Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 777 - 792

PEMINDAI KERENTANAN APLIKASI WEB DINAS KEARSIPAN DAN PERPUSTAKAAN DAERAH KABUPATEN SEMARANG MENGGUNAKAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)

Muhammad Fauzan Rifqi[1], Oris Krianto Sulaiman[2], Aulia Ichsan[3]
Fakultas Teknik Universitas Islam Sumatera Utara[1,2,3]
Email: m.fauzan1004@gmail.com

Informasi

Volume : 2
Nomor : 7
Bulan : Juli
Tahun : 2025
E-ISSN : 3062-9624

Abstract

Dalam era digital saat ini, website instansi pemerintah menjadi media utama dalam menyampaikan informasi kepada masyarakat. Namun, peningkatan penggunaan teknologi juga dibarengi dengan meningkatnya ancaman siber. Penelitian ini bertujuan untuk mengidentifikasi dan menguji kerentanan keamanan pada website Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang dengan fokus terhadap serangan SQL Injection dan Cross-Site Scripting (XSS). Penelitian menggunakan metode Information System Security Assessment Framework (ISSAF) yang meliputi tahap planning, assessment, dan reporting. Proses pengujian dilakukan dalam lingkungan terkendali menggunakan berbagai tools seperti WhatWeb, WHOIS, NMAP, Arachni, dan SQLMap. Hasil penelitian menemukan lima kerentanan, di antaranya empat dengan tingkat risiko tinggi dan satu berisiko rendah. Dua di antaranya berhasil dieksploitasi, yaitu SQL Injection dan XSS Reflected. Temuan ini menunjukkan bahwa website tersebut masih rentan terhadap serangan siber dan memerlukan perbaikan keamanan segera. Penelitian ini juga memberikan rekomendasi mitigasi untuk setiap kerentanan yang ditemukan guna meningkatkan perlindungan sistem.

Kata Kunci: *Budaya Organisasi, Motivasi Kerja, Lingkungan Kerja Fisik, Kinerja Pegawai*

A. PENDAHULUAN

Dalam era digitalisasi, aplikasi web merupakan alat utama yang digunakan pemerintah Indonesia untuk mengelola informasi secara digital yang tujuannya untuk memberikan layanan kepada masyarakat. Dengan adanya website masyarakat dapat mengakses dan menerima informasi dengan cepat dan efisien, seperti berita, layanan pengaduan, dan informasi publik lainnya.

Dinas Kearsipan dan Perpustakaan Daerah Kabupatan Semarang melalui laman web nya mempunyai peran penting dalam menyampaikan informasi publik seperti kegiatan dan program literasi, arsip dan perpustakaan, layanan digital dan, berita terkini, sehingga masyarakat dapat mengakses informasi yang dikeluarkan dengan cepat dan efisien.

Namun, seiring dengan berkembangnya teknologi informasi terdapat juga ancaman siber yang makin berkembang dari masa ke masa. Berdasarkan data milik Badan Siber dan Sandi Negara (BSSN) hasil penelusuran pada darknet, ditemukan adanya 56.128.160 temuan data exposure yang berdampak pada 461 stakeholder di Indonesia. Pada kasus web defacement ditemukan sebanyak 5.780 yang menargetkan beberapa domain dan sebanyak 4.071 web defacement terkait judi online yang menargetkan situs pemerintah(BSSN, 2024). Temuan ini menunjukkan bahwasannya situs web pemerintah pun sangat rentan terhadap segala bentuk serangan siber, termasuk 2 diantara serangan yang paling umum yaitu SQL Injection dan Cross Site Scripting (XSS).

Salah satu teknik umum di dunia cyber crime yaitu SQL Injection. Sebagian besar aplikasi modern menggunakan basis data yang persisten untuk meneruskan informasi. Serangan injeksi terjadi ketika seseorang dengan sengaja mengirimkan perintah SQL berbahaya ke server database melalui saluran yang ilegal. Saluran yang paling umum digunakan untuk serangan ini adalah input data yang tidak divalidasi. SQL Injection adalah kerentanan yang terjadi karena input pengguna tidak divalidasi dengan baik, dan ini adalah salah satu metode serangan yang umumnya digunakan dalam aplikasi web (Riyanti dkk., 2024)

Penetration testing adalah sub kategori dari ethical hacking yaitu sebuah metode dan prosedur yang bertujuan untuk menguji dan melindungi keamanan informasi. Penetration testing merupakan aktifitas mengevaluasi sistem keamanan yang sudah dibuat dengan cara melakukan simulasi serangan menggunakan metode yang biasa digunakan oleh peretas. Kegiatan ini perlu mendapat persetujuan legal dari pemilik sistem tersebut. Seperti halnya sekarang sedang terjadi pembobolan maupun hacking pada perusahaan maupun website tertentu yang mengakibatkan kerugian pada pihak yang bersangkutan. Data tersebut dijual dan disalahgunakan oleh pihak yang tidak berwajib dan diperjualbelikan untuk kepentingan sendiri. (Widi Linggih Jaelani dkk., 2023).

Information System Security Assessment Framework (ISSAF) merupakan salah satu metode pemindai kerentanan atau penetration testing yang umum digunakan peniliti keamanan siber untuk menguji, serta menilai keamanan dari sebuah teknologi sistem

informasi. Dengan menggunakan metode ini peneliti dapat menilai suatu keamanan sistem informasi secara terstruktur dan sistematis.

Dalam skripsi ini, penulis menggunakan Information System Security Assessment Framework (ISSAF) sebagai pendekatan sistematis untuk mendeteksi kerentanan serta melakukan pengujian keamanan terhadap aplikasi web Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang. Fokus utama dalam pengujian ini adalah mendeteksi adanya kemungkinan kerentanan terhadap SQL Injection dan XSS, di mana serangan XSS dan SQL Injection termasuk diantara serangan yang paling berbahaya (Anugrah, 2024).

Untuk mendukung penelitian ini, penulis juga melakukan kajian terhadap beberapa penelitian terdahulu yang berkaitan dengan uji penetrasi website diantara lain penelitian oleh (Mu'min dkk., 2024) yaitu menguji sebuah website yang diklaim tidak memiliki kerentanan SQL menggunakan metode injeksi SQL. Penelitian oleh (Kushardianto dkk., 2024) yang melakukan uji penetrasi terhadap website udacoding pada kegiatan pengabdian masyarakat. Penelitian (Faizi dkk., 2023) melakukan pengujian kerentanan pada website Universitas Singaperbangsa Karawang menggukan metode Penetration Execution And Standart (PTES).

Berdasarkan latar belakang yang telah diuraikan, penelitian ini dirumuskan untuk menjawab bagaimana penerapan metode Information System Security Assessment Framework (ISSAF) dengan penetration testing terhadap website Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang, apa saja jenis celah keamanan yang ditemukan, serta rekomendasi mitigasi yang diperlukan untuk meningkatkan keamanan sistem. Agar pembahasan lebih terarah, penelitian ini dibatasi hanya pada pengujian website Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang dengan URL https://arpusda.semarangkab.go.id/, fokus pada kerentanan SQL Injection dan Cross-site Scripting (XSS), serta menggunakan 4 dari 8 tahapan dalam metode ISSAF. Penelitian ini bertujuan untuk menerapkan metode ISSAF dalam melakukan penetration testing pada website tersebut, mengidentifikasi dan menilai celah keamanan SQL Injection serta XSS, serta memberikan rekomendasi mitigasi guna memperkuat sistem.

B. METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan berbagai alat dan bahan untuk mendukung proses pengujian dan penulisan skripsi. Dari sisi perangkat keras, digunakan sebuah laptop dengan spesifikasi AMD Ryzen 7 5700U 1.8 GHz, RAM 16 GB DDR4, dan penyimpanan 1 TB. Sedangkan untuk perangkat lunak, digunakan sistem operasi Windows 11 64-bit, Kali Linux melalui VM Ware Workstation serta Windows Subsystem Linux, web browser Brave, dan alat bantu scanner kerentanan seperti Arachni. Metode pengumpulan data dilakukan dengan studi literatur untuk mengumpulkan referensi terkait keamanan sistem informasi, observasi langsung pada website Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang, serta dilanjutkan dengan pengujian menggunakan metode Information System Security Assessment Framework (ISSAF). Roadmap penelitian meliputi tahapan information gathering dengan WHOIS dan Whatweb untuk mengumpulkan informasi target, mapping network menggunakan NMAP untuk port scanning dan identifikasi firewall, vulnerability identifying memakai Arachni dan manual testing, hingga penetration untuk mengeksploitasi kerentanan SQL Injection dan XSS dengan SQLMAP dan metode manual.

Adapun tahapan rinci penelitian dimulai dari tahap perencanaan penetration testing, permohonan dan persetujuan izin ke pihak terkait, formulasi masalah serta tujuan, dilanjutkan assessment dengan empat tahapan ISSAF (information gathering, mapping network, identifying vulnerabilities, dan penetration). Hasil pengujian ini kemudian dilaporkan dalam bentuk analisis risiko dan rekomendasi mitigasi. Untuk pemindaian detail, digunakan Whatweb untuk mendeteksi teknologi website, WHOIS untuk mendapatkan informasi domain, NMAP untuk pemetaan jaringan, Arachni untuk memindai kerentanan web, SQLMAP untuk menguji SQL Injection, serta uji manual XSS dengan menyisipkan payload pada kolom input website. Semua tahapan diakhiri dengan dokumentasi hasil pengujian dalam laporan lengkap untuk memberikan gambaran risiko keamanan dan solusi mitigasi yang diperlukan.

C. HASIL DAN PEMBAHASAN

Hasil

Hasil dari tahapan pengujian yang dilakukan untuk mencari kerentanan serta melakukan penetrasi terhadap kerentanan yang ditemukan pada aplikasi *web* Dinas Kearsipan dan

Perpustakaan Daerah Kabupaten Semarang menggunakan metode *ISSAF*. Tahapan pengujian meliputi proses pengumpulan informasi dari target yang akan diuji (*Information Gathering*), pemetaan jaringan (*Mapping Network*), mengidentifikasi kerentanan (*Vulnerability Identifying*), serta melakukan pengujian eksploitasi terhadap celah keamanan yang ditemukan (*Penetraion*).

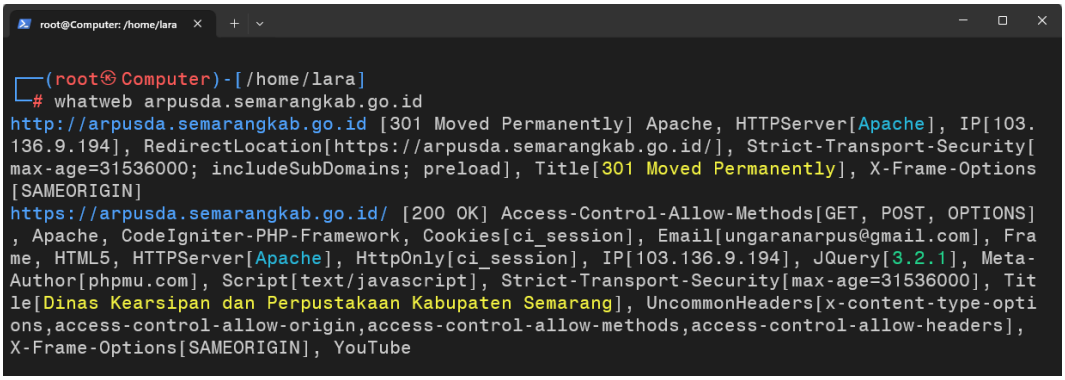
Pembahasan

Information Gathering

Pada tahap *Information Gathering* penulis akan mengumpulkan seluruh informasi mengenai sistem aplikasi *web* Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang yang tersedia di internet. *Information Gethering* menggunakan 2 *tools* sebagai berikut:

WHATWEB

Pengujian menggunakan *tool WHATWEB* dilakukan untuk memindai jenis teknologi *web* yang digunakan oleh sebuah situs.

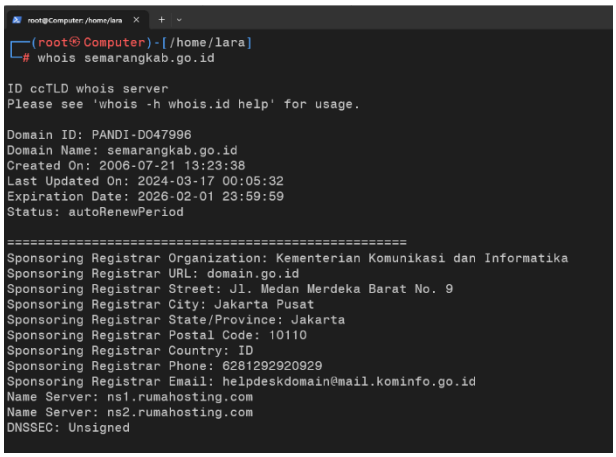


Gambar 1 *WHATWEB*

Dari hasil pemindaian menggunakan *whatweb* penulis memperoleh informasi sebagai berikut ; (a) *IP Address* dari server yaitu 103.136.9.194, (b) *HTTPServer* yang digunakan adalah *Apache, (c)* Versi dari JQuery yaitu 3.2.1, di mana JQuery ini merupakan *library* dari *JavaScript, (d)* Penulisan *script* menggunakan *JavaScript, (e) Website* yang dibangun menggunakan *CodeIgniter-PHP-Framework.*

WHOIS

Sama halnya dengan *whatweb*, *whois* juga *tool open-source* yang fungsinya untuk memindai informasi terkait kepemilikan, organisasi, alamat, tanggal pendaftaran dari *DNS (Domain Name System)*.

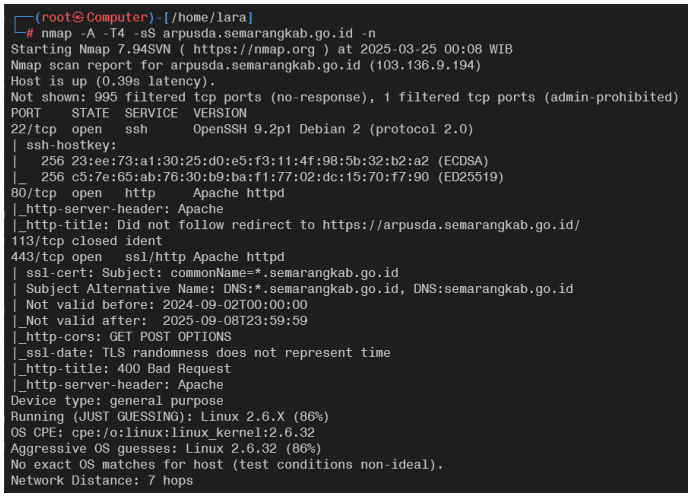


Gambar 2 *WHOIS*

Dengan menggunakan *whois* penulis memperoleh informasi *domain* dari https://arpusda.semarangkab.go.id sebagai berikut : (a) *Domain* yang digunakan adalah semarangkab.go.id, (b) *Domain* dibuat pada tanggal : 21-07-2006, (c) *Domain* terakhir kali diperbarui pada tanggal : 17-03-2024, (d) Menggunakan rumahhosting sebagai layanan *web hosting.*

Mapping Network

Pada tahap *Mapping Network* penulis akan menggali informasi di sisi jaringan yang berkaitan dengan server target yang diuji. Pada tahapan ini informasi yang diperoleh bisa berupa *IP Address*, *Port* jaringan yang terbuka, mendeteksi jenis *firewall* , serta Sistem Operasi yang digunakan oleh *server*. Untuk pengujian pada tahap ini penulis menggunakan *tool NMAP*.



Gambar 3 *NMAP*

Tabel 1 *Service server*

NO	*Ports*	Protokol	Status	*Service*
1.	22	*TCP*	*OPEN*	*SSH*
2.	80	*TCP*	*OPEN*	*HTTP*
3.	113	*TCP*	*CLOSED*	-
4.	443	*TCP*	*OPEN*	*HTTPS*

Gambar 4 *Firewall Identification*

Hasil dari pengujian untuk mengetahui jenis *firewall* yang digunakan dapat dilihat pada gambar 4.4 yang menunjukkan bahwa aplikasi *web* yang diuji tidak menerapkan konfigurasi *firewall* sama sekali.

Vulnerability Identifying

Pada tahap *Vulnerability Identifying* (identifikasi kerentanan) penulis menggunakan *automatic tools arachni* yang akan secara otomatis memindai serta mencari celah keamanan yang mungkin bisa dimanfaatkan untuk tujuan yang tidak baik. Hasil pemindai kerentanan dapat dilihat pada tabel 2.

Tabel 2 Hasil pemindaian menggunakan Arachni

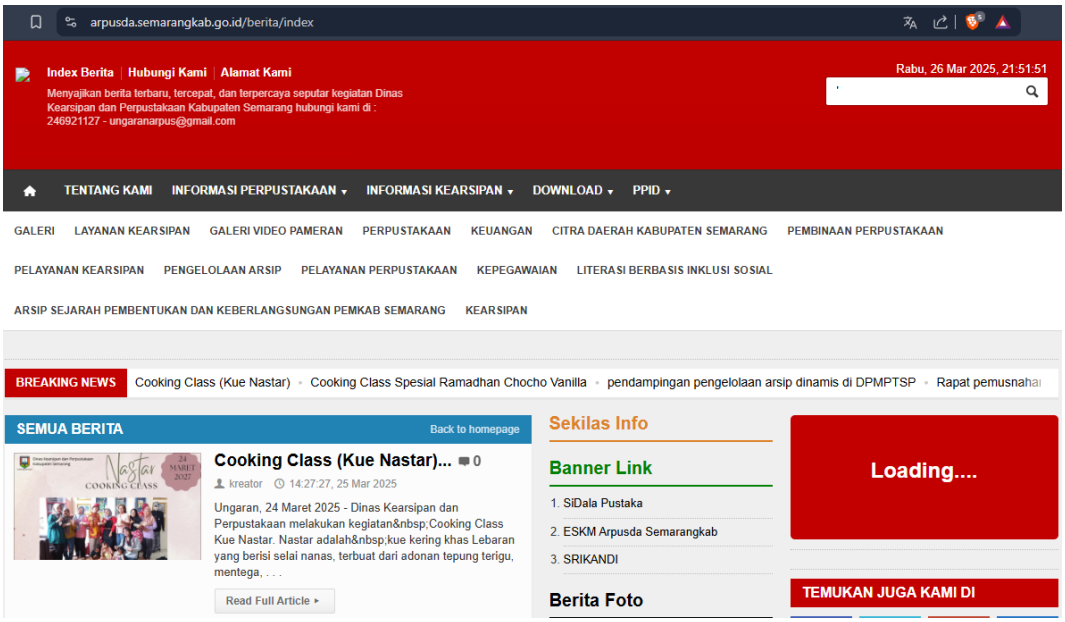
NO	Jenis Celah Keamanan	Deskripsi	Tingkat Ancaman	Dampak
1.	*Access restriction bypass via origin spoof*	Teknik serangan di mana penyerang dapat melewati pembatas akses pada aplikasi *web* dengan	*High*	Pencurian data sensitif, akses tidak sah ke *API*, dimanafaatkan untuk menjalankan serangan *CSRF* dan *XSS*

NO	Jenis Celah Keamanan	Deskripsi	Tingkat Ancaman	Dampak
		memalsukan *header origin* dalam permintaan *HTTP*		
2.	*SQL Injection*	Jenis kerentanan yang dimanfaatkan oleh penyerang untuk menyisipkan perintah *SQL* ke dalam kueri basis data aplikasi	*High*	Pencurian data sensitif, modifikasi atau penghapusan data, eksekusi perintah sistem,
3.	*Cross-Site Scripting (XSS)*	Jenis kerentanan yang memungkinkan penyerang bisa menyisipkan *script* berbahaya ke dalam halaman *web* yang dapat dilihat oleh pengguna lain	*High*	Mencuri data *user* , mengambil alih sesi, melakukan *deface* ,mengarahkan pengguna ke situs yang berbahaya.
4.	*Cross-Site Request Forgery*	Jenis kerentanan yang digunakan untuk menipu korban agar menjalankan aksi yang tidak diinginkan pada aplikasi *web*	*High*	Transfer dana tanpa izin, perubahan (*email*, *password*), pengambilan alih akun.
5.	*Missing 'X-Frame-Options' header*	Aplikasi *web* tidak menyertakan *header X frame option* di dalam respon *HTTP.*	*Low*	Pengguna bisa ditipu untuk melakukan aksi yang berbahaya tanpa sadar, pencurian informasi sensitif.

Penetraion **(Eksploitasi Kerentanan)**

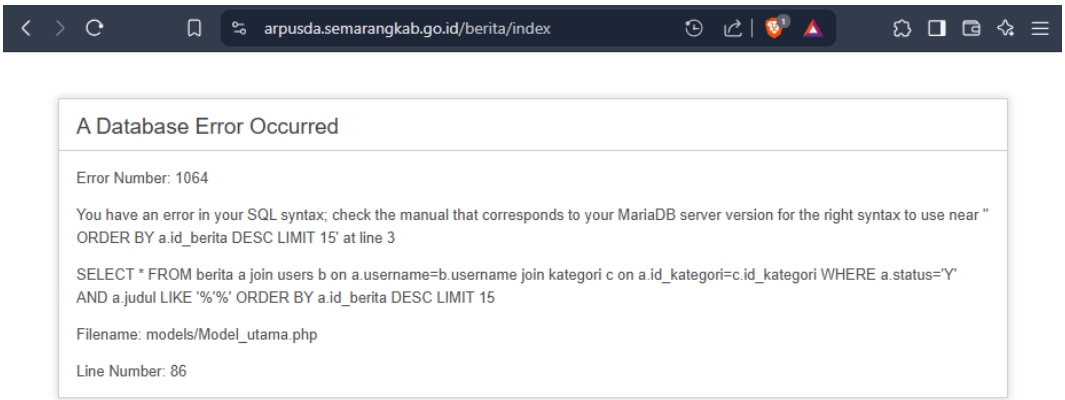
Pada tahap *penetration* akan dilakukan pengujian celah kerentanan yang ditemukan berdasarkan hasil dari *Vulnerability Identifying* pada tahapan sebelumnya terhadap target yang diuji. Adapun 2 dari 5 kerentanan yang akan diuji sebagai berikut :

SQL Injection



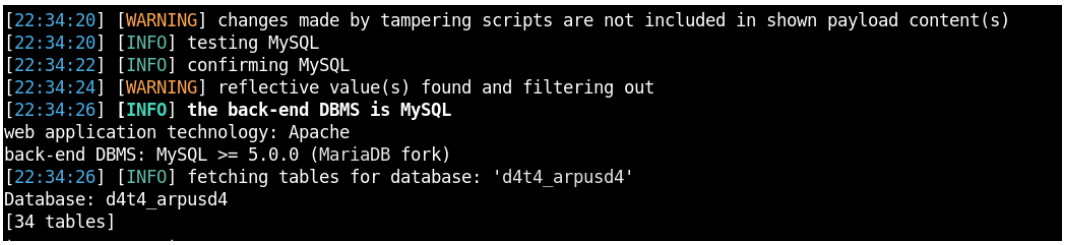
Gambar 5 Laman *Web* Arpusda

Untuk memastikan celah kerentanan ini valid terhadap serangan *SQL Injection* peneliti menginputkan karakter ‘ (kutip satu / *single quote*) di kolom pencarian, karena karakter ini di dalam *query SQL* digunakan untuk membungkus nilai *string*. Jika *input* tidak divalidasi dengan baik maka karakter ini bisa dimanfaatkan untuk mengeksploitasi kerentanan *SQL injection*.



Gambar 6 *Error massage*

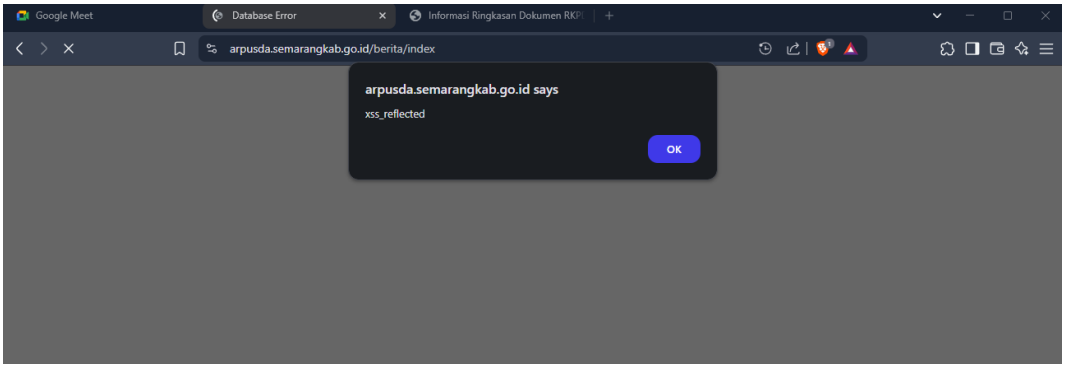
Selanjutnya akan tampil *error message* yang menunjukkan bahwa adanya kesalahan dalam perintah *SQL* yang dieksekusi oleh aplikasi.Karena menampilkan pesan *error* seperti pada gambar 4.5 kerentanan *SQL injection* ini termasuk ke dalam kategori *error-based sqli*.



Gambar 7 *SQLMAP*

Selanjutnya penulis menggunakan *tool sqlmap* seperti pada gambar 4.7 yang menunjukan bahwa kerentanan *sql injection* berhasil dieksploitasi dan menampilkan jumlah *table* dari salah satu *database*.

Cross-Site Scripting (XSS)



Gambar 8 *XSS*

Kerentanan *cross-site scripting (xss)* yang terdapat pada laman *web* berhasil dieksploitasi seperti pada gambar 4.7. Ini termasuk ke dalam jenis kerentanan *xss reflected* yang artinya skrip yang disisipkan dapat dipantulkan kembali oleh *server* dalam respon terhadap permintaan user. Pada eksploitasi ini peneliti menyisipkan skrip sebagai berikut : <script>alert('xss_reflected')</script> yang akibatnya laman *web* menampilkan *pop up* yang berisi pesan *alert*.

Hasil Pengujian

Pelaporan

Pada tahap pelaporan semua data dari hasil pengujian yang sudah dilakukan kemudian dikumpulkan menjadi sebuah laporan. Adapun detail laporan terhadap pengujian pada *website* Dinas Kearsipan dan Perpustakaan Daerah Kab.Semarang sebagai berikut :

Hasil pengumpulan data melalui pemindaian menggunakan tool whatweb dapat dilihat pada tabel 3

Tabel 3 Hasil *Scanning whatweb*

NO	Informasi	Keterangan
1.	*IP Address*	103.136.9.194
2.	*HTTP server*	*Apache*
3.	*Framework*	*CodeIgniter-PHP-Framework*
4.	Bahasa&*Library*	*Javascript, jQuery* v.3.2.1
5.	*HTML version*	*HTML*5
6.	*Cookies*	*Ci_session*
7.	Meta *author*	Phpmu.com

Hasil pengumpulan data melalui pemindaian menggunakan tool whois dapat dilihat pada tabel 4

Tabel 4 Hasil *Scanning whois*

NO	Informasi	Keterangan
1.	*Domain Name*	semarangkab.go.id
2.	Tanggal Registrasi	21 Juli 2006
3.	Terakhir diperbaharui	17 Maret 2024
4.	Tanggal Berakhir	1 Februari 2026
5.	Layanan	rumahhosting.com

Hasil pengumpulan informasi jaringan menggunakan tool NMAP dapat dilihat pada tabel 5

Tabel 5 Hasil *Scanning NMAP*

NO	Informasi	Keterangan
1.	*Port* : 22 (TCP) 80 (TCP) 113(TCP) 443(TCP)	 *Open/SSH* *Open/HTTP* *Closed/-* *Open/HTTPS*
2.	*Operating System*	Linux

3.	*Network Distance*	7 hops
4.	*Firewall*	*Not Present*

Hasil scanning kerentanan menggunakan tool arachni dapat dilihat pada tabel 6

Tabel 6 Hasil *Scanning Arachni*

NO	Jenis Kerentanan	Level Kerentanan
1.	*Access restriction bypass via origin spoof*	*High*
2.	*SQL Injection*	*High*
3.	*Cross-Site Scripting (XSS)*	*High*
4.	*Cross-Site Request Forgery*	*High*
5.	*Missing 'X-Frame-Options' header*	*Low*

Hasil *scanning* kerentanan menggunakan *tool* arachni memperoleh 5 jenis kerentanan dengan 4 jenis kerentanan yang memiliki level *high* dan 1 kerentanan dengan level *low*.

Eksploitasi kerentanan berhasil dilakukan untuk jenis kerentanan *SQL injection* dan *Cross-Site Scripting (XSS)* yang keduanya memiliki level kerentanan *high*. Untuk jenis kerentanan *SQL injection* eksploitasi yang dilakukan sampai tahap menampilkan daftar tabel dari *database* yang digunakan, selain itu untuk jenis kerentanan *Cross-Site Scripting* eksploitasi dengan *payload* <script>alert('xss_reflected')</script> yang diinput pada kolom pencarian berhasil dijalankan.

Langkah mitigasi yang dapat dilakukan untuk mengurangi terjadinya serangan siber dikemudian hari dapat dilihat pada tabel 7

Tabel 7 Langkah Mitigasi

NO	Jenis Kerentanan	Level	Langkah Mitigasi
1.	*Access restriction bypass via origin spoof*	*High*	Menambahkan token *CSRF* sebagai proteksi keamanan
2.	*SQL Injection*	*High*	Validasi *input* pengguna, filter karakter seperti '(*single quote*), "(*double quote*), ;(titik koma).
3.	*Cross-Site Scripting (XSS)*	*High*	Gunakan *output encoding* pada setiap data pengguna

			yang ditampilkan, filter karakter (<,>,") pada input pengguna.
4.	*Cross-Site Request Forgery*	*High*	Gunakan token *CSRF*, membatasi sesi dengan *time-out* ketat.
5.	*Missing 'X-Frame-Options' header*	*Low*	Menambahkan *header http X-Frame-Options: SAMEORIGIN* untuk mencegah *clickjacking*.

D. KESIMPULAN

Berdasarkan hasil pengujian serta pembahasan yang dimuat pada BAB sebelumnya dapat ditarik kesimpulan bahwa :

1) Aplikasi web milik Dinas Kearsipan dan Perpustakaan Daerah Kab.Semarang masih rentan terhadap serangan siber, berdasarkan hasil pengujian penetrasi, terdapat 5 jenis kerentanan di mana 4 kerentanan memiliki tingkat ancaman high dan 1 jenis kerentanan dengan tingkat ancaman low
2) Metode Information System Security Assessment Framework berhasil digunakan sebagai panduan untuk melakukan pengujian secara sistematis, dari tahap perencanaan, pengumpulan informasi, pemetaan jaringan, dan eksploitasi celah kerentanan yang ditemukan.
3) Hasil pengujian menunjukkan bahwa terdapat 2 kerentanan diantaranya SQL Injection error based yang kemudian berhasil dieksploitasi hingga menampilkan struktur basis data, dan kerentanan Cross Site Scripting reflected yang berhasil dieksekusi dengan payload yang sederhana.
4) Aplikasi web yang diuji masih menggunakan teknologi yang umum tanpa hardening tambahan seperti input validation atau pengaturan header keamanan HTTP.

E. DAFTAR PUSTAKA

Ade Gustiyonoo, Irawadi Alwi, E., & Mubarak Abdullah, S. (2024). Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing. Cyber Security dan Forensik Digital, 7(1), 25–33. https://doi.org/10.14421/csecurity.2024.7.1.4432

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web Application Penetration Testing Using SQL Injection Attack. JOIV : International Journal on Informatics Visualization, 5(3), 320. https://doi.org/10.30630/joiv.5.3.470

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

Azwan, M., Adriansyah, A. F., & Fauzan, M. R. A. (2022). PROTOKOL SECURE SOCKET LAYER UNTUK KEAMANAN BERBASIS WEB. 1.

Beranda—OWASP Top 10:2021. (n.d.). Retrieved December 17, 2024, from https://owasp.org/Top10/id/

BSSN, B. (2024). Lanskap Keamanan Siber 2024. Badan Siber dan Sandi Negara (BSSN).

Charly, P., Diatmika, K. E., Prayoga, I. M. P., & Listartha, I. M. E. (2022). Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS. Format : Jurnal Ilmiah Teknik Informatika, 11(1), 77. https://doi.org/10.22441/10.22441/format.2022.v11.i1.008

Faizi, Z., Ridha, A. A., Waluyo, J. H. R., Timur, T., & Barat, J. (2023). ANALISIS WEB SECURITY HOLE MENGGUNAKAN METODE PENETRATION TESTING EXECUTION AND STANDARD (STUDI KASUS : UNIVERSITAS SINGAPERBANGSA KARAWANG). 11(2).

Handayani, A., Apriliani, E., Padrisi, Z., Sugiartha, R. A., Adzhim, M. A., Muhammad, F., Wicaksono, T., Saputro, F. A., & Faridzi, A. (2023). Implementasi Sistem Keamanan Komputer Host Menggunakan Sistem Operasi Fedora Linux.

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). Jurnal Algoritma, 18(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

Kushardianto, N. C., Sari, F. W., Haikal, A., & Idris, M. (2024). Penetrasi Testing Aplikasi Website Udacoding. Jurnal Pengabdian kepada Masyarakat Politeknik Negeri Batam, 5(2), 203–218. https://doi.org/10.30871/abdimaspolibatam.v5i2.7235

Manuhutu, M. A. (2021). Sistem Informasi Promosi Tempat Wisata Di Kota Sorong Berbasis Website (Kasus: Kawasan Wisata Mangrove Klawalu). 5.

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR). Jurnal Informatika Teknologi dan Sains, 4(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mu'min, M. A., Alamin, Z., Fathir, & Ramadhan, S. (2024). Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Website XYZ menggunakan Tools SQLMap. Scientific : Journal of Computer Science and Informatics, 1(2), 47–52. https://doi.org/10.34304/scientific.v1i2.330

Nurbojatmiko, N., Karimiyah, M. S. K., Asnadi, N. M., & Anisyah, R. (2025). ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review. Sinkron, 9(1), 484–492. https://doi.org/10.33395/sinkron.v9i1.14448

Prasetyo, P., & Alimyaningtias, W. N. (2024). ANALISIS PERBANDINGAN METODE PTES DAN ISSAF SEBAGAI UJI KEAMANAN ROUTER DI ZURICH HOTEL BALIKPAPAN.

Putranto, D. P., Jayanta, J., & Hananto, B. (2022). Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack. Informatik : Jurnal Ilmu Komputer, 18(3), 230. https://doi.org/10.52958/iftk.v18i3.4690

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), 9. https://doi.org/10.47134/pjise.v1i4.2623

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), 113.

https://doi.org/10.24843/JIM.2020.v08.i02.p05

Saputra, A. K., & Fahrizal, M. (2021). RANCANG BANGUN BERBASIS WEB CRM (CUSTOMER RELATIONSHIP MANAGEMENT) BERBASIS WEB STUDI KASUS PT BUDI BERLIAN MOTOR HAJIMENA BANDAR LAMPUNG. 17.

Vakhula, O., Kurii, Y., Opirskyy, I., & Susukailo, V. (2024). Security-as-Code Concept for Fulfilling ISO/IEC 27001:2022 Requirements.

Widi Linggih Jaelani, Yanto, Y., & Khoirunnisa, F. (2023). PENETRATION TESTING WEBSITE DENGAN METODE BLACK BOX TESTING UNTUK MENINGKATKAN KEAMANAN WEBSITE PADA INSTANSI (REDACTED). Naratif : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika, 5(1), 1–8. https://doi.org/10.53580/naratif.v5i1.180

Yulia Andarini, R., Hendradi, P., & Nugroho, S. (2023). MENINGKATKAN KEAMANAN TERHADAP SQL INJECTION STUDI KASUS SISTEM KEPEGAWAIAN BNN. Indonesian Journal of Business Intelligence (IJUBI), 6(1). https://doi.org/10.21927/ijubi.v6i1.3161

Zalukhu, A., Purba, S., & Darma, D. (2023). PERANGKAT LUNAK APLIKASI PEMBELAJARAN FLOWCHART. 4(1).