BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Menurut penelitian terdahulu yang telah dikerjakan oleh penelti sebelumnya *tools* yang digunakan cukup bervariasi dan beberapa objek yang berbeda, sehingga hasil yang diberikan juga bervariasi. Oleh karena itu, berikut tabel kajian sebagai pembanding penelitian terdahulu dengan penelitian yang akan dilakukan.

Tabel 2. 1 Penelitian terdahulu

No	Author	Judul	Metode	Hasil
1.	Muhammad Rafi Ramdani, Nono Heryana, Agung Susilo Yuda Irawan	Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)	*penetration testing* dengan *Open Web Application Security Project (OWASP) parameter* keamanan *website* adalah *OWASP Top-10 2021*	• OWASP ZAP, ditemukan 3 celah dengan tingkat risiko high, 5 celah dengan tingkat risiko medium,8 celah dengan tingkat risiko low, dan 3 celah dengan tingkat risiko informational • penetration testing berhasil pada celah keamanan, X-Frame-Options Header Not Set, Application Error Disclosure, Broken Access Control.
2.	Syarif Hidayatulloh, Desky Saptadiaji	Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)	*Open Web Application Security Project (OWASP) parameter* keamanan *website* adalah *OWASP Top-10 2017*	• Dari 13 kerentanan yang ditemukan, ada satu kerentanan dengan tingkat ancaman sedang, yaitu X-Frame-Options Header Not Set, dan 12 kerentanan dengan tingkat ancaman rendah. Kerentanan tersebut termasuk X-Frame-Options Header Not Set, Cookie No HttpOnly Flag, Cookie Without Secure Flag, X-Content-Type-Options Header Missing, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control and Pragma HTTP Header Set, Cookie Without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Absence of Anti-CSRF Tokens, Blind SQL Injection, The X-XSS-Protection header is not defined, The site uses SSL and the Strict-Transport-Security HTTP header is not defined, dan The site uses SSL and Expect-CT header is not present. Berdasarkan CIS Control V8, terdapat 18 kontrol, dengan 6 kontrol di antaranya untuk mengurangi risiko
3.	Yudiana, Anggi Elanda, Robby Lintang Buana	*Analisis kualitas keamanan sistem informasi E-OFFICE berbasis Website pada STMIK Rosma dengan menggunakan OWASP*	*metode OWASP (Open Web Application Security Project) TOP 10*	• Menurut hasil dari OWASP ZAP, sistem informasi e-office di STMIK ROSMA memiliki 13 kerentanan. Dalam kerangka OWASP TOP 10, teridentifikasi bahwa sistem ini memiliki 4 kerentanan utama, yakni Sensitive Data Exposure, Security Misconfiguration, Cross Site Scripting, dan Insecure Deserialization

		Top 10		

Dalam tabel 2.1 terdapat beberapa penelitian sebelumnya yang telah dilakukan. Metode yang digunakan pun kurang lebih sama yaitu *penetration testing* menggunakan OWASP *standart* Top 10. Acuan dan objek yang digunakan berbeda sehingga menghasilkan kerentanan atau *vulnerability* yang bervariasi. Pada penelitian ini melakukan *penetration testing* menggunakan OWASP standart Top 10 dengan objek *website* PT. Sekar Laut Tbk. Peneliti melakukan *penetration testing* pada PT. Sekar Laut Tbk. agar bisa mendapatkan kerentanan atau *vulnerability* yang baru atau berbeda dengan peneliti sebelumnya. Sehingga dapat menjadi acuan pada developer PT. Sekar Laut Tbk. dan Perusahaan lainnya dalam mengamankan keamanan *website*.

2.2 *Website* PT. Sekar Laut Tbk

PT. Sekar Laut Tbk. adalah perusahaan yang bergerak di industri, pertanian, perdagangan, dan pembangunan, fokus utamanya pada sektor manufaktur makanan dan minuman. Perusahaan ini menggunakan *website* sebagai *platform* sistem informasi yang menyimpan berbagai data penting seperti data karyawan, produksi, investor, dan pembayaran.

2.3 *Penetration Testing*

Penetration testing adalah serangkaian proses berisi prosedur dan teknik mengevaluasi keamanan terhadap sistem komputer atau jaringan dengan melakukan simulasi penyerangan untuk mengetahui letak celah-celah kerawanan pada sistem agar kemudian celah tersebut ditutup atau diperbaiki.[3]. Dalam metode *penetration testing* ada beberapa phase atau proses yang dibagi menjadi tiga seperti pada gambar dibawah ini:

Gambar 2. 1 Fase Penetration Testing

1. ***Pre-Attack Phase***

Dalam fase ini kegiatan yang dilakukan adalah meminta persetujuan dari target dan memastikan bahwa target setuju untuk sistemnya dilakukan pengujian. Fase pra-serangan terdiri dari beberapa kegiatan penting, termasuk mendefinisikan dan menyetujui aturan keterlibatan, memahami persyaratan klien secara menyeluruh, menyelesaikan ruang lingkup pengujian, menandatangani perjanjian dan kontrak, dan kemudian mulai mengumpulkan informasi tentang jaringan target[17]. *Fase pre-attack* melibatkan pengintaian atau pengumpulan data. Ini adalah langkah pertama untuk penguji pena. Mengumpulkan data dari Whois, DNS, dan pemindaian jaringan dapat membantu Anda memetakan jaringan target dan memberikan informasi berharga mengenai sistem operasi dan aplikasi yang berjalan pada sistem[16].

2. ***Attack Phase***

Dalam fase ini kegiatan yang dilakukan adalah mulai melakukan sebuah pencarian rentan keamanan yang ada dalam sebuah sistem dan mulai melakukan sebuah serangan dari celah keamanan yang telah ditemukan. Setelah proyek penetration testing dimulai dengan menyelesaikan kegiatan di fase *pra-Attack*. sekarang pada fase ini dimulai untuk menemukan setiap kerentanan dan mengeksploitasi kelemahan yang ditemukan di sistem target[17]. Biasanya penguji yang sudah ahli dalam bidang penetration testing menggunakan beberapa alat yang responsif dan dari beberapa alat yang telah disesuaikan dari celah keamanan yang ada, penguji melakukan pemantauan dan menguji keamanan dari sistem maupun jaringan pada sistem[16].

3. *Post-Attack Phase*

Dalam fase yang terakhir ini proses yang dilakukan adalah mengembalikan sistem ke bentuk awal sebelum dilakukannya penetration testing jika memang ada perubahan. Setelah semua pengujian dilakukan pada sistem atau jaringan target, perlu dilakukan pembersihan dan pemulihan sistem[17]. *Fase post-attack* melibatkan pemulihan sistem ke konfigurasi perangkat normal, yang mencakup menghapus file, membersihkan *entri Registry* jika kerentanan dibuat, dan menghapus share dan koneksi[16].

2.4 OWASP Top 10 *Web Application Security Risks* 2021

OWASP adalah komunitas yang terbuka bagi organisasi untuk mengembangkan, membeli, dan merawat aplikasi yang dapat diandalkan. OWASP tidak memiliki afiliasi dengan perusahaan tertentu dan merupakan organisasi nirlaba yang berfokus pada jaminan keberhasilan jangka panjang proyek-proyeknya. Sebagian besar individu yang terlibat dengan OWASP adalah sukarelawan [12]. Berikut daftar OWASP TOP 10 2021:

OWASP Top 10 Web Application Security Risks 2021
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures

Security Logging and Monitoring Failures
Server-Side Request Forgery

Gambar 2. 2 Daftar Owasp Top 10

2.4.1 *Broken Access Control*

Beberapa aplikasi web memverifikasi izin akses pada tingkat fungsi sebelum membuat fungsionalitas tersebut tersedia bagi pengguna. Meskipun demikian, setelah setiap fitur dapat diakses, program harus melewati pemeriksaan kontrol akses yang sama seperti *server*. Jika permintaan tidak diverifikasi dan melewati sebuah proses autoriasi, penyerang dapat memperoleh akses ke fitur tanpa izin yang diperlukan[12].

2.4.2 *Cryptographic Failures*

Kriptografi mengacu pada metode dan prosedur yang digunakan untuk menjaga kerahasiaan, *non-denial*, integritas, dan keaslian. Kegagalan kriptografi adalah masalah keamanan aplikasi online yang signifikan yang mengekspos data aplikasi sensitif karena metode kriptografi yang lemah atau tidak ada sama sekali.

2.4.3 *Injection*

Seorang penerjemah mungkin menerima atau dikirimi informasi yang tidak dipercaya dari penyerang. Penyerang dapat mengelabui penerjemah dan memicu instruksi tidak sah dengan memberikan informasi berbahaya. Tiga jenis serangan injeksi berikut ini adalah yang paling serius: injeksi SQL, injeksi kode, dan injeksi XPath.

2.4.4 *Insecure Design*

Kerentanan ini dapat terjadi ketika penyerang dapat melakukan sebuah serangan dengan memanfaatkan sebuah *design flaw* pada sebuah perusahaan.

2.4.5 *Security Misconfiguration*

Masalah kesalahan konfigurasi keamanan terjadi ketika satu atau lebih komponen sistem, seperti aplikasi, kerangka kerja, *server* aplikasi, *server web*, *database server*, router jaringan, dan *platform*, tidak dikonfigurasi dengan baik. Pengaturan yang aman harus dilakukan dikembangkan, diterapkan, dan dipelihara.

2.4.6 *Vulnerable and Outdated Components*

Kerentanan ini dapat terjadi ketika penyerang dapat memanipulasi keamanan kode atau sebuah komponen yang telah kadaluarsa.

2.4.7 *Identification and Authentication Failures*

Peretas mengeksploitasi kerentanan ini untuk memanfaatkan otentikasi yang tidak tepat nama menunjukkan. Seorang peretas dapat mengakses informasi pengguna, kata sandi, sesi ID, dan lainnya kredensial masuk, menimbulkan risiko keamanan.

2.4.8 *Software and Data Integrity Failures*

Kegagalan integritas perangkat lunak dan data disebabkan oleh kode dan infrastruktur yang menyebabkannya tidak melindungi terhadap pelanggaran integritas.

2.4.9 *Security Logging and Monitoring Failures*

Tanpa pencatatan, tindakan dan kejadian mencurigakan tidak akan terpantau lebih lama periode tertentu, berpotensi memungkinkan pelanggaran keamanan terus berlanjut tanpa terdeteksi lebih lama dari biasanya akan dengan logging yang lebih baik. Peretas situs web dapat melakukan banyak kerusakan, tetapi peretasan bisa saja terjadi lebih sulit jika pemilik aplikasi web tidak memantau perilaku kode yang mencurigakan aktivitas. Sistem pemantauan bisa sangat berguna dalam situasi ini.

2.4.10 *Server-Side Request Forgery*

Penyerang dapat mengeksploitasi kerentanan ini untuk mengirim permintaan ke lokasi yang tidak diinginkan melalui aplikasi sisi server

2.5 OWASP ZAP

OWASP ZAP adalah alat pemindai kerentanan yang dikembangkan oleh organisasi OWASP. Alat ini merupakan salah satu proyek yang paling aktif dalam OWASP karena terus menerus dikembangkan. OWASP ZAP bersifat *open-source*, memungkinkan siapa pun untuk berkontribusi dalam pengembangannya.[4]

2.6 *Vulnerability Assessment*

Vulnerability Assessment adalah sebuah metode untuk melakukan sebuah pengukuran terhadap tingkat keamanan dari sebuah sistem. *Vunerability Assessment* adalah pemindaian sistem, *software*, atau jaringan adalah proses untuk mengidentifikasi kelemahan dan celah yang ada. Celah ini dapat memberikan akses yang tidak sah kepada penyerang untuk menyerang target mereka.[7] Suatu sistem mungkin memiliki kerentanan kontrol akses, kerentanan kondisi batas, kerentanan validasi masukan, kerentanan otentikasi, kerentanan kelemahan konfigurasi, dan Kerentanan Penanganan Pengecualian, dll. Ada 2 tipe pemindaian pada *vulnerability Assessment* yaitu:

1. *Authenticated Scan*

   Sebuah pemindaian kerentanan yang dilengkapi dengan kredensial yang valid untuk target yang dilakukan pemindaian kerentanan[16].

2. *Unauthenticated scan*

   Sebuah pemindaian kerentanan dimana tidak ada kredensial untuk target yang dilakukan pemindaian kerentanan. Oleh karena itu pemindaian ini hanya melakukan pemindaian pada bagian-bagian yang tidak memerlukan sebuah otentikasi.

Vulnerability asessement dapat dilakukan dengan melakukan pemindaian dengan beberapa *tools* yang memang ditujukan untuk melakukan proses pemindaian celah keamanan. Dengan bantuan pemindai kerentanan, seseorang dapat dengan mudah mengidentifikasi kelemahan kesalahan konfigurasi yang umum, akun dengan kata sandi yang lemah atau *default*, tidak diinginkan atau tidak digunakan layanan, dan file atau direktori dengan izin yang lemah[10].