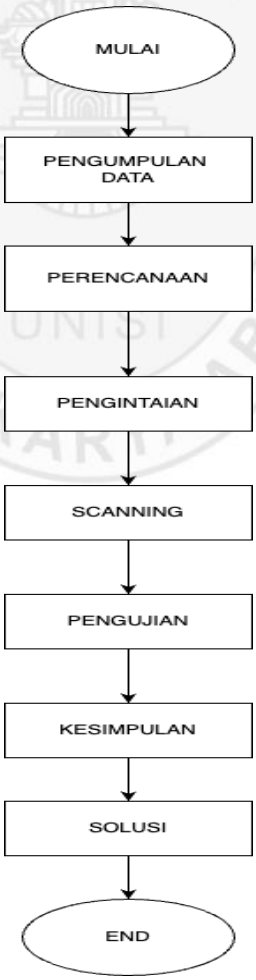
Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

BAB III

METODE PENELITIAN

3.1 Alur Penelitian

Pengujian penetrasi pada suatu situs perlu disesuaikan dengan karakteristik konfigurasi *website* maupun server agar standar keamanan yang digunakan dapat diterapkan secara tepat [37]. Pada Sistemasi UNISI, analisis kerentanan dilaksanakan dengan mengikuti rangkaian kerja OWASP ZAP. Prosedurnya mencakup perencanaan, pengintaian, scanning, penyusunan *report*, penentuan solusi, serta penarikan kesimpulan. Urutan proses tersebut divisualisasikan melalui Gambar 3.1.



Gambar 3.1 Alur Penelitian

3.2 Metode Pengumpulan Data

Pelaksanaan kajian menggunakan dua cara dalam memperoleh informasi yang diperlukan, yaitu observasi dan studi literatur.

3.2.1 Observasi

Observasi dilakukan melalui peninjauan langsung terhadap Sistemasi UNISI sebagai objek yang dianalisis. Kegiatan ini dimaksudkan untuk memahami keadaan situs, susunan halaman, fasilitas yang tersedia, mekanisme autentikasi, alur pemasukan serta pengolahan informasi, hingga fungsi yang dapat digunakan oleh pengguna.

Selama pengamatan, bagian sistem yang berpotensi menjadi sasaran pemeriksaan keamanan turut dipetakan. Area tersebut antara lain halaman masuk, formulir, parameter URL, pengelolaan sesi, serta fungsi lain yang melibatkan komunikasi antara pengguna dan aplikasi. Informasi yang diperoleh kemudian digunakan untuk menyusun batas pemeriksaan serta skenario *penetration testing*. Seluruh proses dilakukan sesuai ruang lingkup yang telah ditetapkan dengan tetap memperhatikan izin serta keamanan sistem yang menjadi objek kajian.

3.2.2 Studi Literatur

Pengumpulan informasi melalui studi literatur dilakukan dengan menelaah berbagai sumber yang mempunyai keterkaitan dengan pembahasan. Referensi yang digunakan mencakup artikel jurnal, buku, prosiding konferensi, tugas akhir, maupun sumber digital lain yang

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

mendukung topik kajian. Hasil telaah tersebut dipakai sebagai pijakan untuk pengembangan kajian lebih lanjut.

3.3 Perencanaan

Tahap perencanaan menjadi dasar sebelum kegiatan *penetration testing* dilaksanakan. Pada bagian ini ditetapkan batas pengujian, tujuan pelaksanaan, kebutuhan sumber daya, serta jadwal kegiatan. Kondisi infrastruktur, aplikasi yang terlibat, dan kemungkinan ancaman juga dipelajari agar skenario pengujian dapat dirancang secara tepat. Selain itu, seluruh pihak yang terlibat perlu memperoleh pemahaman yang selaras mengenai sasaran dan prosedur evaluasi yang akan digunakan.

Pada kajian ini, Sistemasi UNISI diamati untuk memperoleh informasi yang dibutuhkan sebagai dasar evaluasi. Pengamatan juga dimanfaatkan untuk melihat perkembangan sistem setelah perubahan *website* pada tahun 2023. Selama periode tersebut, beberapa pembaruan pada fitur, tampilan, dan desain dari versi sebelumnya menuju versi baru dicatat untuk menilai kemungkinan pengaruhnya terhadap kondisi perlindungan *website*.

3.4 Pengintaian

Pengintaian merupakan proses awal untuk memperoleh informasi mengenai target sebelum pemeriksaan lebih lanjut dilakukan. Pada tahap ini, sebanyak mungkin informasi yang relevan dikumpulkan mengenai *website* atau sistem sasaran tanpa menjalankan tindakan yang berpotensi mengganggu layanan. Data yang diperoleh dapat mencakup struktur jaringan, teknologi yang diterapkan, serta informasi lain yang dapat dimanfaatkan dalam menyusun tahapan pemeriksaan

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

berikutnya. Proses pengumpulan tersebut dapat dilakukan melalui pemindaian DNS, pencarian data yang tersedia untuk publik, maupun penelusuran metadata.

3.5 *Scanning*

Setelah pengintaian, proses dilanjutkan dengan scanning untuk menemukan indikasi kelemahan. Perangkat dan teknik pemindaian digunakan untuk menganalisis sistem maupun aplikasi, termasuk memeriksa port terbuka dan konfigurasi yang tidak aman. OWASP ZAP dapat dimanfaatkan untuk menelusuri berbagai indikasi kelemahan, termasuk potensi injeksi *SQL* maupun *Cross-Site Scripting* (*XSS*) serta jenis kerentanan lain yang dapat terdeteksi selama pemindaian.

3.6 Pengujian Kerentanan *Website*

Sesudah scanning dan identifikasi kerentanan, laporan disusun untuk merangkum temuan selama *penetration testing*, kategori risiko, serta bukti teknis yang diperoleh. Laporan tersebut ditujukan agar pihak yang berkepentingan memperoleh gambaran yang mudah dipahami mengenai bentuk ancaman yang berhasil ditemukan beserta konsekuensinya terhadap perlindungan sistem.

3.6.1 *Tested Website Determination*

Kajian ini mengkaji *website* dalam lingkup organisasi akademik yang digunakan pada Universitas Islam Indragiri, untuk keperluan publikasi UNISI yaitu, https://sistemasi.ftik.unisi.ac.id.

3.6.2 *Software Installation*

Menginstal aplikasi OWASP ZAP versi 2.11.1 pada sistem operasi Windows 11 sangat berguna untuk meningkatkan keamanan situs web.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Aplikasi ini membantu dalam mendeteksi dan menganalisis kerentanan yang mungkin ada pada situs web. Untuk mendapatkan aplikasi ZAP secara resmi, pengguna dapat mengunduhnya melalui situs web OWASP di alamat https://www.zaproxy.org/.

3.6.3 *Vulnerabillity Testing*

Pengujian kerentanan dijalankan melalui OWASP ZAP dengan menetapkan alamat situs yang akan diperiksa sebagai sasaran pemindaian. Setelah URL dimasukkan, aplikasi menjalankan proses eksplorasi otomatis menggunakan mekanisme *traditional spider*. Melalui mekanisme tersebut, struktur serta konten pada situs dapat ditelusuri untuk menemukan bagian yang memiliki indikasi kelemahan.

3.7 Kesimpulan

Kesimpulan adalah bagian akhir dari proses penetration testing. Pada tahap ini, Peneliti menyimpulkan hasil uji penetrasi secara keseluruhan, memberikan ringkasan tentang tingkat keamanan sistem yang diuji, dan menilai efektivitas langkah-langkah perbaikan yang telah dilakukan. Peneliti juga dapat mengidentifikasi langkah selanjutnya yang diperlukan untuk memastikan keamanan berkelanjutan dari sistem, seperti pengujian ulang atau implementasi kontrol keamanan tambahan.

3.8 Solusi

Hasil pemindaian menyediakan berbagai informasi mengenai temuan keamanan, termasuk bentuk peringatan, klasifikasi risiko, dan rincian pendukung lainnya. Data tersebut digunakan untuk memahami karakteristik setiap kelemahan serta menjadi dasar dalam menentukan tindakan penanganan yang sesuai.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Setelah titik lemah pada Sistemasi UNISI berhasil dipetakan, tindakan korektif kemudian disusun sesuai jenis masalah yang ditemukan. Penerapan tindakan tersebut diarahkan untuk memperkuat perlindungan situs sekaligus menjaga informasi dan integritas sistem dari kemungkinan ancaman.

3.9 Bahan dan Alat Penelitian

Perangkat yang mendukung pelaksanaan kajian terdiri atas komponen *hardware* dan *software*. Spesifikasi keduanya disajikan pada Tabel 3.1 sebagai gambaran sarana yang digunakan selama proses pengujian.

Tabel 3.1 Bahan dan Alat Penelitian

***Hardware* dan Sistem Operasi**	***Software***
Lenovo 82h7 Processor : 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80 GHz RAM : 8 GB System type : 64-bit Operating system, x64-based processor	OWASP ZAP : Digunakan sebagai perangkat pemeriksaan kerentanan *website*.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri