

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

**SKRIPSI**

Oleh

MUHAMMAD FAUZAN RIFQI

71210915053



**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS ISLAM SUMATERA UTARA**

**2025**

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

*Assalamu'alaikum Warahmatullahi Wabarakatuh*

Alhamdulillah, segala puji dan syukur kepada kehadiran Allah SWT atas limpahan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul **“PEMINDAI KERENTANAN APLIKASI *WEB* DINAS KEARSIPAN DAN PERPUSTAKAAN DAERAH KABUPATEN SEMARANG MENGGUNAKAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)*”** sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Program Studi Informatika Fakultas Teknik Universitas Islam Sumatera Utara.

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa tidak mungkin terselesaikan tanpa adanya bantuan, dukungan, bimbingan, dan nasehat dari berbagai pihak. Pada kesempatan ini penulis menyampaikan rasa terima kasih sebesar-besarnya kepada:

1. Ibu Dr. Safrida, S.E., M.Si, selaku Rektor Universitas Islam Sumatera Utara
2. Ibu Ir. Hj. Darlina Tanjung, M.T., selaku Dekan Fakultas Teknik Universitas Islam Sumatera Utara.
3. Bapak Mhd. Zulfansyuri Siambaton, S.T., M.Kom., selaku Ketua Program Studi Teknik Informatika Universitas Islam Sumatera Utara.

4. Bapak Oris Krianto Sulaiman, S.T, M.Kom selaku pembimbing (satu) yang telah bersedia membimbing, meluangkan waktu, memberikan saran serta solusi selama penyelesaian skripsi.
5. Bapak Aulia Ichsan, ST, M.Kom, selaku pembimbing (dua) yang telah bersedia membimbing, meluangkan waktu, memberikan saran serta solusi selama penyelesaian skripsi.
6. Seluruh Bapak dan Ibu serta Staf dan Karyawan yang telah mengajarkan dan membantu segala urusan saat di Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Sumatera Utara
7. Kepada orang tua yang selalu mendo'akan serta memberi nasihat selama pengerjaan tugas akhir ini.
8. Kepada teman-teman seperjuangan yang selalu sama-sama dalam hal suka dan duka, serta selalu memberikan semangat dan motivasi

Penulis berharap semoga skripsi ini dapat memberi manfaat dan pengetahuan kepada pembaca. Penulis menyadari bahwa dalam penulisan skripsi ini masih banyak kekurangan. Karena itu kritik dan saran sangat diharapkan yang bersifat membangun dalam menyempurnakan penulisan skripsi ini serta bermanfaat bagi penulis maupun pembaca.

Medan,            Juni 2025

Muhammad Fauzan Rifqi

NPM : 71210915053

## DAFTAR ISI

<b>ABSTRAK .....</b>	<b>i</b>
<b>KATA PENGANTAR.....</b>	<b>ii</b>
<b>DAFTAR ISI.....</b>	<b>iv</b>
<b>DAFTAR GAMBAR.....</b>	<b>vi</b>
<b>DAFTAR TABEL .....</b>	<b>vii</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>viii</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1    Latar Belakang .....	1
1.2    Rumusan Masalah .....	4
1.3    Batasan Masalah.....	4
1.4    Tujuan.....	4
1.5    Manfaat .....	5
1.6    Metodologi Penelitian .....	5
1.7    Sistematika Penulisan .....	6
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>8</b>
2.1 <i>Website</i> .....	8
2.1.1    Pengertian <i>Website</i> .....	8
2.1.2    Jenis-Jenis <i>Website</i> .....	8
2.1.3    Keamanan <i>Website</i> .....	9
2.1.4    Aspek Keamanan <i>Website</i> .....	9
2.2    Pemindai Kerentanan ( <i>Penetration Testing</i> ) .....	10
2.2.1    Pengertian <i>Penetration Testing</i> .....	10
2.2.2    Jenis-Jenis <i>Penetration Testing</i> .....	11
2.3 <i>OWASP</i> .....	11
2.4    ISO/IEC 27001.....	14
2.5 <i>SQL Injection</i> .....	15
2.6 <i>Cross Site Scripting (XSS)</i> .....	15
2.7 <i>Information System Security Assessment Framework (ISSAF)</i> .....	16

2.8	Penelitian Terdahulu.....	20
2.9	<i>Flowchart</i> .....	22
<b>BAB III METODE PENELITIAN .....</b>		<b>24</b>
3.1	Alat dan Bahan Yang Digunakan .....	24
3.2	Metode Pengumpulan Data .....	25
3.3	Pengujian dan Analisis .....	25
3.3.1	<i>Roadmap</i> Penelitian .....	25
3.3.2	Kerangka Penelitian .....	26
3.3.3	Tahapan Pemindaian Menggunakan <i>Whatweb</i> .....	29
3.3.4	Tahapan Pemindaian Menggunakan <i>Whois</i> .....	30
3.3.5	Tahapan Pemindaian Menggunakan <i>NMAP</i> .....	31
3.3.6	Tahapan Pemindaian Menggunakan <i>Arachni</i> .....	32
3.3.7	Tahapan Pengujian <i>SQL Injection</i> .....	34
3.3.8	Tahapan Pengujian <i>Cross-Site Scripting (XSS) Reflected</i> .....	35
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>		<b>37</b>
4.1	Hasil .....	37
4.2	Pembahasan.....	37
4.2.1	<i>Information Gathering</i> .....	37
4.2.2	<i>Mapping Network</i> .....	39
4.2.3	<i>Vulnerability Identifying</i> .....	41
4.2.4	<i>Penetraion</i> (Eksploitasi Kerentanan) .....	43
4.3	Hasil Pengujian .....	46
4.3.1	Pelaporan.....	46
<b>BAB V KESIMPULAN DAN SARAN .....</b>		<b>50</b>
5.1	KESIMPULAN .....	50
5.2	SARAN .....	51
<b>DAFTAR PUSTAKA.....</b>		<b>52</b>

## DAFTAR GAMBAR

<b>Gambar 2.1</b> ISSAF Framework.....	17
<b>Gambar 3.1</b> Tahapan Penelitian.....	26
<b>Gambar 3.2</b> Alur kerja whatweb.....	29
<b>Gambar 3.3</b> Alur kerja whois.....	30
<b>Gambar 3.4</b> Alur kerja NMAP.....	31
<b>Gambar 3.5</b> Alur kerja arachni .....	32
<b>Gambar 3.6</b> Alur kerja sqlmap.....	34
<b>Gambar 3.7</b> Alur kerja pengujian XSS .....	35
<b>Gambar 4.1</b> WHATWEB.....	38
<b>Gambar 4.2</b> WHOIS .....	39
<b>Gambar 4.3</b> NMAP.....	40
<b>Gambar 4.4</b> Firewall Identification .....	41
<b>Gambar 4.5</b> Laman Web Arpusda.....	43
<b>Gambar 4.6</b> Error message .....	44
<b>Gambar 4.7</b> SQLMAP .....	44
<b>Gambar 4.8</b> XSS.....	45

## DAFTAR TABEL

<b>Tabel 2.1</b> Roadmap ISSAF .....	19
<b>Tabel 2.2</b> Penelitian Terdahulu .....	20
<b>Tabel 2.3</b> Simbol Flowchart .....	23
<b>Tabel 3.1</b> Kebutuhan Perangkat Keras .....	24
<b>Tabel 3.2</b> Kebutuhan Perangkat Lunak .....	24
<b>Tabel 3.3</b> Roadmap Penelitian .....	25
<b>Tabel 4.1</b> Service server .....	40
<b>Tabel 4.2</b> Hasil pemindaian menggunakan Arachni .....	41
<b>Tabel 4.3</b> Hasil Scanning whatweb .....	46
<b>Tabel 4.4</b> Hasil Scanning whois .....	47
<b>Tabel 4.5</b> Hasil Scanning NMAP .....	47
<b>Tabel 4.6</b> Hasil Scanning Arachni .....	48
<b>Tabel 4.7</b> Langkah Mitigasi .....	49

## DAFTAR LAMPIRAN

<b>Lampiran</b>	<b>Halaman</b>
1. SK Pembimbing	<b>L-1</b>
2. Kartu Bimbingan Doping 1	<b>L-2</b>
3. Kartu Bimbingan Doping 2	<b>L-3</b>
4. Surat Izin Penelitian dari Fakultas	<b>L-4</b>
5. Surat Balasan Izin Penelitian	<b>L-5</b>

## 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., Sugiarta, 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).