Jurnal Publikasi Teknik Informatika
Volume 4 Nomor 3, September 2025
e-ISSN : 2808-8972 p-ISSN : 2808-9367, Hal 46-60
DOI: https://doi.org/10.55606/jupti.v4i3.5234
Available Online at: https://journalcenter.org/index.php/jupti

Analisis Keamanan Website E-Pinter terhadap Serangan *SQL Injection* dan XSS

Josua Karlos Manuel[1*], Rezki Kurniati[2]
[1-2] Teknik Informasi, Politeknik Negeri Bengkalis, Bengkalis, Indonesia
josuakarlos2003@gmail.com[1], rezki@polbeng.ac.id[2]

Alamat Kampus: Jl. Bathin Alam Desa Sungai Alam, Bengkalis, Riau
*Korespondensi penulis: josuakarlos2003@gmail.com**

Abstract. *Website security is a crucial aspect of ensuring data integrity, confidentiality, and availability, especially in the face of increasingly sophisticated cyber threats. E-Pinter, a digital licensing service platform, is highly vulnerable to cyberattacks such as SQL Injection and Cross-Site Scripting (XSS), both of which can potentially compromise its system and the sensitive information stored within. This study aims to evaluate the security level of the E-Pinter website against these two types of attacks through a combination of manual and automated penetration testing methods designed to identify existing vulnerabilities. The SQL Injection tests involved inserting various payloads into input parameters to assess whether the database could be manipulated, while the XSS tests were conducted by embedding malicious scripts into unvalidated inputs to determine the likelihood of user interface exploitation. The results revealed several weaknesses that attackers could exploit, potentially leading to data leaks, unauthorized access, and disruptions to system operations. These findings highlight that the E-Pinter platform, as a critical public service system, requires immediate strengthening of its security protocols. As a mitigation effort, the research recommends the implementation of prepared statements to protect against SQL Injection attacks and the use of functions such as htmlspecialchars() to prevent the execution of malicious XSS scripts. Furthermore, it emphasizes the importance of continuous security monitoring, regular penetration testing, and proper input validation as essential practices for sustainable website protection. By adopting these measures, the security of E-Pinter can be significantly enhanced, ensuring the safety of user data, improving public trust in digital government services, and reducing the risk of exploitation in the future, especially as digital transformation accelerates in public administration and service delivery*.

Keywords: *Cross-Site Scripting, Penetration Testing, Security, SQL Injection, Website*.

Abstrak. Keamanan situs web merupakan aspek krusial dalam memastikan integritas, kerahasiaan, dan ketersediaan data, terutama dalam menghadapi ancaman siber yang semakin canggih. E-Pinter, sebuah platform layanan lisensi digital, sangat rentan terhadap serangan siber seperti SQL Injection dan Cross-Site Scripting (XSS), yang keduanya berpotensi membahayakan sistem dan informasi sensitif yang tersimpan di dalamnya. Studi ini bertujuan untuk mengevaluasi tingkat keamanan situs web E-Pinter terhadap kedua jenis serangan ini melalui kombinasi metode uji penetrasi manual dan otomatis yang dirancang untuk mengidentifikasi kerentanan yang ada. Uji SQL Injection melibatkan penyisipan berbagai muatan ke dalam parameter input untuk menilai apakah basis data dapat dimanipulasi, sementara uji XSS dilakukan dengan menyematkan skrip berbahaya ke dalam input yang tidak divalidasi untuk menentukan kemungkinan eksploitasi antarmuka pengguna. Hasil penelitian mengungkapkan beberapa kelemahan yang dapat dieksploitasi oleh penyerang, yang berpotensi menyebabkan kebocoran data, akses tidak sah, dan gangguan pada operasi sistem. Temuan ini menyoroti bahwa platform E-Pinter, sebagai sistem layanan publik yang penting, memerlukan penguatan protokol keamanannya segera. Sebagai upaya mitigasi, penelitian ini merekomendasikan penerapan pernyataan siap pakai untuk melindungi dari serangan Injeksi SQL dan penggunaan fungsi seperti htmlspecialchars() untuk mencegah eksekusi skrip XSS berbahaya. Lebih lanjut, penelitian ini menekankan pentingnya pemantauan keamanan berkelanjutan, pengujian penetrasi berkala, dan validasi input yang tepat sebagai praktik penting untuk perlindungan situs web yang berkelanjutan. Dengan mengadopsi langkah-langkah ini, keamanan E-Pinter dapat ditingkatkan secara signifikan, memastikan keamanan data pengguna, meningkatkan kepercayaan publik terhadap layanan pemerintah digital, dan mengurangi risiko eksploitasi di masa mendatang, terutama seiring dengan percepatan transformasi digital dalam administrasi publik dan penyediaan layanan.

Kata kunci: *Cross-Site Scripting,* Keamanan*, Penetration Testing, SQL Injection,* Website*.*

Received: Juli 23, 2025; Revised: Agustus 05, 2025; Accepted: Agustus 20, 2025; Online Available: Agustus 22, 2025

1. LATAR BELAKANG

Internet telah menjadi sarana komunikasi global yang memberikan kemudahan akses informasi, mendukung perkembangan ilmu pengetahuan, teknologi, hiburan, dan bisnis. Namun, di balik manfaat tersebut, aspek keamanan sering kali terabaikan. Hingga saat ini, belum ada website yang sepenuhnya aman dari ancaman siber. Kerentanan pada aplikasi web dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk memperoleh akses ilegal, mencuri data sensitif, atau mengganggu ketersediaan layanan. Oleh karena itu, keamanan menjadi komponen penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data yang disimpan pada suatu sistem.

Salah satu platform yang berperan penting dalam pelayanan publik adalah E-Pinter, inovasi layanan daring Kabupaten Bengkalis yang mempermudah proses perizinan usaha maupun perizinan bangunan. Website ini menyimpan data penting yang bersifat sensitif, sehingga menjadi target potensial serangan siber. Apabila tidak dilindungi dengan baik, kerentanan keamanan dapat mengakibatkan kebocoran informasi, manipulasi data, bahkan gangguan operasional. Beberapa teknik serangan yang sering digunakan adalah SQL Injection (SQLI) dan Cross-Site Scripting (XSS). SQLI memungkinkan penyerang memanipulasi perintah SQL untuk mengakses atau mengubah data pada database, sedangkan XSS memanfaatkan celah validasi input untuk menyisipkan skrip berbahaya yang dapat dieksekusi di sisi pengguna.

Penelitian terdahulu menunjukkan bahwa kedua jenis serangan ini menjadi ancaman umum bagi berbagai website. Studi pada aplikasi web bWAPP mengungkapkan bagaimana simulasi SQLI dan XSS dapat digunakan untuk mengidentifikasi celah keamanan dan menguji efektivitas metode pencegahan. Penelitian lainnya membahas penetrasi testing pada website rental mobil dan institusi pendidikan, yang menemukan bahwa input form, URL, dan parameter pencarian merupakan titik rawan yang dapat dieksploitasi. Hasil dari penelitian-penelitian tersebut menunjukkan bahwa meskipun upaya mitigasi telah dilakukan, masih terdapat celah yang dapat dimanfaatkan oleh penyerang, menandakan perlunya strategi keamanan yang lebih komprehensif.

Kebaruan penelitian ini terletak pada fokus pengujian keamanan website E-Pinter sebagai platform layanan publik daerah yang memiliki peran strategis dalam proses perizinan. Belum ada studi sebelumnya yang secara spesifik menguji keamanan E-Pinter terhadap SQLI dan XSS menggunakan kombinasi pengujian manual dan otomatis. Penelitian ini diharapkan dapat mengidentifikasi potensi kerentanan serta memberikan rekomendasi teknis seperti penggunaan prepared statements dan penerapan fungsi validasi input untuk meningkatkan

keamanan. Dengan demikian, hasil penelitian ini dapat menjadi kontribusi nyata dalam memperkuat keamanan sistem layanan publik berbasis web, melindungi data pengguna, dan mengurangi risiko eksploitasi di masa mendatang.

2. KAJIAN TEORITIS

Kajian teoritis pada penelitian ini mengacu pada berbagai studi terdahulu yang membahas pengujian dan penguatan keamanan website terhadap serangan siber, khususnya SQL Injection (SQLI), Cross-Site Scripting (XSS), serta metode pengujian menggunakan framework keamanan seperti OWASP, ISSAF, dan PTES. Berbagai penelitian sebelumnya menunjukkan bahwa celah keamanan pada aplikasi web masih sering ditemukan, bahkan pada sistem yang digunakan untuk layanan publik atau pendidikan, sehingga diperlukan pendekatan sistematis dalam mendeteksi dan menanggulanginya.

Penelitian yang dilakukan pada aplikasi web bWAPP menunjukkan bahwa teknik SQLI dan XSS dapat dimanfaatkan untuk mengeksploitasi celah keamanan jika validasi input tidak dilakukan dengan baik. Studi ini menekankan pentingnya penerapan input validation, penggunaan prepared statements, pembatasan hak akses pengguna, serta penerapan output encoding sebagai langkah pencegahan. Hasil ini sejalan dengan penelitian yang mengoptimalkan penetrasi testing pada website rental mobil CV. Merdeka Auto Rental, yang berhasil mengidentifikasi 12 celah keamanan dan memperbaikinya dengan menambahkan fungsi PHP untuk menghapus karakter berbahaya, sehingga website menjadi lebih tahan terhadap SQLI dan XSS.

Pendekatan penetrasi testing juga diterapkan pada website STIE Samarinda, yang menemukan 14 fitur form rentan terhadap SQLI dan XSS. Rekomendasi yang diberikan mencakup pelaksanaan pengujian keamanan secara berkala, validasi input, sanitasi output, dan pembaruan strategi keamanan sesuai perkembangan ancaman. Perlindungan berbasis Web Application Firewall (WAF), seperti yang digunakan dalam penelitian dengan ModSecurity, terbukti efektif memblokir serangan SQLI dan XSS melalui penerapan aturan yang telah ditentukan.

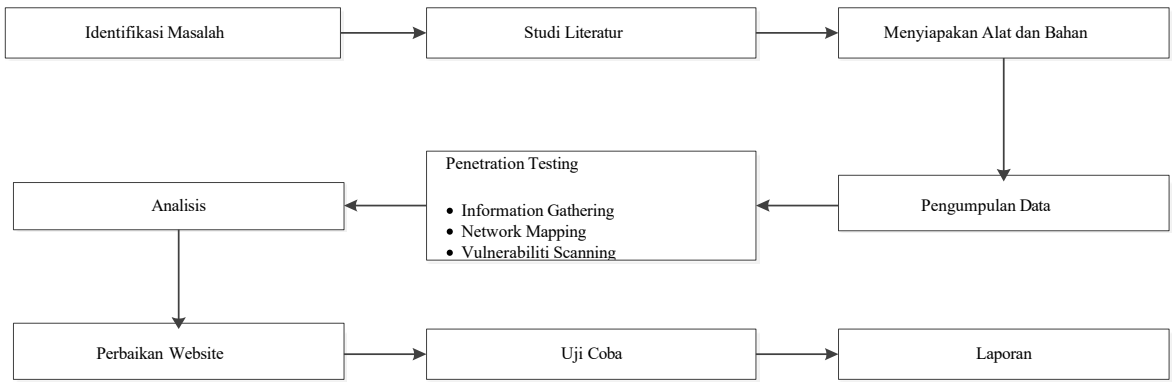
Metode penilaian keamanan menggunakan framework ISSAF juga banyak digunakan. Studi pada website Universitas Internasional Batam dan SMK Al-Kautsar menunjukkan bahwa framework ini mampu mengidentifikasi kerentanan terhadap berbagai ancaman, termasuk DDoS, port scanning, dan serangan berbasis injeksi. Penelitian lainnya yang menggunakan metode PTES pada website min2kotabengkulu.sch.id mendapati tingkat kerentanan rendah, namun tetap menekankan pentingnya pemantauan dan perbaikan berkala.

Selain itu, pemindaian menggunakan OWASP ZAP, seperti pada penelitian analisis kerentanan website perusahaan, dapat mengidentifikasi ancaman seperti backdoor dan celah eksploitasi lainnya. Temuan-temuan ini menunjukkan bahwa meskipun banyak metode keamanan telah diterapkan, ancaman siber terhadap aplikasi web tetap berkembang, sehingga strategi keamanan harus bersifat adaptif, berlapis, dan dilakukan secara berkesinambungan.

Berdasarkan kajian tersebut, penelitian ini memposisikan diri dengan memanfaatkan metode pengujian SQLI dan XSS, serta alat bantu keamanan OWASP, untuk menganalisis dan memperkuat keamanan website E-Pinter. Pendekatan ini diharapkan dapat memberikan kontribusi praktis dalam melindungi sistem layanan publik berbasis web dari potensi eksploitasi, sekaligus memperkaya literatur terkait strategi keamanan siber pada layanan pemerintahan daring.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan uji penetrasi (penetration testing) berbasis metode Information System Security Assessment Framework (ISSAF) untuk mengevaluasi keamanan website E-Pinter terhadap serangan SQL Injection (SQLI) dan Cross-Site Scripting (XSS). ISSAF dipilih karena kerangka kerja ini memiliki tahapan yang terstruktur, mulai dari identifikasi masalah hingga penyusunan rekomendasi perbaikan, sehingga proses pengujian menjadi lebih sistematis dan terarah.



Gambar 1. Tahapan Penelitian

Desain Penelitian

Desain penelitian dibagi ke dalam tiga tahap utama:

a. Planning and Preparation

Tahap ini mencakup identifikasi masalah pada website E-Pinter, penentuan ruang lingkup pengujian, serta studi literatur terkait SQLI, XSS, dan teknik pengujian keamanan terbaru. Persiapan perangkat keras dan perangkat lunak dilakukan untuk memastikan kelancaran pengujian.

b. Assessment

Pada tahap ini dilakukan pengumpulan informasi (information gathering) menggunakan Whois, pemetaan jaringan (network mapping) menggunakan Nmap, serta pengujian SQLI dan XSS baik secara manual maupun otomatis. Alat yang digunakan antara lain SQLmap, Burp Suite, dan OWASP ZAP. Pengujian SQLI dilakukan dengan menyisipkan payload pada parameter input untuk menguji potensi manipulasi database, sedangkan pengujian XSS dilakukan dengan menyisipkan skrip berbahaya untuk melihat respon sistem.

c. Reporting

Tahap akhir meliputi analisis hasil pengujian, identifikasi kerentanan, penyusunan rekomendasi teknis, perbaikan pada website, uji coba ulang, serta dokumentasi hasil secara menyeluruh.

Populasi dan Sampel Penelitian

Objek penelitian adalah website E-Pinter Kabupaten Bengkalis yang digunakan sebagai platform pelayanan perizinan daring. Sampel pengujian difokuskan pada halaman, formulir, dan parameter input yang memiliki interaksi langsung dengan database atau memproses data dari pengguna.

Teknik dan Instrumen Pengumpulan Data

Pengumpulan data dilakukan melalui:

a. Observasi langsung untuk memahami struktur dan modul fungsional website.
b. Pengujian manual dengan memasukkan payload SQLI dan XSS pada titik input yang dipilih.
c. Pengujian otomatis menggunakan tool seperti Whois, Nmap, SQLmap, Burp Suite, Kali Linux, dan OWASP ZAP.

Instrumen penelitian meliputi laptop Acer dengan prosesor AMD Ryzen 3 3250U, RAM 8 GB, HDD 500 GB, koneksi WiFi dan data seluler, serta sistem operasi Windows 10 dan Kali Linux.

Alat Analisis Data

Analisis dilakukan berdasarkan prinsip ISSAF, meliputi:

a. Identifikasi titik lemah berdasarkan hasil pengujian.
b. Analisis tingkat risiko kerentanan terhadap aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data.
c. Penyusunan rekomendasi teknis, seperti penggunaan prepared statements untuk mencegah SQLI dan penerapan output encoding serta validasi input untuk mencegah XSS.

Model Penelitian

Model penelitian mengikuti siklus Planning and Preparation → Assessment → Reporting. Siklus ini memastikan setiap tahap terhubung secara berkesinambungan sehingga hasil pengujian dapat diimplementasikan secara langsung dan memberikan dampak nyata terhadap peningkatan keamanan website E-Pinter.

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil penelitian menunjukkan bahwa tahap pengumpulan informasi berhasil mengidentifikasi domain, subdomain, dan port yang digunakan oleh website E-Pinter. Proses pemetaan jaringan ini memberikan gambaran awal mengenai infrastruktur yang digunakan, termasuk layanan yang berjalan pada port tertentu. Beberapa port terdeteksi dalam kondisi terbuka, yang berpotensi dimanfaatkan sebagai titik masuk oleh penyerang. Temuan ini menjadi dasar dalam perancangan pengujian lanjutan untuk mendeteksi kerentanan SQL Injection (SQLI) dan Cross-Site Scripting (XSS) baik secara manual maupun menggunakan alat bantu seperti SQLmap, Burp Suite, dan OWASP ZAP.

Pembahasan hasil ini menunjukkan bahwa adanya port terbuka tanpa pengamanan memadai selaras dengan temuan penelitian sebelumnya yang menekankan pentingnya konfigurasi keamanan jaringan sebagai lapisan pertahanan awal. Penelitian terdahulu juga mengungkapkan bahwa celah pada konfigurasi jaringan sering kali menjadi pintu masuk awal serangan siber. Keunggulan penelitian ini adalah pemanfaatan hasil pemetaan sebagai panduan fokus pengujian, sehingga langkah-langkah pengujian lebih efisien. Namun, keterbatasan

penelitian adalah ruang lingkupnya yang hanya mencakup SQLI dan XSS, sehingga potensi celah keamanan lain belum dianalisis secara menyeluruh. Meskipun demikian, hasil penelitian ini dapat menjadi acuan strategis dalam memperkuat keamanan website E-Pinter, khususnya dalam mengamankan titik masuk potensial dari serangan.

Target Website Pengujian

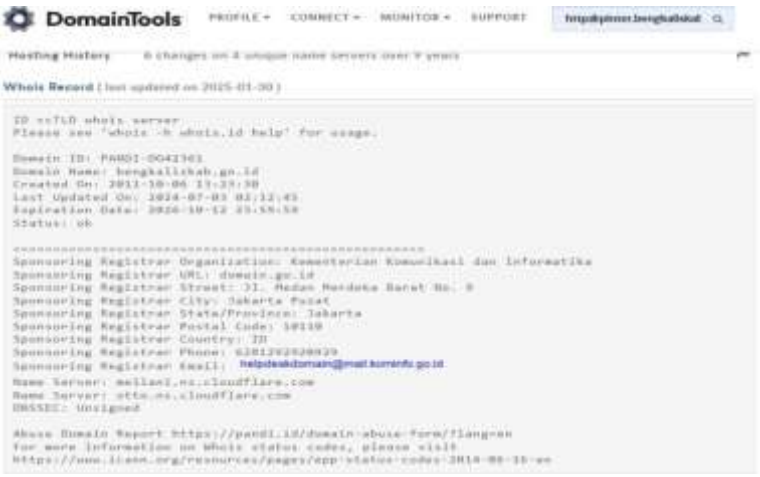
Website yang akan diuji adalah E Pinter, yang merupakan sebuah platform menawarkan berbagai layanan serta informasi.

Gambar 2. Halaman Tampilan Website e-pinter

Gambar 3. Halaman Tampilan Login e-pinter

Pencarian Informasi

WHOIS merupakan alat yang digunakan untuk mendapatkan informasi tentang pemilik domain dan alamat IP. Dengan memanfaatkan *WHOIS*, pengguna dapat mengetahui berbagai detail, termasuk nama pemilik, alamat, nomor telepon, dan tanggal pendaftaran domain. Prosesnya dimulai dengan mengunjungi situs penyedia WHOIS, di mana pengguna hanya perlu memasukkan nama domain yang ingin dicari dan mengklik tombol pencarian. Hasil yang muncul akan menampilkan informasi mengenai pemilik dan rincian registrasi lainnya.



Gambar 4. Halaman Tampilan Hasil Who is Website Target

Tabel 1. Hasil Who Is

Nama Domain	bengkaliskab.go.id
ID Domain	PANDE-0042361
Tanggal Pembuatan	2011-10-06 13:23:30
Tanggal Diperbarui	2024-07-05 02:12:45
Tanggal Kedaluwarsa	2026-10-12 23:59:59
Status	Active

Serangan SQL Injection

Peneliti melakukan uji SQL Injection pada formulir login Website E-Pinter dengan tujuan menguji apakah mekanisme verifikasi kredensial rentan terhadap manipulasi query. Secara normal proses login memeriksa kecocokan username dan password melalui query seperti:

SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password'; Dalam pengujian, peneliti memasukkan payload injeksi pada kolom username atau password (mis. ' OR '1'='1'; --) untuk melihat bagaimana server merespons. Payload ini mengubah logika query sehingga kondisi menjadi selalu benar dan sisa perintah SQL diabaikan karena -- (comment), sehingga berpotensi melewati autentikasi tanpa kredensial valid.

Secara operasional, percobaan mencakup beberapa variasi teknik injeksi (bypass/boolean-based, error-based, dan union-based) untuk mengidentifikasi jenis kerentanan dan perilaku aplikasi terhadap input berbahaya. Setiap percobaan dicatat dengan teliti: payload yang digunakan, respons HTTP (redirect, pesan error, isi halaman), indikasi akses (mis. akses

ke dashboard), dan jejak server jika tersedia (pesan log atau error). Hasil observasi tersebut kemudian diklasifikasikan sebagai rentan atau tidak rentan, dan dilengkapi dengan catatan tentang kemungkinan penyebab (mis. tidak ada prepared statement, validasi input lemah, atau error disclosure).

Tabel 2. Baypass Query Sql Injection

No	Baypas Query SQL Injection
1	or 1=1
2	or 1=1--
3	or 1=1#
4	or 1=1/*
5	admin' --
6	admin' or '1'='1
7	admin' or '1'='1'--
8	admin' or '1'='1'#
9	admin' or 1=1
10	admin'or 1=1 or ''='
11	admin' or 1=1/*
12	admin') or ('1'='1
13	admin') or ('1'='1'--
14	admin') or ('1'='1'#

Setelah berhasil mendapatkan *query Bypass SQL Injection*, langkah berikutnya adalah mencoba memasukkan query tersebut ke dalam *form* login di website. Tujuannya adalah untuk mengecek apakah *query* tersebut bisa digunakan untuk masuk ke sistem tanpa menggunakan username dan password yang benar.

Gambar 1. Percobaan menggunakan " or 1=1 "

Gambar 2. Percobaan Baypas ke-1

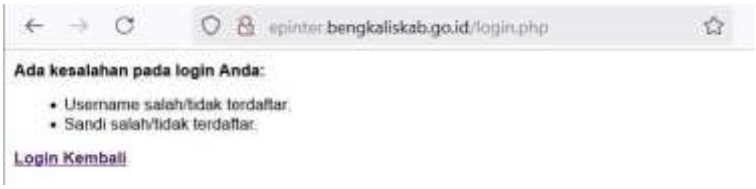
Percobaan login dengan menggunakan *bypass SQL Injection* berupa "or 1=1" dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Gambar 3. Percobaan Menggunakan " or 1=1-- "

Gambar 4. Hasil Percobaan " or 1=1-- "

Percobaan login dengan menggunakan *bypass SQL Injection* berupa " or 1=1--" dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Gambar 5. Percobaan Menggunakan " or 1=1# "



Gambar 6. Hasil Percobaan " or 1=1# "

Percobaan login dengan menggunakan *bypass SQL Injection* berupa " or 1=1# " dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Gambar 7. Percobaan Menggunakan " or 1=1/* "

Gambar 8. Hasil Percobaan " or 1=1/* "

Percobaan login dengan menggunakan *bypass SQL Injection* berupa " or 1=1/* " dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Gambar 9. Percobaan Menggunakan " admin' -- "

Gambar 10. Hasil percobaan " admin' -- "

Percobaan login dengan menggunakan *bypass SQL Injection* berupa "admin' -- " dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Gambar 11. Percobaan Menggunakan " admin' or '1'='1 "

Gambar 12. Hasil Percobaan " admin' or '1'='1 "

Percobaan login dengan menggunakan *bypass SQL Injection* berupa "admin' or '1'='1 " dinyatakan tidak berhasil. Ini menunjukkan bahwa sistem login pada website mampu mencegah serangan tersebut dan tidak memberikan akses meskipun menggunakan input yang bertujuan untuk mengecoh verifikasi.

Serangan XXS

XSS atau *Cross-Site Scripting* adalah serangan di mana penyerang menanamkan kode berbahaya (umumnya *JavaScript*) ke dalam sebuah situs *web*. Kode tersebut kemudian tampil di halaman yang diakses oleh pengguna lain. <h1> By hasil </hi>

Hasil Temuan Xss

Gambar 17. Hasil temuan xss 1

Kode tersebut kemudian tampil di halaman yang diakses oleh pengguna lain. <h1> By hasil </hi>.

Gambar 18. Hasil temuan xss 2

5. KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa website E-Pinter memiliki kerentanan keamanan terhadap serangan SQL Injection dan Cross-Site Scripting (XSS) yang berpotensi dimanfaatkan penyerang untuk menyisipkan kode berbahaya, mengakses informasi login, maupun memanipulasi data penting. Pengujian manual dan otomatis menggunakan SQLMap serta XSS testing berhasil mengidentifikasi beberapa titik lemah, termasuk terekspos nya struktur database dan keberhasilan eksekusi skrip XSS pada antarmuka pengguna. Risiko yang ditimbulkan meliputi kebocoran data, gangguan integritas, dan penurunan ketersediaan sistem, yang dapat berdampak pada kelancaran layanan publik berbasis web. Langkah mitigasi seperti penerapan prepared statements untuk mencegah SQL Injection dan penggunaan fungsi htmlspecialchars() untuk menangkal XSS terbukti efektif mengurangi risiko setelah dilakukan perbaikan dan uji ulang. Penelitian ini tidak hanya memenuhi tujuan awal untuk mengidentifikasi celah keamanan dan memberikan solusi teknis, tetapi juga memberikan

manfaat praktis bagi pengembang aplikasi web sebagai acuan penerapan validasi input/output dan strategi mitigasi keamanan.Berdasarkan temuan tersebut, disarankan agar pengelola website E-Pinter melakukan uji keamanan secara berkala dengan metode manual maupun otomatis untuk mendeteksi celah baru yang mungkin muncul, serta menerapkan prepared statements pada seluruh query database dan validasi output seperti htmlspecialchars() guna mencegah eksploitasi. Tim pengembang juga perlu meningkatkan kesadaran dan kompetensi keamanan aplikasi melalui pelatihan rutin, serta menerapkan kebijakan keamanan berkelanjutan seperti pembaruan sistem, audit kode sumber, dan penggunaan Web Application Firewall (WAF). Mengingat penelitian ini hanya berfokus pada SQL Injection dan XSS, penelitian selanjutnya diharapkan dapat memperluas cakupan pengujian terhadap jenis serangan lain, seperti Distributed Denial of Service (DDoS) atau kelemahan autentikasi, sehingga dapat memberikan gambaran yang lebih komprehensif mengenai keamanan sistem informasi publik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Politeknik Negeri Bengkalis atas dukungan fasilitas dan kesempatan yang diberikan, serta kepada pengelola website E-Pinter Kabupaten Bengkalis atas izin dan akses untuk pengujian keamanan sistem. Ucapan terima kasih juga disampaikan kepada dosen pembimbing, tim penguji, rekan-rekan, dan semua pihak yang telah membantu sehingga penelitian ini dapat terselesaikan dengan baik.

DAFTAR REFERENSI

Aliero, M. S., Ghani, I., Zainudden, S., Khan, M. M., & Bello, M. (2015). Review on SQL injection protection methods and tools. *Jurnal Teknologi (Sciences & Engineering), 77*(13). https://doi.org/10.11113/jt.v77.6359

Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis celah keamanan pada website dengan menggunakan metode penetration testing dan framework ISSAF pada Website SMK Al-Kautsar. *LEDGER: Journal Informatic and Information Technology, 2*(1), 1–13.

Anugrah, T. (2024). Penetration testing keamanan website STIE Samarinda menggunakan teknik SQL injection dan XSS. *Jurnal Informatika dan Teknik Elektro Terapan, 12*(1). https://doi.org/10.23960/jitet.v12i1.3882

Dahlan, M., Latubessy, A., Nurkamid, M., & Anggraini, L. (2014). Pengujian dan analisa keamanan website terhadap serangan SQL injection (Studi kasus: Website UMK). *Jurnal Sains dan Teknologi, 7*(1), 13–19.

Hasibuan, A. F., & Handoko, D. (2023). Analisis kerentanan website dengan aplikasi OWASP ZAP. *Jurnal Ilmu Komputer dan Sistem Informasi, 2*(2), 257–270. https://doi.org/10.70340/jirsi.v2i2.51

Herman, H., Riadi, I., Kurniawan, Y., & Rafiq, I. A. (2023). Analisis keamanan website menggunakan Information System Security Assessment Framework (ISSAF). *Jurnal Teknologi Informatika dan Komputer, 9*(1), 126–136. https://doi.org/10.37012/jtik.v9i1.1439

Muhammad, H. H., Hadiana, A. I., & Ashaury, H. (2023). Pengamanan aplikasi web dari serangan SQL injection dan cross-site scripting menggunakan web application firewall. *JATI (Jurnal Mahasiswa Teknik Informatika), 7*(5), 3265–3273. https://doi.org/10.36040/jati.v7i5.7320

Muhyidin, Y., Totohendarto, M. H., & Undamayanti, E. (2022). Perbandingan tingkat keamanan website menggunakan Nmap dan Nikto dengan metode ethical hacking. *Jurnal Teknologika, 12*(1), 80–89.

Mujiati, H. (2013). Analisis dan perancangan sistem informasi stok obat pada Apotek Arjowinangun. *Indonesian Journal of Computer Science (Speed FTI UNSA), 9330*(2), 1–6.

Prasetyo, S. E., & Hassanah, N. (2021). Analisis keamanan website Universitas Internasional Batam menggunakan metode ISSAF. *Jurnal Ilmiah Informatika, 9*(2), 82–86. https://doi.org/10.33884/jif.v9i02.3758

Risky, M. A. Z., & Yuhandri, Y. (2021). Optimalisasi dalam penetration testing keamanan website menggunakan teknik SQL injection dan XSS. *Jurnal Sistim Informasi dan Teknologi*, 215–220. https://doi.org/10.37034/jsisfotek.v3i4.68

Saputra, D. W., Pradini, R. S., & Anshori, M. (2025). Analisis dan rekomendasi keamanan website Kampus X menggunakan ISSAF. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi, 6*(1), 830–843. https://doi.org/10.35870/jimik.v6i1.1306

Smith, A. B. (2019). Analisis keamanan jaringan menggunakan intrusion prevention system. *Journal of Cybersecurity, 17*(3), 105–120.

Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Analisis keamanan sistem informasi akademik berbasis web menggunakan framework ISSAF. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 12*(1). https://doi.org/10.35889/jutisi.v12i1.1191

Utama, D. A., Khairil, K., & Supardi, R. (2024). Analisis keamanan website menggunakan PTES (Penetration Testing Execution and Standard). *Jurnal Media Infotama, 20*(1), 106–112.