EXPLORE
Jurnal Sistem Informasi dan Telematika
(Telekomunikasi, Multimedia dan Informatika)

Analisis Keamanan Website Sekolah Dasar Terhadap XSS dan Brute Force

Anastasia Angela, Desak Made Candra Pratiwi, Luh Putu Dian Satriani, I Made Edy Listartha
Jurusan Teknik Informatika, Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Singaraja, Indonesia
anastasia@student.undiksha.ac.id*, desak.candra@students.undiksha.ac.id, dian.satriani@student.undiksha.ac.id
listartha@undiksha.ac.id

Abstract- The advancement of information technology has increased the use of websites in the education sector, including at the elementary school level, which indirectly raises cybersecurity risks. Vulnerabilities such as *Cross-Site Scripting* (*XSS*) and *brute force* attacks may lead to data leakage, unauthorized access, and system manipulation. This study aims to assess the security level of an elementary school website by identifying existing vulnerabilities and analyzing their impacts. The method used is *penetration testing* with a *black box* approach based on the OWASP Top 10, carried out through the stages of *reconnaissance*, *vulnerability assessment*, *exploitation*, and *post-exploitation*. The testing process employed tools such as Burp Suite and Hydra. The results show that the system is vulnerable to *XSS* attacks, both *reflected* and *stored*, due to inadequate input validation and sanitization. In addition, the system has weaknesses in its authentication mechanism, making it vulnerable to *brute force* attacks due to the absence of security features such as *rate limiting* and *account lockout*. These vulnerabilities may lead to *session hijacking*, *account enumeration*, and unauthorized system access. The contribution of this study is to extend web security research in the educational context to elementary school websites, which have been relatively less discussed in previous studies, and to show that the combination of *XSS* and *brute force* vulnerabilities in small-scale websites can create potential layered attack risks when input validation and authentication mechanisms are inadequate. Based on these findings, it can be concluded that the website security level remains suboptimal and requires improvements in input validation, authentication mechanisms, and the implementation of additional security controls to strengthen system resilience.

Keywords: Website Security, Penetration Testing, Cross Site Scripting, Brute Force, Elementary School Website

Abstrak- Perkembangan teknologi informasi telah mendorong peningkatan penggunaan website dalam sektor pendidikan, termasuk pada tingkat sekolah dasar, yang secara tidak langsung juga meningkatkan risiko keamanan siber. Kerentanan seperti *Cross-Site Scripting* (*XSS*) dan serangan *brute force* berpotensi menyebabkan kebocoran data, akses tidak sah, serta manipulasi sistem. Penelitian ini bertujuan untuk menilai tingkat keamanan sebuah website sekolah dasar dengan mengidentifikasi kerentanan yang ada serta menganalisis dampaknya. Metode yang digunakan adalah *penetration testing* dengan pendekatan *black box* yang mengacu pada OWASP Top 10, melalui tahapan *reconnaissance*, *vulnerability assessment*, *exploitation*, dan *post-exploitation*. Proses pengujian dilakukan menggunakan *tools* seperti Burp Suite dan Hydra. Hasil penelitian menunjukkan bahwa sistem rentan terhadap serangan *XSS*, baik *reflected* maupun *stored*, yang disebabkan oleh kurangnya validasi dan sanitasi input. Selain itu, sistem juga memiliki kelemahan pada mekanisme autentikasi sehingga rentan terhadap serangan *brute force* akibat tidak adanya fitur keamanan seperti *rate limiting* dan *account lockout*. Kerentanan tersebut dapat menyebabkan *session hijacking*, *account enumeration*, serta akses tidak sah ke dalam sistem. Kontribusi penelitian ini adalah memperluas kajian keamanan website pendidikan ke konteks sekolah dasar yang masih relatif jarang dibahas pada penelitian terdahulu, serta menunjukkan bahwa kombinasi kerentanan *XSS* dan *brute force* pada website berskala kecil dapat membentuk potensi risiko serangan berlapis apabila tidak didukung validasi input dan mekanisme autentikasi yang memadai. Berdasarkan hasil tersebut, dapat disimpulkan bahwa tingkat keamanan website masih belum optimal dan memerlukan peningkatan pada validasi input, penguatan mekanisme autentikasi, serta penerapan kontrol keamanan tambahan untuk meningkatkan ketahanan sistem.

Kata Kunci: Keamanan Website, Penetration Testing, Cross Site Scripting, Brute Force, Website Sekolah Dasar

1. Pendahuluan

Pemanfaatan website dalam berbagai sektor, khususnya pendidikan, semakin meningkat seiring dengan pesatnya perkembangan teknologi informasi. Website kini tidak hanya digunakan sebagai sarana penyampaian

informasi, tetapi juga berperan dalam pengelolaan data pengguna. Di sisi lain, intensitas penggunaan tersebut turut diikuti oleh meningkatnya risiko keamanan siber yang memanfaatkan celah pada sistem. Serangan seperti *Cross-Site Scripting* (XSS) dan *brute force* menjadi ancaman yang signifikan karena berpotensi menimbulkan kebocoran data, manipulasi sistem, serta akses tidak sah ke dalam sistem [1]. Ancaman ini juga berkaitan dengan meningkatnya praktik *cybercrime* [2], serta meningkatnya berbagai bentuk *cyber attack* pada sistem berbasis web [3].

Penelitian sebelumnya menunjukkan bahwa kerentanan keamanan web umumnya disebabkan oleh lemahnya pengolahan input pengguna. Studi oleh [4] menemukan bahwa seluruh plugin WordPress yang diuji memiliki kerentanan XSS, dengan dominasi *stored XSS* sebesar 92,5%, yang menunjukkan rendahnya penerapan validasi, sanitasi, dan *encoding* input pada sistem. Selain itu, penelitian lain yang dilakukan oleh [5] menunjukkan bahwa meskipun tidak semua eksploitasi berhasil mendapatkan akses langsung, kerentanan seperti *reflected XSS* tetap dapat dimanfaatkan untuk serangan lanjutan seperti *phishing* dan pencurian data. Temuan ini menunjukkan bahwa kerentanan tidak selalu bergantung pada keberhasilan eksploitasi penuh, tetapi juga pada potensi dampak yang ditimbulkan.

Meskipun berbagai penelitian telah dilakukan, terdapat keterbatasan pada konteks objek penelitian yang sebagian besar berfokus pada sistem berskala besar seperti website kampus, CMS WordPress, atau sistem informasi akademik. Penelitian-penelitian tersebut umumnya dilakukan pada sistem dengan struktur keamanan yang relatif lebih kompleks dan pengelolaan yang lebih baik. Hal ini menimbulkan kesenjangan *(gap)* penelitian, yaitu belum banyaknya kajian yang secara spesifik mengevaluasi keamanan website pada lingkungan pendidikan dasar, seperti sekolah dasar, yang umumnya memiliki keterbatasan dalam penerapan kontrol keamanan, sumber daya, serta minimnya evaluasi keamanan secara berkala.

Berbeda dengan penelitian sebelumnya yang membahas website SMA menggunakan OWASP [6], website SMP dengan pengujian *rate limiting* [7], aplikasi pendidikan berbasis WordPress terhadap *SQL Injection* [8] serta plugin WordPress terhadap *XSS* [4], penelitian ini berfokus pada website sekolah dasar yang belum banyak dibahas dalam kajian keamanan website pendidikan. Website sekolah dasar dipilih karena meskipun memiliki kompleksitas rendah, sistem ini tetap memiliki titik input pengguna dan mekanisme autentikasi yang berpotensi menjadi celah keamanan. Kebaruan penelitian ini terletak pada perluasan konteks kajian keamanan website pendidikan ke tingkat sekolah dasar serta analisis kombinasi kerentanan *XSS* dan *brute force* sebagai potensi risiko keamanan berlapis pada website berskala kecil. Untuk menjawab kesenjangan tersebut, penelitian ini menggunakan pendekatan *penetration testing* berbasis OWASP Top 10 dengan teknik *black box*.

Selain itu, penelitian ini tidak hanya mengidentifikasi kerentanan, tetapi juga menganalisis keterkaitan antar kerentanan seperti XSS dan *brute force* yang berpotensi membentuk serangan berlapis *(multi-stage attack)*. Pendekatan sistem juga perlu mempertimbangkan aspek *user-centered* [9], serta pentingnya efisiensi dan pengelolaan sistem TI yang baik untuk mengurangi risiko kesalahan konfigurasi dan kelemahan sistem [10].

Penelitian ini difokuskan pada pengungkapan kerentanan keamanan pada website sekolah dasar, khususnya yang berkaitan dengan serangan XSS dan *brute force*, sekaligus menilai dampak yang ditimbulkan terhadap kinerja dan keamanan sistem. Hasil penelitian diharapkan dapat memberikan rekomendasi perbaikan serta meningkatkan kesadaran akan pentingnya keamanan sistem, terutama pada website dengan skala kecil yang selama ini kurang mendapat perhatian.

2. Landasan Teori

A. Penelitian Terdahulu

Beberapa penelitian sebelumnya telah membahas pengujian keamanan website pendidikan menggunakan OWASP dan penetration testing. [6] menganalisis kerentanan website SMA Negeri 2 Amlapura menggunakan OWASP Risk Rating dan menemukan adanya kategori risiko High, Medium, dan Low yang dapat membantu pengelola sistem menentukan prioritas mitigasi keamanan.

[7] melakukan pengujian pada website SMP Negeri 3 Semarapura dengan fokus pada *rate limiting* dan XSS menggunakan OWASP ZAP. Penelitian tersebut menunjukkan pentingnya pengujian terhadap halaman login dan input pengguna untuk mengetahui ada tidaknya pembatasan akses berulang serta potensi eksekusi payload berbahaya.

[11] meneliti keamanan website SMA Greenschool menggunakan metode OWASP dengan pengujian XSS. Penelitian tersebut menjelaskan bahwa XSS dapat digunakan untuk menyisipkan skrip berbahaya yang berpotensi mencuri data penting atau mengganggu keamanan pengguna apabila validasi input tidak diterapkan dengan baik.

Pada sisi autentikasi, [12] melakukan pengujian brute force pada web server sistem informasi akademik menggunakan penetration testing. Hasil penelitian menunjukkan bahwa kelemahan autentikasi dapat dimanfaatkan untuk memperoleh username dan password, sehingga sistem berpotensi diambil alih oleh penyusup.

[4] menganalisis keamanan plugin WordPress terhadap XSS dan menemukan bahwa lemahnya validasi, sanitasi, dan *encoding* input menjadi penyebab utama kerentanan XSS. [5] melakukan *penetration testing* pada sistem informasi website kampus dengan pengujian XSS dan *brute force*, serta menunjukkan bahwa XSS tetap berpotensi dimanfaatkan untuk *phishing* atau pencurian data meskipun akses langsung ke sistem tidak berhasil diperoleh.

Berdasarkan penelitian terdahulu tersebut, dapat disimpulkan bahwa pengujian keamanan website pendidikan telah banyak dilakukan. Namun, sebagian besar penelitian masih berfokus pada sistem pendidikan

EXPLORE: ISSN: 2087-2062, Online ISSN: 2686-181X / DOI: http://dx.doi.org/10.36448/jsit.v17i1.4871

tingkat menengah, perguruan tinggi, CMS, atau platform tertentu, sedangkan kajian yang secara khusus membahas keamanan website sekolah dasar masih relatif terbatas. Padahal, website sekolah dasar juga memiliki urgensi untuk diuji karena berperan sebagai media informasi publik dan berpotensi memuat data pengguna yang perlu dilindungi. Penelitian ini memberikan kontribusi dengan menganalisis keamanan website sekolah dasar menggunakan pendekatan *black box penetration testing* serta menguji dua kerentanan utama, yaitu XSS dan *brute force*. Selain mengidentifikasi celah keamanan, penelitian ini juga membahas potensi dampak lanjutan seperti *session hijacking*, *account enumeration*, dan akses tidak sah. Dengan demikian, penelitian ini diharapkan dapat memperkaya kajian keamanan website pada sektor pendidikan dasar sekaligus menjadi masukan praktis bagi pengelola website sekolah dalam meningkatkan validasi input, pengamanan autentikasi, dan mitigasi risiko serangan siber.

B. Keamanan Website

Keamanan website merupakan aspek penting dalam sistem berbasis web yang bertujuan untuk melindungi data dan informasi dari akses tidak sah, penyalahgunaan, serta berbagai ancaman siber. Pesatnya perkembangan teknologi informasi mendorong penggunaan website tidak hanya sebagai media informasi, tetapi juga sebagai sarana pengolahan dan penyimpanan data, yang turut meningkatkan risiko terhadap ancaman keamanan [6].

Kerentanan pada website umumnya disebabkan oleh kelemahan dalam proses pengembangan sistem, seperti kesalahan penulisan kode program (*coding error*) dan kesalahan konfigurasi (*misconfiguration*). Kondisi ini dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengeksploitasi celah keamanan dan memperoleh akses ke dalam sistem [6]. Selain itu, dalam praktiknya tidak ada sistem yang sepenuhnya aman karena selalu terdapat kemungkinan adanya celah yang dapat dimanfaatkan oleh penyerang [13].

Di lingkungan pendidikan, risiko keamanan website cenderung lebih tinggi karena tingkat kesadaran terhadap keamanan digital masih relatif rendah. Hal ini menyebabkan sistem yang digunakan rentan terhadap berbagai ancaman siber akibat kurangnya pemahaman dalam pengelolaan keamanan informasi [8].

Selain faktor tersebut, lemahnya mekanisme pengelolaan input dan kontrol akses pada sistem juga menjadi penyebab utama munculnya kerentanan pada website. Kondisi ini menunjukkan bahwa penerapan keamanan tidak hanya bergantung pada teknologi, tetapi juga pada proses pengelolaan dan kesadaran pengguna dalam menjaga keamanan sistem [14].

Dengan demikian, keamanan website perlu menjadi perhatian utama dalam pengembangan sistem guna meminimalkan risiko kerentanan serta melindungi data dan informasi yang dikelola.

C. OWASP Top 10

OWASP Top 10 merupakan standar yang dikembangkan oleh komunitas *Open Web Application Security Project* (OWASP) sebagai acuan dalam mengidentifikasi sepuluh risiko keamanan paling kritis pada aplikasi web. OWASP berfungsi sebagai pedoman bagi pengembang dan praktisi keamanan untuk memahami serta mencegah kerentanan yang dapat membahayakan sistem [7]. Sepuluh risiko tersebut meliputi *Broken Access Control*, *Cryptographic Failures*, *Injection*, *Insecure Design*, *Security Misconfiguration*, *Vulnerable and Outdated Components*, *Identification and Authentication Failures*, *Software and Data Integrity Failures*, *Security Logging and Monitoring Failures*, serta *Server-Side Request Forgery*, yang digunakan sebagai dasar dalam proses pengujian keamanan dan *penetration testing* [15].

D. Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) merupakan salah satu jenis serangan keamanan pada aplikasi web yang termasuk dalam kategori *code injection attack*, di mana penyerang menyisipkan kode berbahaya, umumnya berupa *JavaScript*, ke dalam halaman web yang kemudian dijalankan di sisi klien (browser pengguna) [11]. Serangan ini memanfaatkan kelemahan dalam pengolahan input pada aplikasi web sehingga memungkinkan penyerang mencuri data sensitif, mengendalikan sesi pengguna, atau menjalankan kode berbahaya tanpa disadari oleh pengguna [16].

Serangan XSS umumnya terjadi akibat kegagalan sistem dalam memfilter dan membersihkan input pengguna, yang memungkinkan kode berbahaya dieksekusi saat data tersebut ditampilkan kembali pada halaman web. Hal ini menyebabkan browser mengeksekusi skrip tersebut seolah-olah berasal dari website yang sah, sehingga meningkatkan risiko pencurian data dan manipulasi sistem [16].

Berdasarkan mekanisme serangannya, XSS dibagi menjadi tiga jenis utama, yaitu *reflected XSS*, *stored (persistent) XSS*, dan *DOM-based XSS*.

1. Reflected XSS

   Reflected XSS merupakan jenis XSS yang paling umum terjadi dan relatif mudah dilakukan oleh penyerang. Pada serangan ini, kode berbahaya dikirim melalui input seperti URL atau form, kemudian langsung ditampilkan kembali oleh server tanpa disimpan dalam database. Serangan ini biasanya memanfaatkan teknik *social engineering*, seperti mengirimkan tautan berbahaya kepada korban. Ketika korban mengklik tautan tersebut, skrip akan dijalankan di browser dan dapat digunakan untuk mencuri cookie atau melakukan *session hijacking* [11].

2. Stored (Persistent) XSS

   Stored XSS atau *persistent XSS* merupakan jenis serangan di mana kode berbahaya disimpan secara permanen dalam sistem, misalnya pada database melalui fitur seperti buku tamu atau kolom komentar. Ketika pengguna lain mengakses halaman tersebut, skrip akan otomatis dijalankan pada browser mereka [11]. Jenis ini memiliki tingkat risiko yang lebih tinggi dibandingkan *reflected XSS* karena dapat menyerang banyak pengguna sekaligus dan berdampak lebih luas [16].

3. DOM-Based XSS

   DOM-Based XSS merupakan jenis serangan XSS yang terjadi pada sisi klien, di mana *payload* dijalankan

EXPLORE: ISSN: 2087-2062, Online ISSN: 2686-181X / DOI: http://dx.doi.org/10.36448/jsit.v17i1.4871

akibat manipulasi terhadap struktur *Document Object Model* (DOM) di browser pengguna. Pada jenis ini, perubahan tidak terjadi pada respons server, melainkan pada bagaimana browser memproses dan menampilkan data berdasarkan skrip yang berjalan [16]. Hal ini membuat serangan lebih sulit dideteksi karena tidak melibatkan perubahan langsung pada server.

Dengan demikian, XSS menjadi salah satu ancaman serius dalam keamanan website karena dapat mengeksploitasi kelemahan pada pengolahan input dan interaksi pengguna, serta berdampak langsung pada keamanan data dan sesi pengguna.

E. Brute Force Attack

Brute force attack dapat didefinisikan sebagai metode serangan yang memanfaatkan percobaan berulang terhadap berbagai kombinasi hingga menemukan kredensial yang valid. Dalam konteks website, serangan ini sering digunakan untuk mencari direktori atau file tersembunyi dengan memanfaatkan daftar kata (*wordlist*) yang berisi kemungkinan nama direktori atau path yang ada pada sistem [17]. Teknik ini bekerja dengan mengirimkan sejumlah besar permintaan ke server target hingga ditemukan respons yang valid, sehingga memungkinkan penyerang mengidentifikasi celah keamanan yang dapat dieksploitasi lebih lanjut.

F. Penetration Testing

Penetration testing dapat dipahami sebagai pendekatan evaluasi keamanan dengan cara mensimulasikan serangan terhadap sistem, aplikasi, atau jaringan, dengan tujuan mengidentifikasi kerentanan yang memungkinkan terjadinya eksploitasi oleh pihak tidak sah. Pengujian ini bertujuan untuk menemukan celah keamanan sehingga dapat dilakukan tindakan pencegahan sebelum terjadi serangan nyata. Proses *penetration testing* umumnya dilakukan melalui beberapa tahapan, seperti pengumpulan informasi, identifikasi kerentanan, eksploitasi, dan analisis hasil pengujian, sehingga dapat memberikan gambaran menyeluruh mengenai tingkat keamanan suatu sistem. Dengan pendekatan ini, pengujian keamanan dapat dilakukan secara sistematis untuk mengidentifikasi serta meminimalkan risiko terhadap ancaman siber [18].

3. Metode Penelitian

A. Data

Penelitian ini menggunakan data yang diperoleh dari informasi kerentanan keamanan pada website SDN di Kec. Baturiti. Data yang dikumpulkan meliputi struktur halaman website, parameter input, mekanisme autentikasi, serta respons sistem terhadap berbagai skenario pengujian. Data tersebut diperoleh melalui observasi langsung terhadap sistem serta hasil simulasi pengujian keamanan menggunakan tools *penetration testing*. Selain itu, penelitian ini juga didukung oleh referensi dari literatur terkait keamanan web sebagai dasar dalam mengidentifikasi jenis kerentanan

B. Pengumpulan Data

Pengumpulan data dilakukan dengan menggunakan dua metode, yaitu:

1. Studi pustaka

Pengumpulan data dilakukan dengan mencari berbagai literatur seperti buku, jurnal, serta sumber ilmiah lainnya yang berkaitan dengan keamanan website, teknik *penetration testing*, dan standar OWASP Top 10. Kajian literatur dimanfaatkan sebagai dasar konseptual untuk menentukan metode yang digunakan dan merancang skenario pengujian.

2. Observasi dan Pengujian

Pengumpulan data dilakukan dengan mengamati langsung website target serta melakukan simulasi pengujian keamanan. Pengujian dilakukan menggunakan pendekatan *black box testing*, yaitu pengujian dari perspektif eksternal, di mana peneliti tidak memiliki akses langsung terhadap kode sumber, konfigurasi server, basis data, maupun log internal sistem. Validasi kerentanan dilakukan melalui verifikasi manual dan simulasi eksploitasi terbatas. Pada kerentanan *XSS*, validasi dilakukan dengan mengamati apakah *payload* yang dimasukkan melalui parameter atau *form* dapat direfleksikan, disimpan, dan dieksekusi kembali oleh *browser*. Sementara itu, pada pengujian *brute force*, validasi dilakukan dengan membandingkan pola respons sistem, seperti pesan kesalahan, *response length*, dan *response time*, untuk mengidentifikasi perbedaan antara kredensial tidak valid dan kredensial yang berpotensi valid. Tools yang digunakan dalam proses ini antara lain Burp Suite untuk analisis dan manipulasi permintaan HTTP serta Hydra untuk melakukan simulasi serangan *brute force* pada mekanisme autentikasi. Keterbatasan pendekatan *black box testing* dalam penelitian ini adalah hasil pengujian hanya menggambarkan kerentanan yang dapat diamati dari sisi pengguna atau penyerang eksternal, sehingga kelemahan yang bersifat internal, seperti kesalahan konfigurasi tersembunyi, kelemahan logika aplikasi, celah pada kode sumber, atau kerentanan yang membutuhkan akses administratif tidak dapat dianalisis secara mendalam.

C. Metode

Metode yang digunakan dalam penelitian ini adalah *penetration testing* untuk mengevaluasi tingkat keamanan website. Metode ini dipilih karena mampu mensimulasikan serangan nyata dari pihak eksternal dalam mengidentifikasi kerentanan sistem. Pendekatan ini telah banyak digunakan dalam penelitian keamanan aplikasi web, termasuk pada penelitian yang dilakukan oleh [14] yang menggunakan tahapan pengujian serupa dalam menganalisis kerentanan pada aplikasi web pendidikan. Proses *penetration testing* dilakukan melalui beberapa tahapan utama, yaitu:

1. Reconnaissance

Tahap pengumpulan informasi awal terkait target, seperti struktur website, *endpoint*, serta teknologi yang digunakan.

2. Vulnerability Assessment

Tahap identifikasi potensi kerentanan berdasarkan analisis parameter input, form, dan respons sistem terhadap input tidak valid.

3. Exploitation

Tahap pengujian untuk mengetahui apakah kerentanan dapat dimanfaatkan. Kerentanan *Cross-Site Scripting* (XSS) dan kelemahan pada mekanisme autentikasi terhadap serangan *brute force* menjadi fokus utama dalam pengujian pada penelitian ini. Pengujian *XSS* dalam penelitian ini dibatasi pada *reflected XSS* dan *stored XSS* karena kedua jenis kerentanan tersebut ditemukan pada titik input yang tersedia selama proses identifikasi kerentanan, seperti parameter URL, form pendaftaran, dan fitur buku tamu. Sementara itu, *DOM-based XSS* tidak diuji secara eksperimental karena pengujian dilakukan menggunakan pendekatan *black box* dan tidak ditemukan indikasi awal adanya manipulasi DOM pada sisi klien yang dapat dieksploitasi secara langsung.

4. Post Exploitation

Pada tahap ini dilakukan penilaian terhadap dampak yang timbul akibat eksploitasi kerentanan, seperti potensi penyalahgunaan akses dan terpaparnya data sensitif.

Alur penelitian yang digunakan dalam proses ini ditunjukkan pada di bawah ini.

Gambar 1. Alur Penelitian

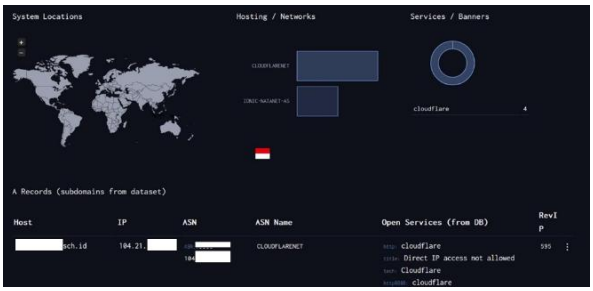
4.Hasil dan Pembahasan

Hasil penelitian ini diperoleh melalui serangkaian pengujian keamanan menggunakan metode *penetration testing* terhadap website SDN di Kec. Baturiti. Sebelum pengujian dilakukan, peneliti telah memperoleh izin dari pihak sekolah selaku pengelola website, dan seluruh proses pengujian dilakukan secara terbatas tanpa mengubah, merusak, atau mengganggu layanan sistem. Pengujian dilakukan secara sistematis melalui beberapa tahapan, yaitu *reconnaissance*, *vulnerability assessment*, *exploitation*, dan *post-exploitation*, dengan tujuan untuk mengidentifikasi serta menganalisis kerentanan yang terdapat pada sistem.

Hasil yang diperoleh dalam setiap tahapan pengujian disajikan secara bertahap dan diikuti dengan pembahasan yang menjelaskan hubungan antar temuan serta dampaknya terhadap keamanan sistem. Fokus analisis dalam penelitian ini mencakup kerentanan *Cross-Site Scripting* (*XSS*) dan kelemahan mekanisme autentikasi terhadap serangan *brute force*, yang selanjutnya dievaluasi berdasarkan tingkat risiko dan potensi eksploitasinya. Pemilihan kedua jenis serangan tersebut didasarkan pada hasil identifikasi *attack surface*, di mana website target memiliki beberapa titik input pengguna, seperti form pencarian, parameter URL, form buku tamu, serta halaman login. Titik input tersebut memiliki keterkaitan langsung dengan potensi *XSS*, sedangkan halaman login berkaitan dengan risiko *brute force* dan *account enumeration*. Oleh karena itu, pengujian difokuskan pada *XSS* dan *brute force* agar analisis sesuai dengan karakteristik kerentanan yang paling relevan pada website target.

A. Reconnaissance (Information Gathering)

Tahap awal pengujian dilakukan melalui proses *reconnaissance* untuk mengumpulkan informasi terkait target sistem. Berdasarkan hasil pengujian, website yang menjadi objek penelitian adalah website SDN di Kec. Baturiti dengan alamat https://sdn********.sch.id/. Sistem ini diketahui menggunakan teknologi berbasis PHP dengan dukungan *web server* LiteSpeed serta dilindungi oleh layanan Cloudflare. Keberadaan Cloudflare memengaruhi proses *penetration testing* karena informasi teknis server asli, seperti alamat IP *origin* dan konfigurasi infrastruktur langsung, tidak dapat diidentifikasi secara terbuka. Oleh karena itu, pengujian dalam penelitian ini difokuskan pada celah yang tetap dapat diamati dari sisi aplikasi web, seperti validasi input, respons halaman, dan mekanisme autentikasi. Selain itu, dilakukan identifikasi terhadap *attack surface* untuk menentukan titik masuk yang berpotensi menjadi celah keamanan. Identifikasi *attack surface* dilakukan dengan menelusuri halaman-halaman utama website, mengamati fitur yang menerima input pengguna, serta menganalisis parameter yang dikirim melalui URL maupun *form*. Setiap titik input kemudian diklasifikasikan berdasarkan potensi kerentanannya, seperti input teks dan parameter URL yang dikaitkan dengan potensi *XSS*, serta halaman login yang dikaitkan dengan potensi *brute force* dan *account enumeration*. Beberapa *entry point* yang ditemukan meliputi *form* pencarian, parameter URL, *form* buku tamu, serta halaman login pengguna. Keberadaan berbagai titik input ini menunjukkan adanya potensi kerentanan apabila tidak dilakukan validasi input secara optimal. Hasil pengumpulan informasi target tersebut disajikan pada gambar berikut.



Gambar 2. Informasi Target

B. Vulnerability Assessment

Tahap selanjutnya adalah *vulnerability assessment*, yaitu proses identifikasi kerentanan pada sistem. Pengujian difokuskan pada *kerentanan Cross-Site Scripting* (XSS) yang berpotensi terjadi pada input pengguna.

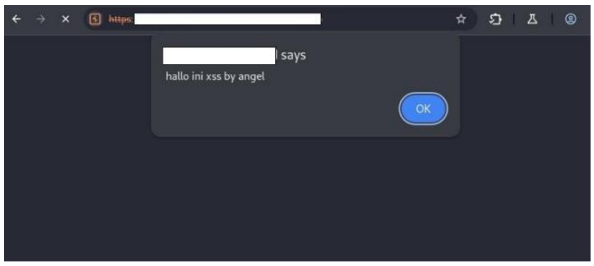
1. Reflected XSS

Melalui proses pengujian, teridentifikasi adanya celah keamanan berupa *reflected XSS* pada fitur pendaftaran pengguna. Kerentanan ini terjadi karena sistem tidak menerapkan mekanisme validasi dan sanitasi input secara memadai, khususnya pada sisi server (*server-side validation*),

EXPLORE: ISSN: 2087-2062, Online ISSN: 2686-181X / DOI: http://dx.doi.org/10.36448/jsit.v17i1.4871

sehingga data yang dimasukkan oleh pengguna direfleksikan kembali ke halaman tanpa proses penyaringan yang aman. Keberhasilan eksploitasi *reflected XSS* diukur berdasarkan kemampuan *payload* untuk melewati proses penyaringan, direfleksikan kembali oleh sistem, dan dieksekusi oleh *browser* pada sisi klien. Pada pengujian ini, keberhasilan eksploitasi ditunjukkan dengan munculnya *pop-up alert* pada browser setelah *payload* dimasukkan, sebagaimana ditampilkan pada Gambar 3. Hal ini mengindikasikan bahwa sistem belum menerapkan mekanisme *filtering* dan *output encoding* yang memadai terhadap karakter atau skrip berbahaya.

Kerentanan ini termasuk dalam kategori OWASP Top 10: A03 Injection, khususnya *Cross-Site Scripting* (XSS). Dampak yang ditimbulkan tidak hanya terbatas pada eksekusi skrip sederhana, tetapi juga berpotensi digunakan untuk mencuri cookie autentikasi pengguna, melakukan manipulasi tampilan halaman, hingga pengambilalihan sesi (*session hijacking*). Kondisi ini berpotensi menyebabkan *account takeover*, di mana penyerang dapat memperoleh akses penuh terhadap akun pengguna tanpa otorisasi. Temuan ini menunjukkan bahwa sistem belum menerapkan prinsip *secure coding*, khususnya dalam pengelolaan input dan output data pengguna. Berdasarkan analisis dan dukungan kajian literatur, kerentanan ini dikategorikan dalam tingkat risiko medium (*medium risk*). Kategori tersebut merujuk pada penelitian Gustiyono [19] yang mengidentifikasi *reflected XSS* pada kolom input sebagai kerentanan dengan tingkat risiko medium, karena dapat dieksploitasi untuk menampilkan *pop-up*, melakukan *phishing*, atau mencuri data pengguna. Kondisi ini mengindikasikan bahwa kerentanan XSS masih menjadi masalah umum pada aplikasi web yang tidak menerapkan validasi input secara optimal.



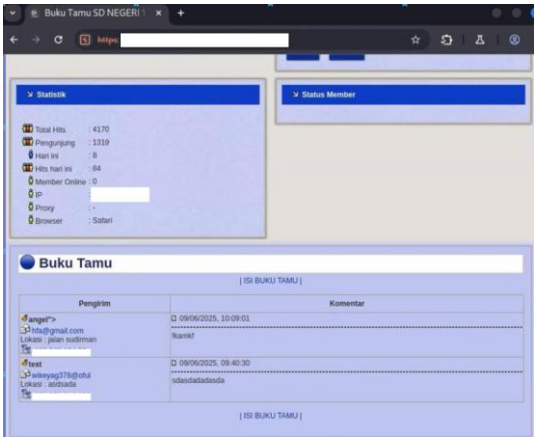
Gambar 3. Hasil Uji *Reflected* XSS

2. Stored XSS

Pengujian juga mengidentifikasi adanya kerentanan *stored Cross-Site Scripting* (*XSS*) pada fitur buku tamu. Kerentanan ini terjadi karena sistem tidak melakukan validasi dan sanitasi input sebelum data disimpan ke dalam basis data. Berbeda dengan *reflected XSS*, *payload* pada kerentanan ini tersimpan di dalam sistem dan dapat ditampilkan kembali setiap kali halaman buku tamu diakses oleh pengguna lain. Validasi keberhasilan *stored XSS* dilakukan dengan memasukkan *payload* melalui fitur buku tamu, kemudian memuat ulang halaman untuk memastikan bahwa *payload* tersebut tetap tersimpan dan ditampilkan kembali pada halaman buku tamu. Keberhasilan pengujian ditunjukkan ketika *payload* tetap muncul saat halaman buku tamu diakses ulang, sebagaimana ditampilkan pada Gambar 4. Hal ini menunjukkan bahwa sistem tidak hanya gagal dalam memfilter input sebelum data disimpan, tetapi juga belum menerapkan mekanisme *output encoding* secara memadai saat menampilkan kembali data kepada pengguna.

Kerentanan ini termasuk dalam kategori OWASP Top 10: A03 – *Injection*, dan memiliki dampak yang lebih luas dibandingkan *reflected XSS* karena bersifat persisten. Dampak yang dapat ditimbulkan meliputi penyisipan skrip berbahaya, manipulasi tampilan halaman, pencurian data pengguna, serta penyebaran serangan ke banyak pengguna apabila *payload* yang tersimpan berhasil dieksekusi pada sisi klien. Temuan ini mengindikasikan bahwa sistem memiliki kelemahan serius dalam pengelolaan data input dan penyimpanan, yang dapat dimanfaatkan untuk serangan berkelanjutan.

Berdasarkan analisis, kerentanan ini dikategorikan dalam tingkat risiko *high*. Kondisi tersebut mengindikasikan bahwa pengelolaan input dan output data yang tidak aman masih menjadi kelemahan umum dalam pengembangan aplikasi web.



Gambar 4. Hasil Uji *Stored* XSS

C. Exploitation

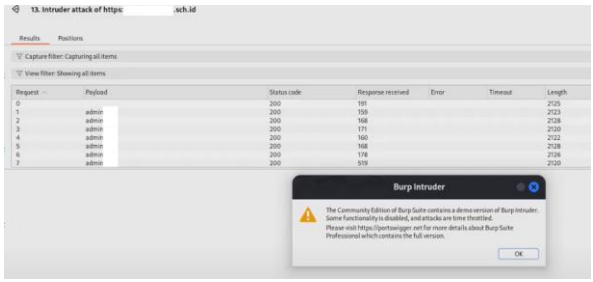
Tahap *exploitation* berfokus pada validasi praktis terhadap kerentanan yang ditemukan, guna memastikan apakah celah tersebut dapat dimanfaatkan untuk memperoleh akses ilegal ke sistem.

1. Brute Force Menggunakan Burp Suite

Pengujian terhadap mekanisme autentikasi dilakukan menggunakan Burp Suite Intruder untuk mengevaluasi ketahanan sistem terhadap serangan *brute force*. Pengujian difokuskan pada halaman login pengguna guna menganalisis kekuatan mekanisme autentikasi yang

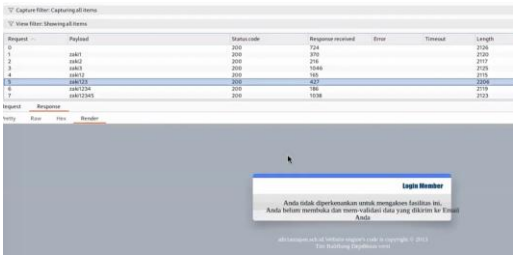
diterapkan. Metode yang digunakan adalah *dictionary attack*, yaitu dengan mencoba berbagai kombinasi username dan password yang umum digunakan. Efektivitas Burp Suite Intruder dalam pengujian ini dievaluasi berdasarkan kemampuannya mengotomatisasi pengiriman kombinasi kredensial, mencatat respons sistem terhadap setiap percobaan login, serta menampilkan perbedaan respons melalui parameter seperti *status code*, *response length*, *response time*, dan pesan yang dikembalikan oleh sistem.

Pada tahap awal, dilakukan pengiriman sejumlah kombinasi kredensial untuk mengamati respons sistem terhadap setiap percobaan login. Hasil pengujian menunjukkan bahwa sistem memberikan respons yang bervariasi, yang kemudian dianalisis berdasarkan parameter *response length* dan *response time* untuk mengidentifikasi perbedaan perilaku server. Aktivitas pengujian menggunakan Burp Suite Intruder ditunjukkan pada Gambar 5, yang memperlihatkan proses otomatisasi pengiriman payload ke sistem login.



Gambar 5. Aktivitas *Brute Force*

Selanjutnya, dilakukan pengujian lanjutan dengan variasi *payload* yang lebih spesifik pada parameter *username* dan *password* untuk mengidentifikasi pola respons sistem terhadap kombinasi kredensial tertentu. Berdasarkan hasil pengujian, ditemukan adanya perbedaan signifikan pada salah satu kombinasi kredensial. Perbedaan *response length* digunakan sebagai indikator awal karena percobaan login dengan kredensial tidak valid umumnya menghasilkan respons dengan pola dan panjang konten yang relatif serupa, seperti pesan kesalahan *username* atau *password* tidak valid. Namun, pada salah satu *payload*, yaitu zaki123, sistem menghasilkan *response length* sebesar 2206 serta waktu respons yang lebih lama dibandingkan percobaan lainnya. Sebagaimana ditunjukkan pada Gambar 7, respons sistem menampilkan pesan bahwa pengguna tidak diperkenankan mengakses sistem karena akun belum melakukan verifikasi melalui email. Hal ini menunjukkan bahwa respons yang diberikan bukan lagi respons kegagalan login umum, melainkan respons terhadap akun yang dikenali oleh sistem. Dengan demikian, kombinasi kredensial tersebut diindikasikan berpotensi valid, meskipun akses tetap dibatasi oleh mekanisme verifikasi tambahan.



Gambar 6. Hasil Pengujian *Brute Force* Menggunakan Burp Intruder

Temuan ini menunjukkan bahwa sistem mampu membedakan antara kredensial valid dan tidak valid, yang secara tidak langsung membuka peluang terjadinya *account enumeration*. Selain itu, tidak ditemukan mekanisme pengamanan tambahan seperti pembatasan jumlah percobaan login (*rate limiting*) maupun penguncian akun (*account lockout*), sehingga meningkatkan risiko eksploitasi melalui serangan *brute force* secara berulang.

Lebih lanjut, hasil pengujian juga mengindikasikan adanya kombinasi kredensial yang berpotensi valid berdasarkan perbedaan respon sistem. Hal ini menunjukkan adanya kelemahan dalam mekanisme autentikasi, khususnya dalam pengelolaan keamanan akun pengguna. Berdasarkan analisis tersebut, kerentanan ini dikategorikan dalam tingkat risiko medium (*medium risk*) dengan potensi peningkatan dampak apabila eksploitasi berhasil menyebabkan pengambilalihan akun pengguna. Kategori ini ditentukan berdasarkan beberapa indikator, yaitu adanya perbedaan respons sistem terhadap percobaan login tertentu, potensi *account enumeration*, tidak adanya mekanisme *rate limiting*, serta tidak adanya mekanisme *account lockout*. [20] menunjukkan bahwa kondisi serupa pada mekanisme login, seperti absennya *rate limiting*, absennya *account lockout*, dan adanya perbedaan respons autentikasi, dapat membuka peluang serangan *brute force* dan *password enumeration*, dengan tingkat risiko yang dikategorikan sebagai medium. Kerentanan ini termasuk dalam kategori OWASP Top 10: A07 – Identification and Authentication Failures, yang berkaitan dengan kelemahan dalam mekanisme autentikasi sistem.

2. Brute Force Menggunakan Hydra

Pengujian lanjutan dilakukan menggunakan *tools* Hydra untuk mengotomatisasi serangan *brute force* pada halaman login pengguna. Metode yang digunakan adalah *dictionary attack* dengan memanfaatkan kombinasi *username* dan *password* umum yang bersumber dari *wordlist* yang telah disiapkan. *Wordlist* disusun dalam dua berkas, yaitu daftar *username* dan daftar *password*. Daftar tersebut berisi variasi nama pengguna, kombinasi angka, serta kata sandi umum yang sering digunakan pada sistem autentikasi sederhana. Penyusunan *wordlist* bertujuan untuk mensimulasikan pola serangan *dictionary attack* secara terbatas dan terkendali, guna mengevaluasi apakah sistem memiliki mekanisme pembatasan percobaan login seperti *rate limiting* dan *account lockout*. Dalam proses pengujian, Hydra mencoba sebanyak 254.214 kombinasi kredensial.

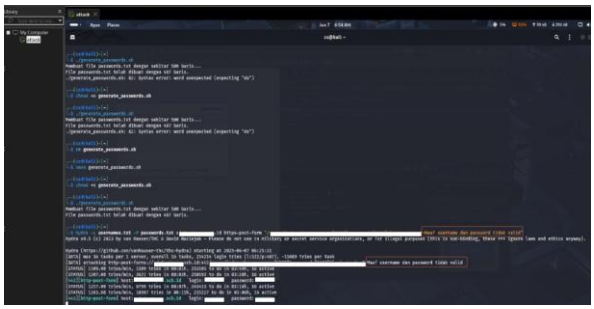
Secara umum, sistem memberikan respons kegagalan berupa pesan "Maaf username dan password tidak valid". Namun, ditemukan beberapa respons yang berbeda dari

EXPLORE: ISSN: 2087-2062, Online ISSN: 2686-181X / DOI: http://dx.doi.org/10.36448/jsit.v17i1.4871

pola umum tersebut, yang mengindikasikan kemungkinan adanya kredensial yang valid. Hasil pengujian menunjukkan bahwa terdapat dua akun yang menghasilkan respons berbeda dan berpotensi berhasil digunakan untuk proses login.

Selain itu, sistem tidak memiliki mekanisme pembatasan percobaan login seperti *rate limiting* maupun *account lockout*. Kondisi ini memungkinkan Hydra untuk melakukan ratusan ribu percobaan tanpa hambatan signifikan. Proses ini memang membutuhkan waktu yang lebih lama karena banyaknya kombinasi yang diuji, namun tanpa adanya kontrol pembatasan, probabilitas keberhasilan dalam mengidentifikasi akun valid menjadi semakin besar.

Dengan demikian, dapat disimpulkan bahwa sistem memiliki kerentanan terhadap serangan *brute force* karena memungkinkan percobaan berbagai kombinasi kredensial secara berulang tanpa mekanisme pembatasan yang memadai. Tidak adanya *rate limiting* dan *account lockout*, serta adanya perbedaan respons terhadap kombinasi kredensial tertentu, menunjukkan adanya kelemahan autentikasi yang dapat membuka peluang *account enumeration* dan akses tidak sah.



Gambar 6. Brute Force Menggunakan Hydra

D. Analisis Post Exploitation

Pada penelitian ini, tahap *post-exploitation* dilakukan untuk menganalisis dampak dari kerentanan yang berhasil dieksploitasi, khususnya pada serangan *Cross-Site Scripting (XSS)* dan *brute force*. Pada kerentanan XSS, dampak yang diidentifikasi meliputi potensi eksekusi skrip berbahaya pada sisi klien yang dapat dimanfaatkan untuk mencuri data sesi pengguna (*session hijacking*), melakukan manipulasi tampilan halaman, serta menyisipkan konten berbahaya.

Sementara itu, pada serangan *brute force*, sistem memungkinkan identifikasi kredensial yang berpotensi valid melalui perbedaan *response* yang dihasilkan. Kondisi ini membuka peluang terjadinya akses tidak sah serta penyalahgunaan akun pengguna. Tidak adanya mekanisme pengamanan seperti *rate limiting* dan *account lockout* semakin meningkatkan risiko eksploitasi lanjutan, karena penyerang dapat melakukan percobaan login secara berulang hingga menemukan kombinasi kredensial yang tepat.

Hasil analisis juga menunjukkan bahwa kerentanan yang ditemukan tidak berdiri sendiri, melainkan dapat saling berkaitan dan memperbesar risiko serangan lanjutan. Kombinasi antara *XSS* dan *brute force* memungkinkan terjadinya serangan berlapis (*multi-stage attack*) yang dapat memperluas dampak terhadap sistem. Keterkaitan *XSS* dengan *multi-stage attack* dapat terjadi ketika kerentanan *XSS* digunakan sebagai tahap awal untuk menjalankan skrip berbahaya pada sisi pengguna, yang dapat mengarah pada pencurian informasi sesi, manipulasi tampilan halaman, atau pengalihan pengguna ke halaman tertentu. Informasi yang diperoleh dari tahap awal tersebut dapat dimanfaatkan untuk mendukung tahap serangan berikutnya, seperti *account enumeration*, percobaan login berulang, atau penyalahgunaan akun melalui kelemahan autentikasi. Dengan demikian, kombinasi *XSS* dan *brute force* meningkatkan risiko karena penyerang dapat mengeksploitasi beberapa kelemahan secara berurutan, bukan hanya satu celah keamanan secara terpisah. Berdasarkan temuan tersebut, diperlukan penerapan mekanisme keamanan yang lebih komprehensif, terutama pada aspek validasi input dan penguatan sistem autentikasi.

Tabel 1 Evaluasi Dampak dan Mitigasi Kerentanan

Jenis Kerentanan	Dampak Post-Exploitation	Potensi Risiko	Rekomendasi Mitigasi
Reflected XSS	Eksekusi skrip pada browser pengguna melalui input yang tidak difilter	Pencurian data sesi, phishing, manipulasi tampilan	Terapkan validasi dan sanitasi input/output, serta gunakan Content Security Policy (CSP)
Stored XSS	Payload tersimpan dan dieksekusi setiap halaman diakses	Serangan terhadap banyak pengguna, session hijacking, penyisipan konten berbahaya	Filter input sebelum disimpan, encoding output, serta pembatasan karakter berbahaya
Brute Force	Identifikasi kredensial melalui perbedaan respons sistem	Akses tidak sah, enumerasi akun, pengambilalihan akun	Terapkan rate limiting, account lockout, serta multi-factor authentication (MFA)

5. Kesimpulan

Berdasarkan hasil pengujian, website yang diuji masih memiliki kelemahan yang cukup menonjol, terutama pada aspek validasi input dan sistem autentikasi. Adanya kerentanan *Cross-Site Scripting* (*XSS*), baik dalam bentuk *reflected* maupun *stored*, mengindikasikan bahwa proses

validasi serta sanitasi input belum diterapkan secara memadai, sehingga membuka peluang terjadinya eksekusi skrip berbahaya di sisi pengguna.

Selain itu, mekanisme autentikasi yang digunakan juga belum cukup kuat dalam menghadapi serangan *brute force*. Hal ini terlihat dari tidak diterapkannya kontrol keamanan seperti *rate limiting* dan *account lockout*, yang berpotensi meningkatkan risiko terjadinya akses tidak sah ke dalam sistem.

Temuan tersebut memperlihatkan bahwa implementasi kontrol keamanan dasar pada aplikasi web, khususnya di lingkungan website pendidikan, masih perlu ditingkatkan. Oleh sebab itu, diperlukan penerapan strategi keamanan yang lebih menyeluruh, seperti penguatan validasi input, penerapan *Content Security Policy* (*CSP*), pembatasan percobaan login, serta penggunaan *multi-factor authentication* (*MFA*) guna meningkatkan ketahanan sistem terhadap ancaman siber.

Sebagai pengembangan penelitian selanjutnya, pengujian keamanan dapat diperluas pada kategori kerentanan lain dalam OWASP Top 10, seperti *Broken Access Control*, *Security Misconfiguration*, dan *Vulnerable and Outdated Components*. Selain itu, penelitian lanjutan dapat dilakukan pada beberapa website sekolah dasar di wilayah berbeda agar diperoleh gambaran yang lebih luas mengenai tingkat keamanan website pendidikan dasar. Penelitian selanjutnya juga dapat menggunakan pendekatan penilaian risiko yang lebih terukur, seperti *Common Vulnerability Scoring System* (*CVSS*), agar tingkat risiko setiap kerentanan dapat dikategorikan secara lebih objektif.

6. Ucapan Terima kasih

Penulis mengucapkan terima kasih kepada pihak sekolah selaku pengelola website yang telah memberikan izin dan kesempatan dalam pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing yang telah memberikan arahan, masukan, serta pendampingan selama proses penyusunan artikel. Penulis turut menyampaikan terima kasih kepada seluruh pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, sehingga penelitian ini dapat diselesaikan dengan baik.

7. Daftar Pustaka

[1] R. Abdullah And F. Fachri, "Mitigasi Keamanan Webserver Sistem Informasi Akademik Terhadap Serangan Brute Force Menggunakan Penetration Testing," *Remik*, Vol. 9, No. 3, Pp. 885–896, Aug. 2025, Doi: 10.33395/Remik.V9i3.15104.

[2] G. A. J. Saskara, M. O. G. Permana, And I. M. G. Sunarya, "Security Analysis Of Indonesia E-Commerce Platform Against The Risk Of Phishing Attacks," *International Journal Of Advances In Applied Sciences*, Vol. 14, No. 2, Pp. 533–541, Jun. 2025, Doi: 10.11591/Ijaas.V14.I2.Pp533-541.

[3] K. A. Suputri *Et Al.*, "Perbandingan Tools Vulnerability Scanning Pada Pengujian Sebuah Website," *Jurnal Informatik*, Vol. 18, P. 2022, Dec. 2022, [Online]. Available: Https://Www.Geeksforgeeks.Org/Rapidscan-The-Multi-Tool-Web-Vulnerability-Scanner-In-Kali-Linux/.

[4] A. S. Andrian, M. Data, And H. Nurwarsito, "Analisis Keamanan Plugin Wordpress Terhadap Kerentanan Cross-Site Scripting," *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, Vol. 10, No. 1, Pp. 2548–964, 2026, [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[5] I. K. R. J. Prayoga, P. W. Gunawan, And I. N. Bernadus, "Analisis Keamanan Sistem Informasi Website Metode Penetration Test," *Semantik*, Vol. 11, 2025.

[6] I. M. E. Listartha, I. M. A. P. Mitha, M. W. A. Arta, And I. Km. W. Y. Arimika, "Analisis Kerentanan Website Sma Negeri 2 Amlapura Menggunakan Metode Owasp (Open Web Application Security Project)," *Simkom*, Vol. 7, No. 1, Pp. 23–27, Jan. 2022, Doi: 10.51717/Simkom.V7i1.63.

[7] D. D. Cahyani, L. P. W. P. Dewi, K. D. R. Suryadi, And I. M. E. Listartha, "Analisis Kerentanan Website Smp Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting Dan Owasp," *Insert: Information System And Emerging Technology Journal*, Vol. 2, No. 2, Dec. 2021.

[8] I. M. E. Listartha, G. A. J. Saskara, I. G. L. A. R. Putra, I. G. A. A. D. Indradewi, And B. G. K. Yudistira, "Digital Defender: Penguatan Literasi Digital Untuk Menangkal Ancaman Siber Di Kalangan Pelajar Smk Negeri Bali Mandara," In *Seminar Nasional Pengabdian Kepada Masyarakat*, Nov. 2025.

[9] P. Y. Pratiwi, M. M. P. Kertiyasa, And I. G. A. A. D. Indradewi, "Front End Design Of Design Asset Sales Information System With Human Centered Design (Hcd) Approach," *Andalasian International Journal Of Applied Science, Engineering And Technology*, Vol. 5, No. 3, Pp. 306–320, Nov. 2025, Doi: 10.25077/Aijaset.V5i3.195.

[10] G. S. Santyadiputra, I. M. E. Listartha, And G. A. J. Saskara, "The Effectiveness Of Automatic Network Administration (Ana) In Network Automation Simulation At Universitas Pendidikan Ganesha," In *Journal Of Physics: Conference Series*, Iop Publishing Ltd, Mar. 2021. Doi: 10.1088/1742-6596/1810/1/012028.

[11] K. E. Diatmika, P. Charly, I. M. P. Prayoga, And I. M. E. Listartha, "Pendeteksian Keamanan Website Sma Greenschool Menggunakan Metode Owasp Dengan Pengujian Xss," 2022. [Online]. Available: Https://Owasp.Org/Www-Project-Zap/,

[12] F. Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, Vol. 10, No. 1, Pp. 51–58, Feb. 2023, Doi: 10.25126/Jtiik.2023105872.

[13] A. M. Sari, T. Santhi, D. K. A. M. Putra, M. B. Haekal, I. M. E. Listartha, And G. A. J. Saskara,

"Pengukuran Efektivitas Sql Injection Pada Website Dengan Menggunakan Tools Jsql, Havij, Dan The Mole," *Jurnal J-Com (Jurnal Informatika Dan Teknologi Komputer)*, Vol. 4, No. 2, 2023, [Online]. Available: Http://Testphp.Vulnweb.Com,

[14] K. G. T. Wijaya And I. M. E. Listartha, "Analisis Keamanan Web Aplikasi Pendidikan Berbasis Wordpress Menggunakan Pengujian Penetrasi Sqli," *Jurnal Teknologi Sistem Informasi*, Vol. 6, No. 2, Pp. 387–396, Oct. 2025, Doi: 10.35957/Jtsi.V6i2.13070.

[15] Y. Armando And Rosalina, "Penetration Testing Tangerang City Web Application With Implementing Owasp Top 10 Web Security Risks Framework," *Jisa (Jurnal Informatika Dan Sains)*, 2023, [Online]. Available: Https://Tangerangkota.Go.Id/

[16] S. Suroto And A. Asman, "Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (Xss) Dan Metode Pencegahannya," *Zona Komputer*, Vol. 11, No. 1, 2021, [Online]. Available: Http://Www.Hackers.Com?Yid=

[17] I. M. P. Utama *Et Al.*, "Analisis Perbandingan Kinerja Tool Website Directory Brute Force Dengan Target Website Dvwa," *Jurnal Informatik*, Vol. 18, P. 2022, Dec. 2022, [Online]. Available: Https://Www.Kali.Org/Get-Kali/#Kali-Platforms,

[18] I. M. E. Listartha And G. A. J. Saskara, "Security Testing With Penetration Testing Execution Standard (Ptes) Methods To Find Misconfigurations Vulnerabilities In Network Devices," *Jurnal Elektro Luceat*, Vol. 10, Nov. 2024.

[19] A. Gustiyono, E. I. Alwi, And S. M. Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (Xss) Metode Penetration Testing," *Cybersecurity Dan Forensik Digital*, Vol. 7, No. 1, Pp. 25–33, 2024.

[20] M. I. Halil And Mansur, "Analisis Dan Perbaikan Keamanan Sistem Informasi Web Agribisnis Berbasis Grey-Box Dan White-Box Analysis And Improvement Of An Agribusiness Web Information System Security Using Grey-Box And White-Box Testing," *Sistemasi: Jurnal Sistem Informasi*, 2026, [Online]. Available: Http://Sistemasi.Ftik.Unisi.Ac.Id

EXPLORE: ISSN: 2087-2062, Online ISSN: 2686-181X / DOI: http://dx.doi.org/10.36448/jsit.v17i1.4871