e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 8 No. 2, Desember, 2024, **Hal. 418-427**
DOI: 10.29408/edumatic.v8i2.27109

Deteksi Tingkat Kerentanan Keamanan Website dengan Metode Manual Pentest dan Tools Xspear

Ahmad Jazuli [1], Irma Salamah [1,*], Sopian Soim [1]

[1] Program Studi Sarjana Terapan Teknik Telekomunikasi, Politeknik Negeri Sriwijaya, Indonesia
[*] Correspondence: irma.salamah@yahoo.com

Received: 23 Juli 2024 | Revised: 27 Juli 2024 | Accepted: 14 September 2024 | Published: 19 Desember 2024

Abstrak
Saat ini, internet telah berkembang menjadi sumber informasi untuk berbagai bidang dan kalangan sehingga dapat dengan mudah diakses oleh banyak orang. Injeksi SQL dan XSS *payload* adalah salah satu jenis yang paling umum. Tujuan dari penelitian ini adalah mendeteksi tingkat kerentanan celah keamanan yang ditemukan dan memberikan saran kepada host untuk mengurangi risiko kerentanan tersebut. Jenis penelitian ini adalah kualitatif yang difokuskan deteksi level tingkat celah keamanan pada website hotel embrio. Penelitian ini menggunakan metode evaluasi kerentanan dan pengujian penetrasi, dengan pendekatan uji penetrasi manual terhadap URL yang ditargetkan serta pemindaian kerentanan menggunakan alat bantu *Xspear*. Tahapan penelitian dimulai dengan pengumpulan informasi dari sumber-sumber relevan melalui studi kasus dan kajian literatur dari artikel ilmiah, Instalasi *software* dan *tools* yang akan digunakan, lalu ke tahap inti yaitu mengeksploitasi dengan teknik pentest, serta mencatat hasil analisis kerentanan yang ditemukan. Subjek penelitian adalah website hotel embryo dan objek penelitian adalah celah keamanan yang terdeteksi pada *website* tersebut. Hasil temuan kami didapatkan sebuah parameter dalam website hotel embryo pada menu *room* ditemukan 10 celah kerentanan dengan status *high* sehingga dapat berdampak buruk terutama data penting seperti administrasi, data pribadi, tentang instansi, dan lainnya yang bisa diretas dan disalahgunakan oleh pelaku *cyber*.

Kata kunci: *injeksi sql; kerentanan; website; xspear*

Abstract
Currently, the internet has evolved into a source of information across various fields and demographics, making it easily accessible to many people. SQL injection and XSS payloads are among the most common types. The objective of this research is to detect the level of vulnerability of security gaps found and provide recommendations to the host for mitigating those risks. This research is qualitative in nature, focused on detecting the security gap levels on the Hotel Embryo website. The study uses vulnerability evaluation and penetration testing methods, with a manual penetration testing approach targeting specific URLs and vulnerability scanning using the Xspear tool. The research stages begin with gathering information from relevant sources through case studies and literature reviews of scientific articles, software and tools installation, followed by the core phase, which involves exploitation through pentest techniques and documenting the analysis results of the vulnerabilities found. The research subject is the Hotel Embryo website, and the research object is the security vulnerabilities detected on the website. Our findings identified a parameter in the room menu of the Hotel Embryo website, where 10 vulnerabilities with a HIGH status were discovered, posing significant risks, particularly to important data such as administrative information, personal data, institutional details, and more, which could be hacked and misused by cyber attackers.

Keywords*: sql injection; vulnerability; website; xspear*

PENDAHULUAN

Perkembangan teknologi dan internet semakin hari semakin maju. Perubahan ini membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk dalam cara kita mengakses informasi dan berkomunikasi. Salah satu inovasi yang terus berkembang seiring dengan kemajuan teknologi adalah *website* (Pranata, 2023). *Website*, atau sering juga disebut sebagai situs web, adalah sekumpulan halaman-halaman yang digunakan untuk menampilkan informasi dalam berbagai bentuk. Informasi tersebut bisa berupa teks, gambar diam, gambar bergerak, animasi, suara, atau kombinasi dari semuanya (Cahyo, 2022; Sansena & Samsudin, 2023). Halaman-halaman ini dirancang sedemikian rupa sehingga saling terkait, membentuk satu rangkaian bangunan informasi yang koheren dan mudah diakses. Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis. Tujuan pembuatan sistem keamanan informasi adalah mencegah penyalahgunaan informasi oleh pihak yang tidak berkepentingan atau tidak berhak mengelola informasi tersebut. Dalam menerapkan keamanan informasi, perusahaan organisasi harus memperhatikan 3 aspek yaitu *Confidentiality, Integrity,* dan *Availability* (CIA)(Soewoeh et al., 2023).

Sebagai konsekuensi dari perkembangan teknologi dan peningkatan aksesibilitas alat-alat penetrasi yang tersedia di internet, penting untuk secara berkelanjutan memantau dan meningkatkan kualitas keamanan jaringan, situs web, *server*, dan *database* (Andarini et al., 2023). Pengetahuan mengenai teknik-teknik peretasan yang semakin meluas memungkinkan para penyusup dan penyerang untuk lebih mudah melakukan serangan, sehingga memerlukan upaya preventif yang lebih proaktif dan terstruktur dalam menjaga integritas dan kerahasiaan sistem informasi (Riyanti et al., 2024).

Pada era digitalisasi ini penggunaan website menjadi wadah untuk kebutuhan terkait semua data dan informasi terutama di bidang perhotelan dalam memberikan layanan untuk turis atau pelancong dari tiap mancanegara untuk penginapan selama masa liburan, namun website ini juga tidak terlepas dari serangan *cyber* seperti peretasan akun, eksploitasi data arsip yang bersifat private, dan bentuk kejahatan lainnya (Zirwan, 2022). Ada beberapa jenis serangan situs web yang sering terjadi, termasuk Malware, *Cross-Site Scripting* (XSS), dan SQL Injection (Nugraha et al., 2024). Setiap jenis serangan ini memiliki karakteristik dan metode penyerangan yang berbeda, serta dampak yang bisa sangat merugikan baik bagi individu maupun organisasi. Salah satu jenis serangan yang paling populer dan berbahaya adalah SQL Injection (Laksono, 2021). Untuk pencegahan masalah peretasan data pada *website* embryohotel, kami memberikan solusi dengan melakukan uji penetrasi manual dengan metode GET dan scanning kerentanan dengan bantuan *tools Xspear* untuk mengetahui tingkat celah keamanan yang diindikasi apakah aman atau berbahaya (Astriani, 2021).

Vulnerability assesment adalah alat scanning keamanan sistem dengan tujuan untuk menemukan kemungkinan risiko yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab (Allo, 2024). *Vulnerability scanner* memeriksa infrastruktur dan aplikasi untuk menemukan masalah, seperti konfigurasi yang tidak aman, bug perangkat lunak, dan praktik pengkodean yang buruk (Ramadhan et al., 2022). *Vulnerability testing* banyak digunakan untuk meningkatkan kesadaran tentang pentingnya keamanan informasi di berbagai organisasi. Dengan melakukan penilaian kerentanan secara rutin, perusahaan dapat mendeteksi hampir semua celah keamanan yang umum terjadi pada sistem mereka (Suhaila et al., 2024). Proses ini sangat penting dalam era digital saat ini, di mana ancaman siber semakin meningkat dan menjadi semakin kompleks (Armando et al., 2022).

Metode pengujian penetrasi atau penetration testing merupakan proses penting dalam mengidentifikasi kerentanan di dalam sistem informasi dengan cara mensimulasikan serangan dari pihak yang tidak bertanggung jawab (Armadhani et al., 2022). Metode ini dapat difasilitasi baik dengan menggunakan tools otomatis maupun dilakukan secara manual, tergantung pada

kompleksitas sistem yang diuji dan tujuan pengujian itu sendiri (Pratama, 2019). Dalam pengujian penetrasi, penguji memiliki wewenang untuk melakukan pengujian dengan sengaja mengeksploitasi sistem dan mencari tahu kemungkinan eksploitasi. Tujuan utama dari pengujian penetrasi adalah untuk mengidentifikasi kelemahan yang dapat dieksploitasi dalam suatu lingkungan dengan cara yang lebih aktif dan agresif (Sanjaya et al., 2020).

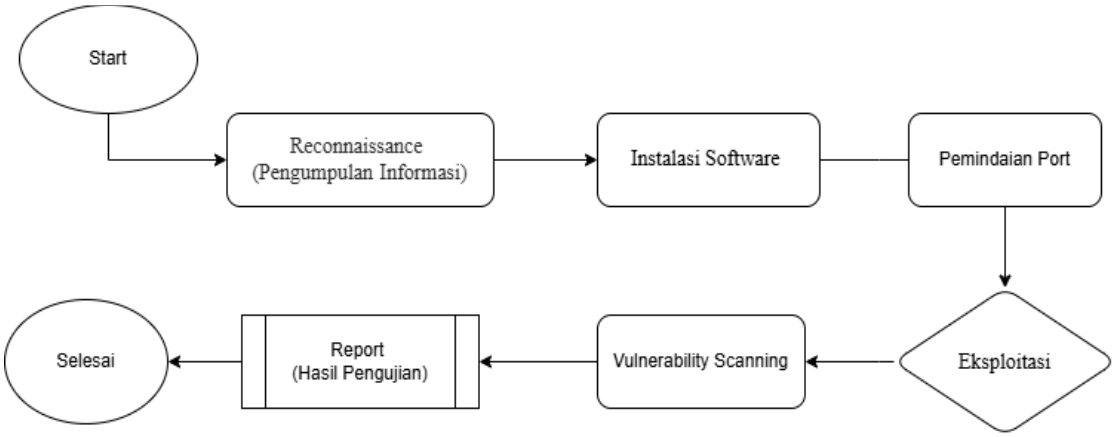
Penelitian sebelumnya yang dilakukan oleh Dasmen et al. (2023) berfokus pada pendeteksian celah kerentanan dalam sistem informasi *e-learning* Universitas Bina Darma dengan menggunakan *tool* Xspear untuk memindai potensi celah keamanan. Hasil analisis menunjukkan bahwa sistem memiliki tingkat kerentanan sedang (*medium*), yang berarti tingkat keamanannya berada pada kisaran 50% aman dan 50% rentan. Namun, hasil tersebut tidak menjamin bahwa situs tersebut sepenuhnya bebas dari ancaman keamanan. Penelitian lain oleh Herawati et al. (2023) menguji kerentanan aplikasi Data Pokok Pendidikan (Dapodik) terhadap serangan SQL *Injection* menggunakan *Acunetix* Web *Vulnerability Scanner*. Hasil penelitian tersebut menunjukkan bahwa aplikasi Dapodik tidak rentan terhadap serangan SQL *Injection*, dengan tingkat kerentanan berada di level nol atau tidak ditemukan celah keamanan.

Meskipun beberapa penelitian sebelumnya, seperti yang dilakukan oleh Dasmen et al. (2023) menggunakan *Xspear* dan Herawati et al. (2023) menggunakan *Acunetix* Web *Vulnerability Scanner*, telah mengidentifikasi tingkat kerentanan dalam berbagai sistem, studi tersebut belum menawarkan solusi konkret untuk meningkatkan keamanan. Oleh karena itu, penelitian ini bertujuan untuk memberikan rekomendasi yang spesifik dan implementatif guna meningkatkan keamanan data secara lebih efisien dan efektif.

Tujuan utama penelitian ini adalah mendeteksi tingkat kerentanan pada situs web Embrio Hotel dan memberikan saran mitigasi kepada pengelola situs untuk mengurangi risiko keamanan. Pengujian ini juga dimaksudkan sebagai langkah pencegahan dini terhadap potensi masalah keamanan, sehingga dapat meminimalkan risiko peretasan data oleh pelaku siber yang berpotensi merugikan pihak hotel.

METODE

Jenis penelitian kami yang dilakukan adalah kualitatif yakni melakukan studi yang mendeskripsikan sesuatu berdasarkan masalah yang ada atau diidentifikasi mendeteksi tingkat celah keamanan dengan *tools Xspear*. Metode scanning dengan *Xspear* menjadi salah satu pendekatan sebagai media meningkatkan keamanan sistem yang dipantau dari level celah yang ditemukan. Adapun tahapan – tahapan yang akan dilakukan dalam pengujian ini yang sudah dipaparkan pada *flowchart* alur pelaksanaan penelitian dan akan dijelaskan metodenya secara deskriptif sesuai dengan yang ditampilkan pada gambar 1.



Gambar 1. *Flowchart* penelitian

Berdasarkan gambar 1, pada tahap awal, kami melakukan *reconnaissance* atau pengumpulan informasi yang relevan dari berbagai sumber seperti dari buku, artikel penelitian, dan sumber referensi pendukung lain (Sutabri, 2024). Dari semua sumber yang diperoleh untuk menjadi lingkup penelitian ini meliputi alamat IP:163.44.198.59, DNS:embryohotel.com, Server: NS1.Netdesignhost.COM(has1,519domains); NS2.Netdesignhost.com (has1,519domains), Bahasa Pemograman: PHP, Database MySQL.

Tahap berikutnya, instalasi *software* yang diperlukan dan menjadi pendukung dalam progress uji manual testing dan scanning kerentanan. Jika sudah disiapkan, Selanjutnya pemindaian Port pada website dengan tujuan mengetahui Port mana saja yang terbuka. Adapun tools yang digunakan ialah *ParamSpider* bertujuan untuk menggali parameter-parameter yang tersembunyi di arsip web tanpa diketahui dari *host* target, dan *tools Xspear* yang digunakan sebagai media scanning sistem untuk mengetahui tingkat atau level celah keamanan yang ditemukan pada website tersebut (Anwari et al., 2022).

Teknik analisis kerentanan sistem dilakukan dengan *tools Xspear*, penggunaan *tools* ini cukup mudah dengan memasukkan parameter yang akan discanning disertai *command* dari tools yang membantu untuk mendapatkan hasil yang maksimal, lalu akan tampil dalam bentuk tabel mengenai tingkat kerentanan apa saja yang didapat. Dengan pendekatan ini merupakan panduan bagi para pengembang dan tim keamanan untuk mengetahui kelemahan pada aplikasi web yang paling sering diserang (Evwiekpaefe et al., 2021). Dengan menginputkan alamat URL disertai command dari *Xspear*, sehingga memberikan informasi yang detail dan rinci dalam menemukan tingkat celah keamanan dengan pernyataan level keparahan yang dianalisa sehingga menjadi laporan bahwa ada celah keamanan yang berpotensi besar untuk dieksploitasi.

HASIL DAN PEMBAHASAN

Hasil

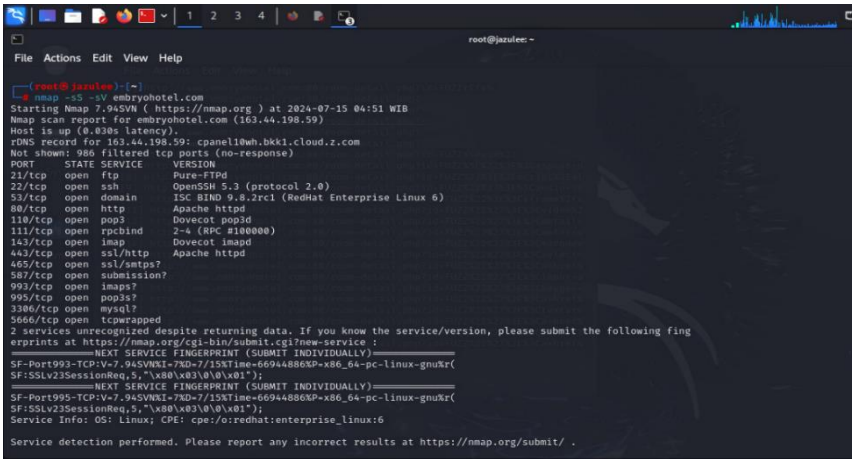
Reconnaissance bertujuan untuk mengumpulkan informasi yang detail terkait website yang ditargetkan sebagai bahan pendukung yang akan dimanfaatkan oleh pelaku cyber sebelum melakukan eksploitasi. Pada proses pengumpulan ini penulis menggunakan *Whois Lookup* untuk mengetahui domain, alamat IP, server serta informasi lainnya. Pada Tabel 1 menampilkan hasil temuan kami berupa informasi yang didapat terkait website yang menjadi target. Ini dilakukan dengan memasukkan domain name atau alamat IP pada menu search, lalu Whois akan memeriksa dan menampilkan informasi yang diperoleh dan sesuai. Data yang diperoleh yakni: domain (embryohotel.com), alamat IP (163.44.198.59), dan Server (NS1.netdesignhost.com (has 1,519 domains);NS2.netdesignhost.com (has 1,519 domains))

Tabel 1. Hasil dari *whois*

Tools		Hasil
Whois	Domain	embryohotel.com
	IP Address	163.44.198.59
	Server	NS1.netdesignhost.com (has 1,519 domains) NS2.netdesignhost.com (has 1,519 domains)

Pada gambar 2, telah dilakukan pemindaian port menggunakan tools Nmap untuk mengidentifikasi *port-port* yang terbuka pada website embryohotel.com. Pemindaian ini bertujuan untuk menganalisis keamanan jaringan dan memastikan bahwa tidak ada *port* yang rentan terhadap serangan dari luar. Dari hasil pemindaian tersebut, *port* yang terbuka ini dapat menjadi pintu masuk bagi ancaman keamanan jika tidak dikelola dengan baik. Oleh karena itu,

penting untuk memahami port mana saja yang terbuka dan mengapa mereka berada dalam kondisi tersebut.

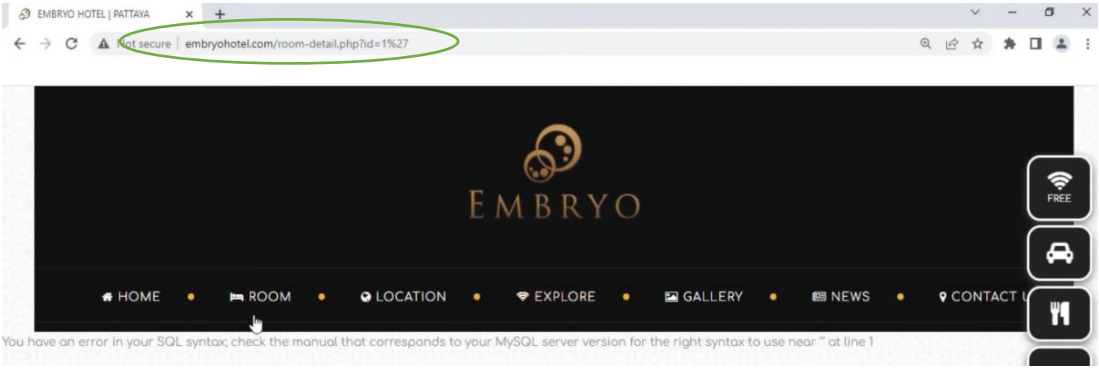


Gambar 2. Hasil pemindaian *port*

Tabel 2. Hasil *port* yang terbuka

Tools	**Hasil**		
	Port yang terbuka	Nama Layanan	Status
Nmap	21/tcp	ftp	*open*
	22/tcp	ssh	*open*
	53/tcp	domain	*open*
	80/tcp	http	*open*
	110/tcp	Pop3	*open*
	111/tcp	rpcbind	*open*
	143/tcp	Imap	*open*
	443/tcp	Ssl/http	*open*
	21/tcp	ftp	*open*

Tabel 2 menunjukkan bahwa hasil *port* pada website yang terbuka ada sekitar 8 *port* dengan *service* masing-masing. Dengan mengetahui informasi dari tabel 2, langkah selanjutnya adalah melakukan tindakan pencegahan dan pengamanan lebih lanjut. Ini termasuk menutup port yang tidak diperlukan atau memperkuat keamanan pada port yang harus tetap terbuka, guna melindungi website embryohotel.com dari potensi ancaman.

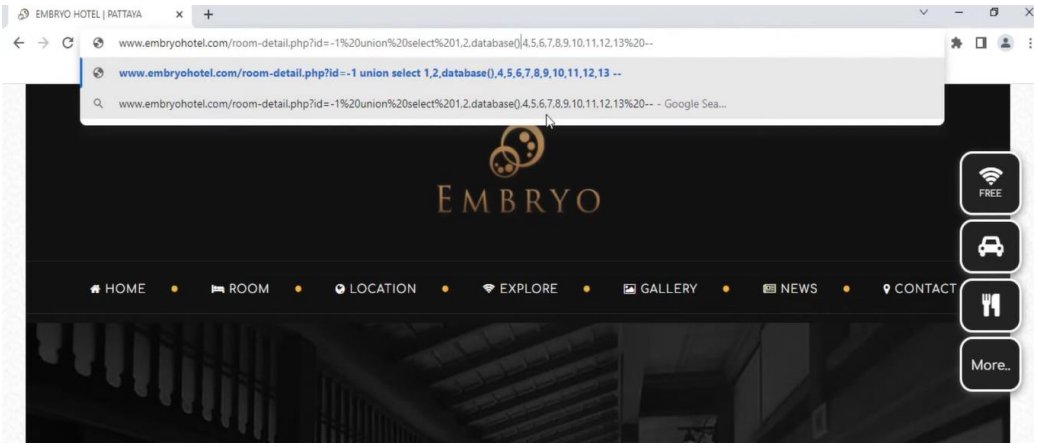


Gambar 3. Penambahan tanda petik

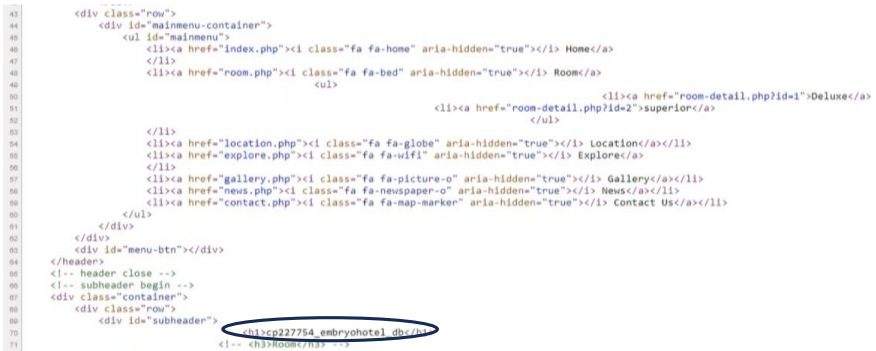
Setelah memperoleh informasi yang cukup terkait *website* hotel embryo, melakukan uji penetrasi manual SQL Injection pada URL website dengan memasukkan tanda petik (‘) di ujung “id=1”. Pengujian dilakukan untuk mengetahui adanya celah keamanan terhadap serangan SQL Injection atau normal seperti biasanya (aman). Setelah diuji, ternyata website tersebut error yang artinya tidak aman atau rentan. Metode yang kami merupakan cara simpel sebagai uji kelayakan suatu website dari injeksi SQL.

Pada gambar 3 menampilkan bentuk uji pentest menginjeksi dengan memberikan tanda petik pada URL *website*. Hasil nya dapat diketahui Ketika halaman website menjadi blank atau *error syntax* SQL sebagaimana yang terlihat hal ini menunjukkan bahwa *website* tersebut tidak aman sehingga mudah untuk melakukan serangan SQL Injection, tetapi jika *website* tidak memberikan respon artinya *website* tersebut aman dari injeksi SQL.

Percobaan SQL Injection secara manual dilakukan dengan menggunakan metode UNION *query*, yang merupakan salah satu teknik umum untuk mengeksploitasi kerentanan dalam basis data melalui injeksi SQL. Metode ini bertujuan untuk menyisipkan perintah SQL tambahan melalui input yang rentan, sehingga penyerang dapat menggabungkan hasil dari beberapa perintah SQL menjadi satu set data. Teknik ini memberikan peluang bagi penyerang untuk memanipulasi data yang diambil dari *server*, sehingga memungkinkan akses ke informasi sensitif.

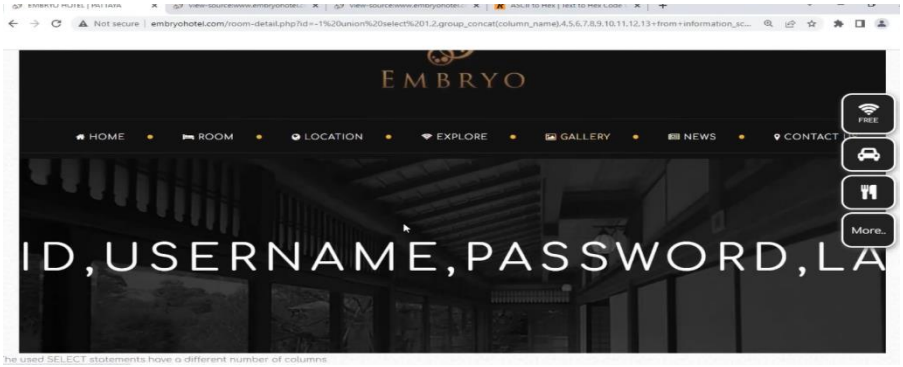


Gambar 4. Injeksi pada *database*

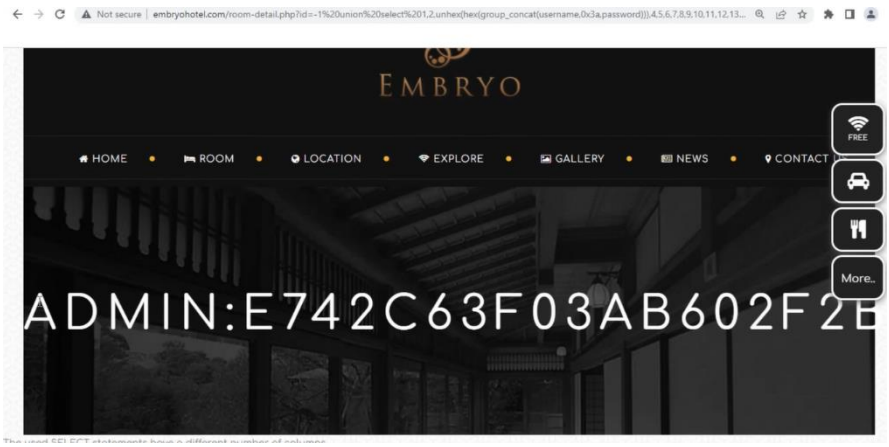


Gambar 5. Keterangan nama database pada sistem

Gambar 4 menampilkan bentuk injeksi SQL dengan memasukkan *database* pada format injeksi hyang dilakukan dengan tujuan untuk melihat *database* yang ada, lalu gambar 5 menunjukkan hasil dari pengujian *pen test* pada URL dalam mengetahui database apa yang ada di *website* tersebut, keterangan nama *database* dapat dilihat pada menu *view source* atau semacam inspect untuk melihat bahasa pemrograman serta data apa saja yang ada.

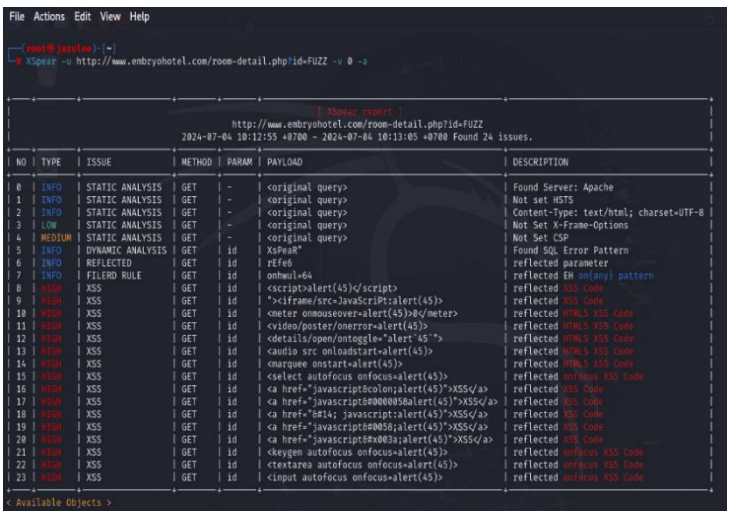


Gambar 6. Injeksi pada *username* dan *password*



Gambar 7. List *username* dan *password*

Pada gambar 6 menampilkan injeksi pada URL dengan memasukkan *username* dan password yang ada pada *website*, di mana kami mencari informasi yang tersimpan dalam kolom Admin. Dengan demikian, penulis dapat mengidentifikasi *username* dan *password*. Kemudian keterangan *username* dan *password* yang diketahui dapat dilihat pada gambar 7 yang menampilkan salah satu *user* yang diduga adalah admin dari *website* tersebut. Dan setelah melakukan uji pen test secara manual dan mengeksploit beberapa data yang perlu Pada tahap ini, kami melakukan scanning kerentanan pada parameter *website* dengan bantuan *tools Xspear* dan command pendukung yang disediakan agar memperoleh hasil yang diinginkan.



Gambar 8. Hasil *scanning dari xspear*

Pada gambar 8, dapat dilihat hasil dari *scanning vulnerability analyst* nya menunjukkan bahwa ditemukan celah keamanan dengan level *high* sekitar 15 *issue* dengan masing-masing payloadnya, 1 dengan *level low* dan 1 lagi *level medium*. Adanya celah kerentanan tersebut dapat berdampak serius karena menjadi peluang besar untuk diretas dan diserang oleh pelaku *cyber* hal ini menjadi laporan penting bagi admin dan penanggung jawab *website* agar lebih peduli dengan keamanan data guna menghindari serangan *cyber* yang dapat merugikan pihak organisasi jika dibiarkan terus menerus tanpa adanya tindakan lanjut.

Pembahasan

Hasil penelitian ini menunjukkan bahwa situs web www.embryohotel.com memiliki indikasi kerentanan keamanan yang teridentifikasi melalui uji penetrasi manual. Situs web ini dinyatakan tidak aman karena mengalami kesalahan (*error*) ketika karakter khusus, seperti tanda petik (') atau simbol lainnya, dimasukkan di ujung tautan URL. Temuan ini mengindikasikan potensi eksploitasi celah keamanan yang dapat berdampak signifikan terhadap integritas dan keamanan data pada situs tersebut. Dengan mengidentifikasi jenis serangan *SQL Injection* yang mungkin terjadi, penguji (*pentester*) dapat merancang serangan yang relevan untuk menguji tingkat keamanan situs web ini.

Apabila kerentanan ini tidak segera diperbaiki, data pribadi yang tersimpan di situs *Embrio Hotel* berisiko mengalami kebocoran, manipulasi, atau akses tidak sah, yang dapat menyebabkan dampak serius, seperti kehilangan data arsip yang bersifat privat, gangguan pada server web, dan peningkatan risiko kejahatan siber. Salah satu solusi yang disarankan adalah penggunaan layanan hosting dengan keamanan tinggi yang mendukung protokol HTTPS. HTTPS menyediakan enkripsi data menggunakan teknik SSL, yang dapat memastikan bahwa data yang dikirimkan tidak dapat dibaca meskipun berhasil disadap (Zabar & Novianto, 2015).

Pada proses evaluasi kerentanan, parameter situs web dianalisis, dan beberapa di antaranya ditemukan rentan. Hasil pengujian menggunakan *tool* Xspear, seperti yang ditunjukkan pada Gambar 10, mengidentifikasi kerentanan dengan status *HIGH*, yang mengindikasikan tingkat risiko keamanan yang serius. Hal ini menunjukkan bahwa parameter tersebut memiliki kelemahan signifikan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Oleh karena itu, disarankan untuk meningkatkan keamanan pada parameter-parameter ini dengan menerapkan prosedur perlindungan yang lebih kuat, seperti penggunaan enkripsi data.

Penelitian sebelumnya oleh Dasmen et al. (2023) juga menemukan kerentanan keamanan dengan tingkat *Medium* pada parameter "id". Namun, penelitian mereka menggunakan pendekatan berbeda, sehingga dalam penelitian kami dilakukan pengujian manual untuk mengidentifikasi fitur atau bagian tertentu yang rentan terhadap serangan. Selain itu, *tool Xspear* juga membantu mendeteksi masalah *Cross-Site Scripting* (XSS), seperti yang diilustrasikan pada Gambar 10. Kerentanan ini memungkinkan penyerang menyusupi dan mengeksploitasi data, yang pada akhirnya dapat meningkatkan risiko serangan siber lainnya.

SIMPULAN

Pengujian yang telah kami lakukan terhadapserangan Injeksi SQL dan XSS menjadi masalah serius di basis web aplikasi. Hasil uji manual *pentest* yang dilakukan pada *website* embryohotel menemukan bahwa ada celah Injeksi SQL menggunakan metode *GET* dengan memasukkan tanda petik (‘) pada bagian URL sehingga dapat dengan mudah mengakses data apa saja yang dimiliki dan berisiko diambil hak akses secara paksa oleh pelaku *cyber*. Dibantu oleh *tool Xspear* untuk *vulnerability scanning*, dapat diketahui bahwa ada celah keamanan dengan level *high* yang cukup banyak sehingga memberikan dampak serius bagi *website* terutama dibidang sekuriti atau keamanan data yang menjadi aset penting bagi hotel emrbyo.

REFERENSI

Allo, A. K., & Widiasari, I. R. (2024). Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *8*(2), 316-323. https://doi.org/10.35870/jtik.v8i2.1723

Andarini, R. Y., Hendradi, P., & Nugroho, S. (2023). Meningkatkan Keamanan Terhadap SQL Injection Studi Kasus Sistem Kepegawaian BNN. *Indonesian Journal of Business Intelligence (IJUBI)*, *6*(1), 34-42. https://doi.org/10.21927/ijubi.v6i1.3161

Anwari, Z. A., Wedana, I. G. P., Deva, J., Widyaputra, K. D. D., Saskara, G. A. J., & Listartha, I. M. E. (2022). Analisis Kerentanan Pada Suatu Website Menggunakan Tools Xspear, Xsscon, Dan Pwnxss. *Jurnal Informatika Teknologi Dan Sains*, *4*(4), 406–412. https://doi.org/10.51401/jinteks.v4i4.2104

Armadhani, A. P., Nofriansyah, D., & Ibnutama, K. (2022). Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *21*(2), 80. https://doi.org/10.53513/jis.v21i2.6119

Armando, R., Melyantara, I. G. A. K. A., Elfariani, R., Latuconsina, D. F. A., & Nasrullah, M. (2022). IT Support Website Security Evaluation Using Vulnerability Assessment Tools. *Journal of Information Systems and Informatics*, *4*(4), 949–957. https://doi.org/10.51519/journalisi.v4i4.330

Astriani, T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(4), 2041–2050. https://doi.org/10.35957/jatisi.v8i4.1232

Cahyo, M. N. (2022). Implementation of Search Engine Optimalization (SEO) on the Village-Owned Enterprises Luhur Sembada Website. *Edumatic: Jurnal Pendidikan Informatika*, *6*(2), 186-194. https://doi.org/10.29408/edumatic.v6i2.6259

Dasmen, R. N., Rasmila, R., Widodo, T. L., Kundari, K., & Farizky, M. T. (2023). Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard). *Jurnal Komputer Dan Informatika*, *11*(1), 91–95. https://doi.org/10.35508/jicon.v11i1.9809

Herawati, N., Budiyanto, V., & Uminingsih. (2023). Analisis Keamanan Sebuah Domain Menggunakan Open Web Application Security Project (OWASP) Zap. *Jurnal Teknologi Technoscientia*, *15*(2), 27–36. https://doi.org/10.34151/technoscientia.v15i2.4013

Laksono, A. T., & Santoso, J. D. (2021). Analysis of Website Security of SMKN 1 Pangandaran Against SQL Injection Attack Using OWASP Method. *The IJICS (International Journal of Informatics and Computer Science)*, *5*(2), 209. https://doi.org/10.30865/ijics.v5i2.3208

Nugraha, L. A., Kautsar, I. A., & Fitrani, A. S. (2024). SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web. *Smatika Jurnal*, *14*(01), 111–123. https://doi.org/10.32664/smatika.v14i01.1224

Pranata, E. J. (2023). Optimalisasi Keamanan Jaringan Komputer Pada Web E-Commerce Menggunakan Netfilter. *Cyber Security Dan Forensik Digital*, *6*(1), 18–24. https://doi.org/10.14421/csecurity.2023.6.1.2337

Pratama, I. P. A. E., & Wiradarma, A. A. B. A. (2019). Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(7), 8–12. https://doi.org/10.5815/ijcnis.2019.07.02

Ramadhan, R. S., Widjajarto, A., & Almaarif, A. (2022). Vulnerability Management Pada Vulnerable Docker Menggunakan Clair Scanner Dan Joomscan Berdasarkan Standar GSA CIO-IT Security-17-80. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *4*(1),

85-93. https://doi.org/10.30865/json.v4i1.4789

Riyanti, A., Rahmanto, B. M., Hardianto, D. R., Yuristiawan, R. D. A., & Setiawan, A. (2024). Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap. *Journal of Internet and Software Engineering*, *1*(4), 1-9. https://doi.org/10.47134/pjise.v1i4.2623

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Sri Arsa, D. M. (2020). Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city). *International Journal of Computer Network and Information Security*, *12*(4), 30–40. https://doi.org/10.5815/ijcnis.2020.04.03

Sansena, Y., & Samsudin, S. (2023). Aplikasi Perhitungan Penyusutan Inventaris Barang menggunakan Decreasing Charge Method Berbasis Website. *Edumatic: Jurnal Pendidikan Informatika*, *7*(1), 169-177. https://doi.org/10.29408/edumatic.v7i1.17572

Soewoeh, C. A. J., Tenda, E., Ketaren, E., Kalengkongan, W. W., & Takaendengan, M. I. (2023). Analisa Kerentanan Website Fmipa Unsrat Berdasarkan Open Web Application Security Project Top 10 Framework. *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, *2*(2), 137–143. https://doi.org/10.33365/jecsit.v2i2.251

Suhaila, D., Muhammad Karim Bachtiar, & Tedi Kurniawan. (2024). Ananlisis Vulnerabilitas dan Pengujian Terhadap Google Gruyere. *Journal of Internet and Software Engineering*, *1*(3), 1-10. https://doi.org/10.47134/pjise.v1i3.2574

Sutabri, T., Wijaya, A., Herdiansyah, M. I., & Negara, E. S. (2024). Evaluasi Risiko Celah Keamanan Aplikasi E-Office menggunakan Metode OWASP. *Edumatic: Jurnal Pendidikan Informatika*, *8*(1), 113-122. https://doi.org/10.29408/edumatic.v8i1.25463

Zabar, A. A., & Novianto, F. (2015). Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux. *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, *4*(2), 69–74. https://doi.org/10.34010/komputa.v4i2.2427

Zirwan, A. (2022). Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi Dan Teknologi*, *4*(1), 70–75. https://doi.org/10.37034/jidt.v4i1.19