khoironi, 2020).

Pada penelitian ini dilakukan tes kerentanan dan pengujian keamanan pada aplikasi web seperti Google Gruyere. Google Gruyere merupakan sebuah aplikasi web yang memungkinkan pengguna untuk menemukan bug dan mempelajari cara memperbaikinya. Sebagai alternatif, BWAPP (*Buggy Web Application*) adalah aplikasi web sumber terbuka yang dirancang sebagai alat uji penetrasi untuk menemukan dan mencegah kerentanan pada web. Setelah mengevaluasi Google Gruyere, kerentanan umum yang diidentifikasi meliputi skrip lintas situs, ketidakcocokan dalam rangkaian karakter, CSRF (*Cross-Site Request Forgery*), pengungkapan waktu dan sebagainya (Barik et al., 2021).

Selain itu, penelitian ini dilakukan untuk melakukan analisis dan pengujian keamanan untuk mengidentifikasi kerentanan keamanan dengan melakukan vulnerabilitas dan

menggunakan penetration testing. Identifikasi kerentanan sistem atau penilaian kerentanan adalah proses mengidentifikasi dan mengukur kerentanan keamanan dalam lingkungan keamanan sistem informasi. Dapat juga diartikan sebagai penilaian rinci terhadap keamanan sistem informasi yang digunakan (Sofyan *et al.* 2023). Kerentanan adalah kelemahan yang membahayakan integritas, kerahasiaan, atau ketersediaan suatu aset. Penilaian kerentanan merupakan bagian dari penilaian risiko dan terdiri dari analisis risiko, pengembangan kebijakan, pelatihan dan implementasi, penilaian kerentanan dan pengujian penetrasi (Zirwan, 2022).

Untuk meminimalisir kejahatan siber pada sistem dan jaringan komputer, perlu dilakukan simulasi serangan untuk mengukur keamanan sistem dan pengujian penetrasi. Pengujian penetrasi menyimulasikan serangan jaringan pada sistem komputer untuk mendeteksi kerentanan, ancaman, dan risiko dalam sistem, aplikasi perangkat lunak, jaringan, dan aplikasi web yang dapat dieksploitasi oleh penyerang (Ardiyasa dan Ndok 2023). Pengujian penetrasi membantu mengembangkan strategi keamanan informasi Anda dengan mengidentifikasi kerentanan secara cepat dan akurat. Hal tersebut memberikan informasi terperinci tentang ancaman keamanan dunia nyata yang dapat dieksploitasi jika dimasukkan ke dalam operasi dan proses keamanan organisasi. Oleh karena itu, memungkinkan organisasi dengan cepat dan akurat mengidentifikasi potensi kerentanan di dunia nyata (Hasibuan dan Elhanafi 2022).

Metode

Metode penelitian mengidentifikasi seluruh tahapan yang terlibat dalam pembuatan suatu struktur kerja atau disebut dengan kerangka kerja. Kerangka kerja digunakan untuk membuat tahapan-tahapan yang harus diselesaikan dalam suatu penelitian, dan tahapan-tahapan tersebut mempengaruhi setiap tahapan dalam mencapai tujuan penelitian. Setelah penelitian dilakukan, maka peneliti akan mengobservasi hasil dari penelitian yang kemudian hasil penelitian akan dianalisis.

Penelitian literatur kerentanan mengacu pada proses memahami dan mengumpulkan informasi dari berbagai sumber dokumen seperti artikel, buku dan laporan penelitian yang terkait kerentanan keamanan pada sistem, aplikasi atau situs web. Dalam konteks keamanan siber, vulnerabilitas adalah langkah mendeteksi, mengidentifikasi dan menyelidiki kerentanan dalam suatu sistem atau infrastruktur jaringan komputer (Sirait et al., 2018).

Peneliti melakukan eksperimen pada *website* menggunakan *pentesting tools. Pentesting tools* merupakan identifikasi kerentanan keamanan dalam kondisi terkendali untuk memprediksi kerentanan sebelum pengguna tidak sah dapat mengeksploitasi sistem organisasi. Pakar sistem penetrasi menggunakan pengujian penetrasi untuk mengatasi masalah terkait penilaian kerentanan dengan fokus pada kerentanan dengan tingkat keparahan tinggi. Pengujian penetrasi dianggap sebagai bagian dari proses manajemen risiko keamanan TI dan dilakukan karena persyaratan internal atau eksternal, bergantung pada situasinya (Hasibuan dan Elhanafi 2022).

Beberapa tes dilakukan seperti *cross site scripting* yang merupakan jenis kerentanan yang terjadi di web dinamis. Hal ini disebabkan karena web yang dibuat tidak dapat memfilter masukan yang dikirim oleh penyerang, sehingga memudahkan penyerang untuk

menyuntikkan kode berbahaya ke dalam web dalam bentuk Javascript atau menggunakannya sebagai akses sah ke suatu situs web dengan tujuan mendapatkan *cookie* dan sesi (Putra *et al.* 2021). Serangan *Cross-Site Scripting* sangat mudah dieksploitasi, karena ada banyak alat gratis yang memungkinkan bahkan orang dengan sedikit pengetahuan peretasan dapat menyerang aplikasi web dengan mudah. XSS adalah jenis serangan injeksi di mana penyerang menyuntikkan skrip berbahaya ke dalam aplikasi web yang rentan. Serangan XSS yang berhasil mengakibatkan pembajakan sesi, penyebaran data sensitif, CSR dan pencurian identitas korban (Stefanus Eko Prasetyo, Haeruddin 2024).

Kemudian dilakukan tes *client state manipulation* yang merupakan jenis serangan lain yang dapat terjadi karena masukan yang tidak divalidasi. Dalam aplikasi web, klien web (atau browser) mengirimkan permintaan ke server web untuk mengakses halaman web. Server web sering kali memanggil program tambahan untuk membantu membuat halaman Web yang dikirimkan ke klien. Secara kolektif, program tambahan ini disebut sebagai aplikasi web. Aplikasi web sering kali menerima masukan dari pengguna. Untuk menjamin keamanan, aplikasi web tidak boleh mempercayai klien dan harus memvalidasi semua masukan yang diterima dari klien (Foundations of Security, 2007).

Selain itu dilakukan *cross site request forgery*. CSRF adalah Serangan terhadap situs web yang berjalan di bawah otoritas korban. Serangan CSRF menyebabkan browser korban yang masuk mengirimkan permintaan HTTP yang berisi cookie sesi dan kredensial ke aplikasi web yang rentan. Skrip lintas situs dianggap sebagai salah satu jenis serangan paling kuat terhadap aplikasi web. Serangan ini terjadi karena input pengguna/klien yang tidak divalidasi. Situs web yang menyimpan cookie memungkinkan pengguna untuk kembali tanpa memasukkan nama pengguna dan kata sandi mereka, sehingga menarik perhatian penyerang yang mungkin ingin menjelajahi lebih banyak fitur situs setelah masuk (Mahdi Maulana Lubis *et al.* 2022).

Dilakukan juga tes dengan melakukan *cross-site script inclusion* (XSSI) adalah jenis serangan di mana file skrip JavaScript dari domain pihak ketiga disuntikkan ke halaman web pengguna. Dalam skenario XSSI, penyerang mengeksploitasi fakta bahwa situs web memuat file skrip dari domain pihak ketiga tanpa memvalidasi atau memfilternya dengan benar. Hal ini dapat terjadi karena situs web Anda bergantung pada sumber daya dari domain pihak ketiga, seperti pustaka atau plugin JavaScript, untuk fungsionalitas tambahan (Mahdi Maulana Lubis *et al.* 2022).

Kemudian path traversal yang memungkinkan peretas mengakses file, direktori, dan perintah di luar direktori root dokumen web. Penyerang dapat memanipulasi URL yang dapat menyebabkan situs web dijalankan atau mengekspos konten file sembarangan di server web (Ita Sopia Fazriani *et al.* 2019). Model traversal adalah mesin terbatas untuk merepresentasikan status (tampilan) antarmuka dan proses transisi di antara keduanya (Tang *et al.*, 2019).

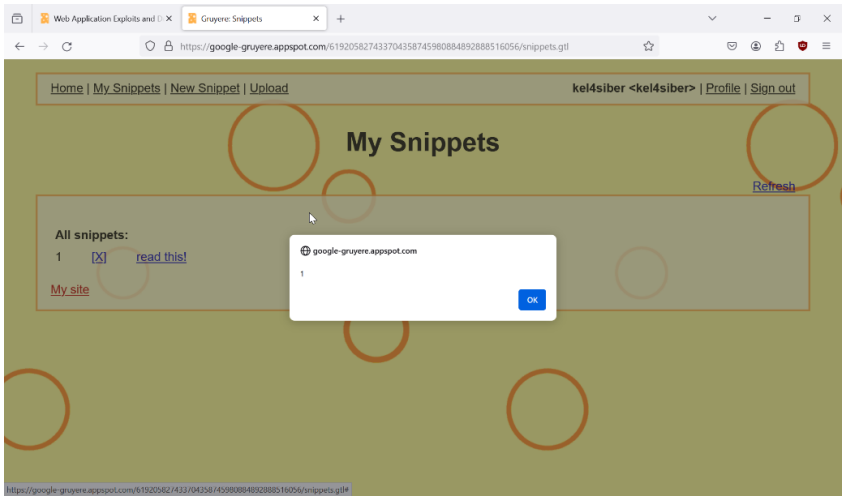
Terakhir yaitu *denial of service* yang merupakan jenis serangan cyber yang membuat infrastruktur atau layanan yang tersedia bagi pengguna yang sah tidak dapat diakses atau tidak tersedia. Varian DoS yang lebih canggih, serangan penolakan layanan terdistribusi (DDoS), menggunakan beberapa perangkat yang terinfeksi malware secara bersamaan untuk melakukan serangan. Serangan DDoS tidak hanya melibatkan satu orang atau perangkat, namun jaringan banyak bot dan komputer yang terinfeksi yang disebut botnet

dan bekerja sama untuk meluncurkan serangan terkoordinasi terhadap suatu target (Ezenwe *et al.* 2020). Serangan DoS dapat dicegah dengan memindai lalu lintas jaringan masuk dan keluar untuk mencari ancaman keamanan. Ketika IPS mendeteksi serangan, ia mencegat atau menolak paket data berbahaya, mencegahnya mencapai tujuannya (Alhafiz *et al.* 2023).

Hasil dan Pembahasan

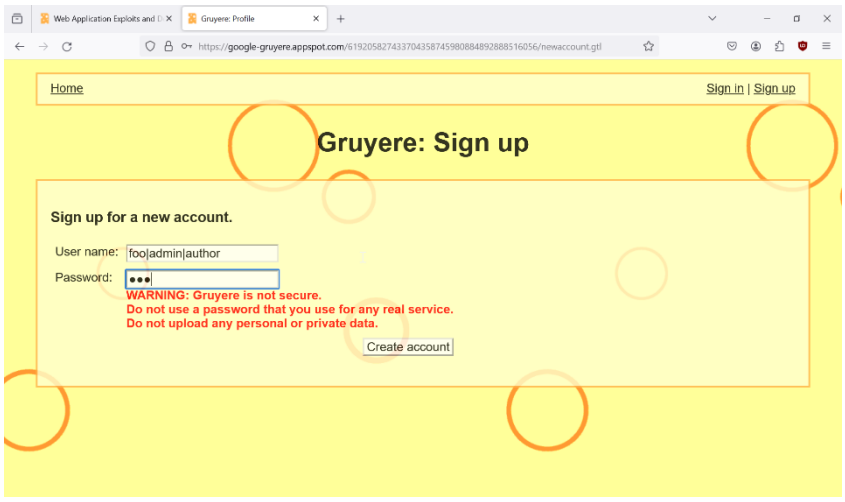
Untuk melaksanakan tes kerentanan dan pengujian keamanan pada aplikasi web seperti Google Gruyere, dilaksanakan langkah-langkah seperti, jalankan instance Google Gruyere, buka source code Google Gruyere, identifikasi celah dalam kode dan lakukan pengetesan terhadap aplikasi web

Google Gruyere menyediakan lingkungan yang aman untuk menguji jenis serangan XSS. Beberapa browser memiliki perlindungan bawaan terhadap serangan XSS. Selain itu terdapat ekstensi browser seperti NoScript yang memberikan perlindungan. Pertama dapat dilakukan login pada Google Gruyere. Setelah itu, unggah file HTML dengan isi skrip dokumen.cookie. Gruyere secara otomatis menyertakan header HTTP X-XSS-Protection: 0 di setiap respons yang dikenali oleh IE dan akan dikenali oleh versi Chrome mendatang. Serangan XSS adalah salah satu jenis serangan paling umum dalam pengembangan web. Serangan XSS biasanya terjadi di sisi klien, penyerang telah mengeksploitasi kerentanan di browser klient. Serangan XSS dapat terjadi ketika browser tidak memiliki mekanisme keamanan yang cukup kuat untuk mencegah berjalannya skrip berbahaya seperti gambar di bawah.



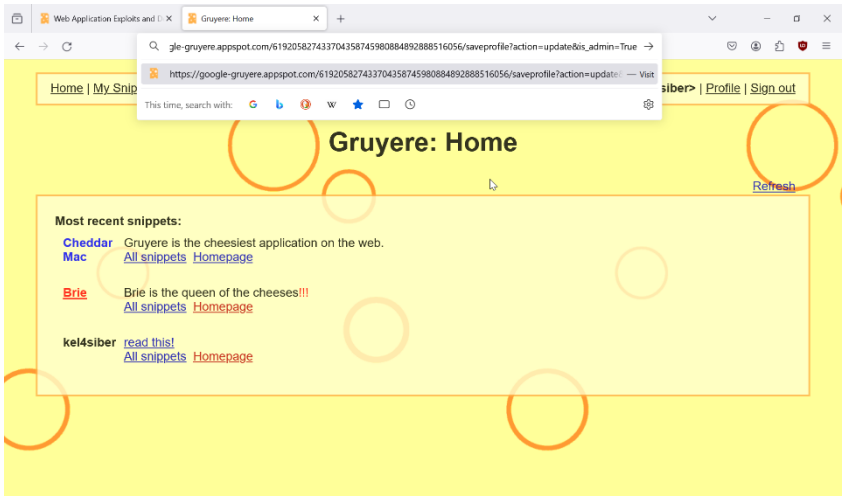
Gambar 1. Serangan XSS pada google gruyere

Setelah dilakukan serangan XSS, kemudian dilakukan serangan *Client-Statement Manipulation*. Ketika pengguna mengklik tombol atau mengirimkan formulir, browser mengirimkan permintaan kembali ke server web. Tujuannya adalah untuk menemukan cara melakukan tindakan modifikasi akun atas nama pengguna Gruyere yang login tanpa sepengetahuan pengguna. Misalkan pengguna ingin mengunjungi situs web yang dikelolanya seperti gambar di bawah.



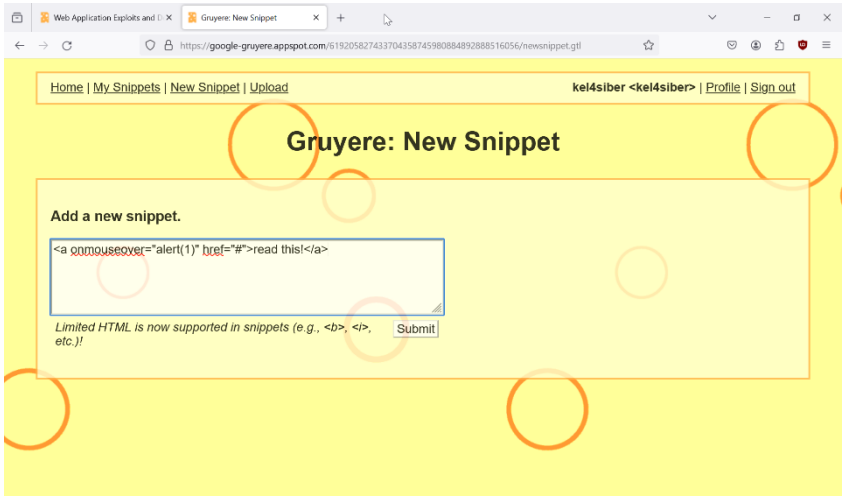
Gambar 2. Situs web yang dikelola

Aplikasi tidak boleh mempercayai data yang dikirim oleh browser karena browser berjalan di komputer yang mungkin dikendalikan oleh penyerang. Gruyere menggunakan cookie untuk menyimpan identitas pengguna yang login. Gruyere melindungi cookie dari manipulasi dengan menambahkan hash ke dalamnya. Meskipun hash tidak memberikan perlindungan yang memadai, hash tersebut tidak perlu dideskripsi untuk melakukan serangan. Gambar di bawah merupakan serangan *client state manipulation* pada google gruyere.



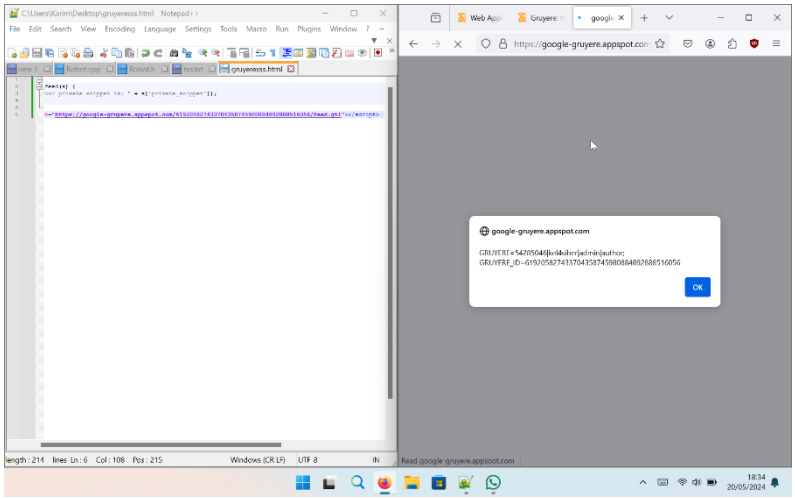
Gambar 3. Serangan client state manipulation

Setelah permintaan diproses, Gruyere harus membuat ulang token dan membandingkannya dengan nilai yang diberikan dalam permintaan. Jika nilainya sama, harus diambil tindakan dan kalau tidak harus ditolak. Dalam serangan CSRF, penyerang memanfaatkan otentikasi yang sudah ada dari pengguna untuk memaksa mereka melakukan tindakan yang tidak dikehendaki, seperti mengirimkan permintaan palsu ke server yang memuat perintah untuk melakukan tindakan tertentu seperti gambar di bawah.



Gambar 4. Serangan CSRF pada google gruyere

Browser mencegah halaman dari satu domain membaca halaman dari domain lain. Namun, hal ini tidak mencegah halaman di satu domain menunjuk ke sumber daya di domain lain. Antara lain, ini memungkinkan rendering gambar dari domain lain dan menjalankan skrip dari domain lain. Skrip yang disertakan tidak memiliki konteks keamanannya sendiri. Oleh karena itu, skrip ini "membocorkan" semua data pengguna seperti gambar di bawah.

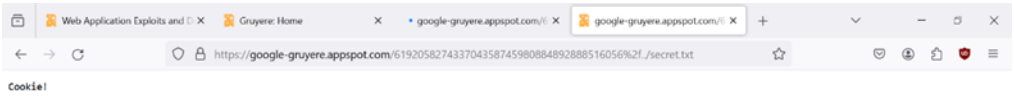


Gambar 5. Serangan XSSI

Ketika file skrip dari domain pihak ketiga disisipkan ke dalam halaman web, penyerang dapat memanfaatkannya untuk memasukkan kode berbahaya atau mengeksekusi serangan XSSI lainnya. Ini dapat mengarah pada eksekusi skrip berbahaya di browser pengguna, yang dapat menyebabkan pencurian data sensitif, pengalihan pengguna ke situs palsu, atau bahkan pengambilalihan akun.

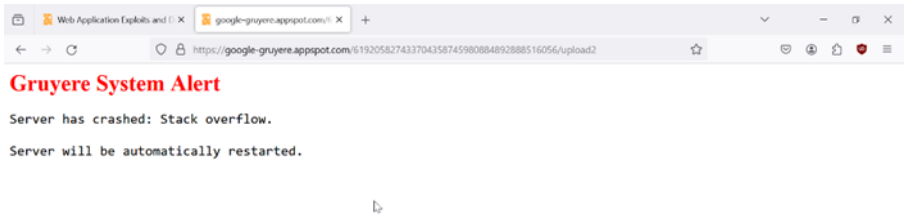
Sebagian besar aplikasi web menyediakan sumber daya statis seperti gambar dan file CSS. Aplikasi seringkali hanya menampilkan semua file dalam satu folder. Serangan *directory traversal*, memungkinkan hacker untuk mengakses file, direktori, dan perintah di luar direktori root dokumen web yang ditentukan. Hal ini terjadi ketika aplikasi web tidak

memvalidasi input pengguna dengan benar, sehingga penyerang bisa menyertakan urutan seperti \../ dalam permintaan URL mereka seperti gambar di bawah.



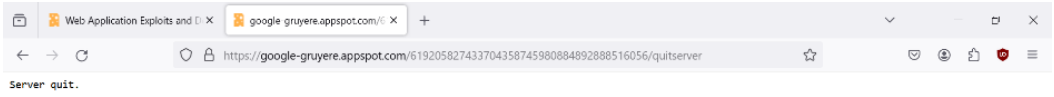
Gambar 6. Serangan directory traversal

Selanjutnya Bentuk umum serangan DoS adalah mengirimkan lebih banyak permintaan ke server daripada yang dapat ditanganinya. Server menghabiskan seluruh waktunya untuk memproses permintaan penyerang dan sangat sedikit waktu untuk memproses permintaan yang sah. Dan serangan apa pun terhadap gruyere akan ditafsirkan sebagai serangan terhadap *app engine* seperti gambar di bawah.



Gambar 7. Serangan terhadap app engine

Serangan DDoS tidak hanya melibatkan satu orang atau perangkat, namun jaringan banyak bot dan komputer yang terinfeksi (disebut botnet) yang bekerja sama untuk meluncurkan serangan terkoordinasi terhadap suatu target. Peretas juga dapat mengeksploitasi kesalahan server untuk mencegah server memproses permintaan, seperti mengirimkan permintaan yang menyebabkan server mogok, kehabisan memori, atau tidak dapat memproses permintaan yang sah seperti gambar di bawah.



Gambar 8. Serangan DDoS

Simpulan

Penelitian ini membahas pentingnya keamanan siber dalam melindungi data dan informasi di era digital. Melalui pengujian keamanan pada aplikasi web seperti Google Gruyere dan BWAPP, penelitian ini mengidentifikasi berbagai kerentanan umum, termasuk *Cross-Site Scripting* (XSS), *Client State Manipulation*, *Cross-Site Request Forgery* (CSRF), dan *Path Traversal*. Penelitian ini menunjukkan bahwa memahami dan mengelola kerentanan ini sangat penting untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam suatu sistem.

Metode yang digunakan dalam penelitian ini melibatkan identifikasi masalah, studi literatur, dan eksperimen menggunakan alat pengujian penetrasi. Tahapan ini membantu dalam memahami celah keamanan yang ada dan bagaimana cara memperbaikinya. Pengujian penetrasi membantu mengembangkan strategi keamanan yang lebih baik dengan mengidentifikasi kerentanan secara cepat dan akurat, sehingga memungkinkan organisasi untuk mengatasi potensi ancaman keamanan sebelum dieksploitasi oleh pihak yang tidak berwenang.

Hasil penelitian menunjukkan bahwa pengujian keamanan yang komprehensif sangat penting dalam melindungi aplikasi web dari berbagai serangan siber. Dengan mengimplementasikan langkah-langkah keamanan yang tepat seperti sanitasi input, penggunaan token CSRF, dan validasi input, pengembang dapat mengurangi risiko serangan dan melindungi data pengguna dari potensi eksploitasi. Kesadaran akan bahaya dan langkah-langkah pencegahan yang sesuai sangat penting untuk meningkatkan keamanan siber dalam aplikasi web.

Daftar Pustaka

Alhafiz MJ, Fauzi A, Dwiansyah A, Indriani BR, Putra FMA, Ridwani RR. (2023). Dampak Denial of Service pada Perusahaan Perbankan di Indonesia. J. Ilmu Multidisiplin. 2(1):114–120.

Ardiyasa IW, Ndok AT. (2023). Penetration Testing Keamanan Sistem Informasi Berbasis Web dengan Metode OSSTMM. Semin. Nas. Corisindo.:348–353.

Ariyaningsih S, Andrianto AA, Kusuma A surya, Rezi. (2023). Korelasi Kejahatan Siber Dengan PercepatanDigitalisasi Di Indonesia. J. Ilmu Huk. Univ. Pas. 1:1–12.

Barik K, Abirami A, Das S, Konar K, Banerjee A. (2021). Penetration Testing Analysis with Standardized Report Generation. Proc. 3rd Int. Conf. Integr. Intell. Comput. Commun. Secur. (ICIIC 2021). 4(Iciic):365–372.doi:10.2991/ahis.k.210913.045.

Daeng Y, Levin J, Razzaq Prayudha M, Putri Ramadhani N, Imanuel S, Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng A. (2023). Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia. J. Soc. Sci. Res. 3(6):1135–1145.

Ezenwe A, Furey E, Curran K. (2020). Mitigating denial of service attacks with load balancing. J. Robot. Control. 1(4):129–135.doi:10.18196/jrc.1427.

Hasibuan M, Elhanafi AM. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. sudo J. Tek. Inform. 1(4):171–177.doi:10.56211/sudo.v1i4.160.

In: Foundations of Security. (2007). Client-State Manipulation. Apress.

Ita Sopia Fazriani N, Cut B, Sanusi. (2019). Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga. Kandidat. 1(1):15–20.

Khoironi SC. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. J. Stud. Komun. dan Media. 24(1):37.doi:10.31445/jskm.2020.2945.

Mahdi Maulana Lubis M, Handoko D, Wulan N. (2022). Analisis Implementasi Laravel 9 Pada Website E-Book Dalam Mengatasi N+1 Problem Serta Penyerangan Csrf dan Xss. Januari. 2023(2):173–187.

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. Polit. J. Ilmu Polit. 14(1):54–62.doi:10.32734/politeia.v14i1.6351.

Putra Y, Yuhandri Y, Sumijan S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. J. Sistim Inf. dan Teknol. 3:56–63.doi:10.37034/jsisfotek.v3i2.44.

Ramadhani F. (2023). Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber. Kult. J. Ilmu Hukum, Sos. dan Hum. 1(1):89–97.

Sirait F, Sofyan M, Putra K. (2018). Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. Januari. 9(1):16.

Sofyan H, Sugiarto M, Akbar BM. (2023). Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN "Veteran" Yogyakarta. J. Inform. dan Teknol. Inf. 20(2):153–162.doi:10.31515/telematika.v20i2.7757.

Stefanus Eko Prasetyo, Haeruddin KA. (2024). SISTEM KEAMANAN WEBSITE DARI SERANGANDENIAL OF SERVICE,SQLINJECTION,CROSS SITE SCRIPTING MENGGUNAKANWEB APPLICATION FIREWALL. Sist. KEAMANAN WEBSITE DARI SERANGANDENIAL Serv. SITE SCRIPTING MENGGUNAKANWEB Appl. FIREWALL. 2(6):42–46.

Susan N, Rachman MF. (2021). Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber. J. Indones. Maju. 1(1):1–11.

Tang J, Li J, Li R, Han H, Gu X, Xu Z. (2019). SSLDetecter: Detecting SSL Security Vulnerabilities of Android Applications Based on a Novel Automatic Traversal Method. Secur. Commun. Networks. 2019.doi:10.1155/2019/7193684.

Zirwan A. (2022). Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner. J. Inf. dan Teknol. 4(1):70–75.doi:10.37034/jidt.v4i1.190.