BAB II
TINJAUAN PUSTAKA

2.1 Kajian Penelitian Terdahulu

Beberapa penelitian yang memanfaatkan *Owasp Zed Attack Proxy (ZAP)* dan *Wazuh* untuk penilaian keamanan di situs web telah sering dilakukan dan diterapkan. Oleh karena itu, untuk mendukung penelitian yang menggunakan metode serupa, peneliti melakukan review terhadap beberapa penelitian yang menggunakan metode serupa. Adapun rincian penelitian terdahulu yang dijadikan acuan atau pedoman oleh peneliti adalah sebagai berikut :

Tabel 1. Kajian Penelitian Terdahulu

No	Judul	Penulis	Tahun	Metode	Hasil
1.	Analisis Celah Keamanan dan Mitigasi *Website* E-Learning ITERA Menggunakan *Owasp Zed Attack Proxy (ZAP)*	Ilham Firman Ashari, Leonard Rizta Anugrah P, Nazla Anditya W, Siraz Tri Denira	2023	Metode penetration testing	Hasil yang didapatkan dalam penelitian ini adalah : *a.* Berdasarkan analisis yang telah dilakukan menunjukkan bahwa *website* e-learning ITERA berhasil diserang menggunakan metode *reverse brute force.* b. Terdapat tiga URI dengan risiko tinggi serangan *SQL Injection.*
2.	Analysis of *Cross Site Request Forgery (CSRF)* Attacks on West Lampung Regency *Websites* Using	Ilham Firman Ashari, Vina Oktariana, Ringgo Galih Sadewo, Salman Damanhuri	2022	Metode penetration testing	Hasil yang didapatkan dalam penelitian ini adalah : a. Dari hasil percobaan didapatkan ada 12 alert dengan resiko low pada *website* Kabupaten lampung barat, pada 12 alert terdapat 53 URL

	OWASP ZAP Tools				pages yang rentan untuk dilakukan serangan.
3.	Analisis Sistem Security Information and Event Management (SIEM) Aplikasi *Wazuh* pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan	Mardhiyah Nas, Farchia Ulfiah, Ulya Putri	2023	Metode penetration testing	Hasil yang didapatkan dalam penelitian ini adalah : a. Dengan melakukan pengujian menggunakan 2 jenis serangan yaitu *Ddos Slowloris* dengan jumlah serangan 10.000, 15.000 dan 20.000 paket data dan *Brute Force* dengan jumlah serangan 20.470 paket data didapatkan bahwa aplikasi wazuh berhasil mendeteksi serangan *DdoS Slowloris* dan *Brute Force* serta dapat mengklasifikasikan keduanya serangan di level 3 hingga 10.

Seperti yang terlihat pada Tabel 1, penelitian yang sudah dilakukan dengan menggunakan metode yang sama sebagai acuan atau rujukan terdapat beberapa perbedaan pada hasil yang diberikan. Walaupun terdapat beberapa perbedaan dalam proses tertentu, hasil yang didapat diakhir masih tetap sama yaitu apakah *website* yang diuji memiliki sebuah celah keamanan yang dapat disusupi oleh *hacker* dan seberapa rentan celah keamanan itu.

2.2 *Website* Dukcapil Kab.Nganjuk

Website Dukcapil Kab.Nganjuk merupakan sebuah *website* yang disediakan oleh pemerintah untuk memberikan akses dan layanan terkait data kependudukan

dan pencatatan sipil kepada masyarakat secara online. Karena *website* Dukcapil Kab.Nganjuk mengelola informasi sensitif seperti nomor identitas, tanggal lahir, alamat, dan informasi lainnya yang dapat digunakan untuk identifikasi pribadi, maka website ini membutuhkan pengecekan apakah sistem pada website tersebut aman atau tidak.

2.3 Penetration Testing

Penetration testing adalah sebuah metode pengujian keamanan yang sering digunakan untuk melakukan pengujian apakah sebuah sistem itu aman atau tidak. Dalam metode penetration testing ada beberapa phase atau proses yang dibagi menjadi tiga yaitu seperti pada gambar dibawah ini :

Gambar 1. Fase Penetration Testing

a) *Pre-Attack Phase*

Pada tahap ini, aktivitas yang dilakukan mencakup memperoleh persetujuan dari target dan memastikan bahwa target memberikan izin untuk dilakukan pengujian pada sistemnya. Tahap pra-serangan melibatkan sejumlah langkah penting, seperti mendefinisikan serta menyepakati aturan keterlibatan, memahami kebutuhan secara mendalam, menentukan ruang lingkup pengujian, dan mulai mengumpulkan informasi terkait jaringan target. Proses ini mencakup kegiatan pengintaian atau pengumpulan data, yang menjadi langkah awal dalam pelaksanaan pengujian. Data yang diperoleh dari layanan seperti Whois, DNS, dan pemindaian jaringan dapat membantu memetakan jaringan target serta memberikan wawasan berharga mengenai sistem operasi dan aplikasi yang digunakan pada sistem tersebut.

b) *Attack Phase*

Pada tahap ini, kegiatan yang dilakukan adalah mulai mencari kerentanan keamanan yang ada dalam suatu sistem dan memanfaatkan celah keamanan yang telah ditemukan untuk melakukan serangan. Setelah fase pra-serangan

selesai dalam proyek pengujian penetrasi, langkah ini difokuskan pada identifikasi kerentanan serta eksploitasi kelemahan pada sistem target. Biasanya, penguji yang berpengalaman dalam pengujian penetrasi menggunakan berbagai alat yang responsif dan disesuaikan dengan celah keamanan yang ada. Dengan bantuan alat tersebut, penguji memantau dan menguji tingkat keamanan sistem atau jaringan secara menyeluruh.

c) *Post-Attack Phase*

Pada tahap terakhir ini, proses yang dilakukan adalah mengembalikan sistem ke kondisi semula sebelum pengujian penetrasi dilakukan, apabila terdapat perubahan. Setelah seluruh pengujian terhadap sistem atau jaringan target selesai, diperlukan langkah pembersihan dan pemulihan sistem. Fase pasca-serangan mencakup pemulihan konfigurasi perangkat ke keadaan normal, termasuk menghapus file yang tidak diperlukan, membersihkan entri Registry yang dibuat selama pengujian, serta menghapus share dan koneksi yang telah dibuat sebelumnya.

Hasil dari penetration testing dapat digunakan untuk membantu memverifikasi apakah *website* tersebut aman atau tidak. Ada beberapa metode yang digunakan untuk melakukan sebuah tes penetrasi pada sebuah web aplikasi. Pada penelitian ini tes penetrasi yang dilakukan adalah :

a) *Cross-site Scripting (XSS)*

Cross-site Scripting atau serangan *XSS* merupakan sebuah jenis serangan yang memanfaatkan celah keamanan pada sebuah sistem dengan melakukan sebuah penyuntikan script yang jahat untuk mencuri beberapa data dan informasi yang bersifat rahasia.

b) *Sql Injection*

Sql Injection merupakan sebuah jenis serangan yang memanfaatkan celah keamanan yang ada pada sebuah sistem dengan melakukan perubahan kueri yang dikirim untuk pengambilan data yang ada pada sebuah database sietem[8]. *Sql Injection* dapat membahayakan perlindungan situs *website* individu dan seluruh infrastruktur database dan jaringan sistem yang menampung aplikasi terkait.

c) *Clickjacking*

Clickjacking merupakan serangan cyber yang dilakukan dengan cara menyamarkan elemen tertentu untuk mengelabui pengguna. Serangan clickjacking adalah teknik serangan yang memancing pengguna untuk mengklik sebuah elemen yang telah disisipkan di halaman website, sehingga data-data rahasia pengguna terungkap dan disalah gunakan oleh pihak yang tidak bertanggung jawab[9].

Maka dari itu perlu dilakukan sebuah penetration testing pada sebuah sistem dapat menjamin agar data pribadi suatu perusahaan aman.

2.4 OWASP Top 10 Web Application Security Risks 2021

OWASP Top 10 Web Application Security Risks 2021 merupakan sebuah framework yang memberikan sebuah standar dokumen keamanan untuk pengembang *website* agar *website* menjadi lebih aman. Pengujian *OWASP* Kerangka Panduan memiliki fokus yang kuat pada tingkat keamanan aplikasi web dalam semua pengembangan perangkat lunak aspek lifecycle yang berbeda dengan penetrasi lainnya pengujian kerangka pengujian keamanan, seperti *ISSAF* dan *OSSTMM*, yang keduanya dimaksudkan untuk menguji keamanan dari implementasi[10]. Pada tahun 2021 sendiri framework ini mengalami beberapa perubahan dari kerentanan yang ada pada 2017 seperti pada gambar dibawah ini :

Gambar 2. Top 10 Web Application Security Risks by OWASP

Pada gambar 2, ada sepuluh kerentanan yang pada sebuah aplikasi dan penjelsannya adalah :

a) A01-Broken Access Control

Kerentanan ini memanfaatkan sistem kontrol yang mengalami sebuah kesalahan yang dapat memungkinkan penyerang dapat melewati sebuah proses autorisasi sehingga penyerang dapat mengakses data yang seharusnya hanya boleh diakses oleh admin.

b) *A02-Cryptographic Failures*

Kerentanan ini dapat terjadi karena pada sebuah aplikasi web memiliki sebuah algoritma kriptografi yang lemah sehingga mengakibatkan data pribadi dapat diperoleh dengan mudah oleh penyerang.

c) *A03-Injection*

Kerentanan ini dapat terjadi ketika penyerang dapat memanipulasi beberapa kode yang dibuat sendiri oleh penyerang.

d) *A04-Insecure Design*

Kerentanan ini dapat terjadi ketika penyerang dapat melakukan sebuah serangann dengan memanfaatkan sebuah design flow pada sebuah perusahaan.

e) *A05-Security Misconfiguration*

Kerentanan ini dapat terjadi ketika penyerang dapat melakukan perubahan pada sebuah software yang ada pada sebuah aplikasi web.

f) *A06-Vulnerable and Outdated Component*

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

g) *A07-Identification and Authentication Failures*

Kerentanan ini dapat dilakukan ketika penyerang dapat melakukan manipulasi indentifikasi pada dirinya.

h) *A08-Software and Data Integrity Failures*

Kerentanan ini dapat dilakukan ketika penyerang dapat memanfaatkan data yang tidak dipercaya untuk melakukan exploitasi.

i) *A09-Security Logging and Monitoring Failures*

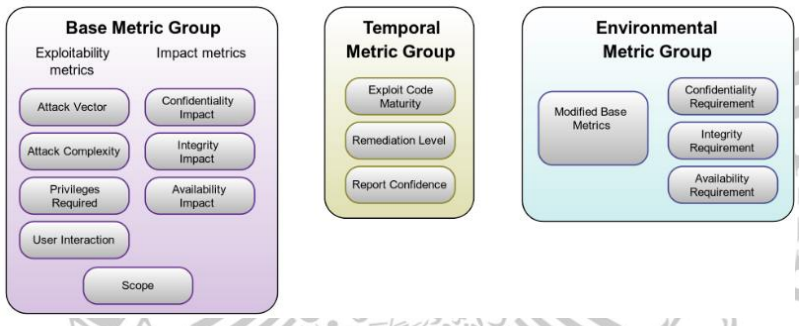
Kerentanan ini dapat dilakukan ketika penyerang dapat melakukan sebuah monitoring pada komunikasi yang dilakukan pada aplikasi web.

j) *A10-Server-Side Request Forgery*

Kerentanan ini dpata dilakukan ketika penyerang dapat meinputkan sebuah entri baru kedalam list.

2.5 CVSS (Common Vulnerability Scoring System)

CVSS (Common Vulnerability Scoring System) adalah sebuah proses penilaian yang digunakan untuk menilai kerentanan pada pengujian sistem[11]. Common Vulnerability Scoring System mempunyai karakteristik teknis utama kerentanan dan menunjukkan output berupa skor numeric yang menunjukkan seberapa parah kerentanan yang terdapat pada sistem[12]. Common Vulnerability Scoring System terdiri dari tiga metric, yaitu : *Base Metric Group, Temporal Metric Group,* dan *Environmental Metric Group*[13]. Masing-masing terdiri dari seperangkat metric, seperti yang ditunjukkan pada gambar 3.



Gambar 3. CVSS Metric Groups [12]

1. *Base Metric Group*

   Base Metric Group merupakan kerentanan yang bersifat konstan dari waktu ke waktu diseluruh lingkungan pengguna.

2. *Temporal Metric Group*

   Temporal Metric Group merupakan kerentanan yang dapat berubah seiring waktu tetapi tidak diseluruh lingkungan pengguna.

3. *Environmental Metric Group*

   Environmental Metric Group merupakan kerentanan yang unik untuk lingkungan pengguna tertentu[13].

Pada penelitian ini metric yang akan digunakan adalah *Base Metric Group* yang dimana *Base Metric Group* memiliki dua set metric didalamnya yaitu,

Exploitability metrics dan *Impact metrics. Exploitability metrics* merupakan metric yang menunjukkan hasil secara langsung dari ekspoitasi yang telah dilakukan dan menampilkan bagian mana saja yang memiliki kerentanan[13]. Metric ini terdiri dari empat komponen yaitu :

1. *Attack Vector*

   Attack Vector merupakan metric yang digunakan untuk menentukan tingkat kemungkinan serangan yang terjadi dan seberapa besar risiko yang terkait dengan kerentanan tersebut.

2. *Attack Complexity*

   Attack Complexity mengukur kompleksitas serangan yang diperlukan untuk mengeksploitasi celah ketika penyerang mendapatkan akses ke sistem target. Penilaian ini memiliki dua kategori yaitu, low dan high.

3. *Privileges Required*

   Privileges Required merupakan proses di mana penyerang mengevaluasi nilai tingkat akses sebelum menggunakan kerentanan yang mereka temukan pada target. Ada tiga kategori dalam evaluasi ini yaitu none, low, dan high.

4. *User Interaction*

   User Interaction merupakan interaksi pada pengguna target dengan melakukan eksploitasi yang sedang dijalankan. Penilaian ini memiliki dua kategori yaitu none dan
   required.

Sedangkan *Impact Metrics* merupakan efek dari kerentanan yang telah berhasil di eksploitasi pada sistem yang diuji dan membantu menilai sejauh mana efek dari kerentanan yang telah sukses dilakukan eksploitasi[13]. Metric ini terdiri dari 3 komponen yaitu :

1. *Confidentiality Impact*

   Metric ini mengukur dampak pada kerahasiaan suatu sistem yang telah berhasil dilakukan penyerangan. Penilaian ini memiliki tiga kategori yaitu, *none*, *low*, dan *high.*

2. *Integrity Impact*

Metric ini mengukur dampak terhadap integritas kerentanan yang telah berhasil di eksploitasi oleh penyerang. Penilaian ini memiliki tiga kategori yaitu, none, low, dan high.

3. *Availability Impact*

   Metric ini mengukur dampak terhadap ketersediaan komponen yang mungkin terpengaruh dari hilangnya data pada sistem yang terkena dampak dari kerentanan yang berhasil di eksploitasi. Penilaian ini memiliki tiga kategori yaitu, none, low, dan high.

Hasil akhir dari sistem penilaian CVSS bernama *Base Score*, yang dimana dimulai dari angka 0.0 – 10.0 untuk menentukan tingkat keparahan dari celah keamanan atau kerentanan yang telah ditemukan pada suatu *website.* Dapat dilihat pada tabel 2.

Tabel 2. CVSS Score [12]

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Pada tabel 2 merupakan tingkat keparahan dari lima level yaitu, *None, Low, Medium, High, dan Critical.* Yang mana dimulai dari level terendah *None* 0.0 sampai level tertinggi *Critical* 10.0 yang masing-masing nilainya memiliki rating dan score sendiri. Berikut ini merupakan rumus perhitungan *Base Score Formula* untuk mendapatkan nilai yang akurat, bisa dilihat pada gambar 4.

The Base Score formula depends on sub-formulas for Impact Sub-Score (ISS), Impact, and Exploitability, all of which are defined below:

ISS =	1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]
Impact =	
If Scope is Unchanged	6.42 × ISS
If Scope is Changed	$7.52 \times (ISS - 0.029) - 3.25 \times (ISS - 0.02)^{15}$
Exploitability =	8.22 × AttackVector × AttackComplexity × PrivilegesRequired × UserInteraction
BaseScore =	
If Impact <= 0	0, *else*
If Scope is Unchanged	Roundup (Minimum [(Impact + Exploitability), 10])
If Scope is Changed	Roundup (Minimum [1.08 × (Impact + Exploitability), 10])

Gambar 4. Base Score Formula

Pada gambar 4, terdapat rumus Base Score Formula yang mana untuk menemukan nilai akhir dari Base Score adalah dengan menambahkan nilai dari impact metrics dan exploitability metrics. Rumus yang digunakan tergantung dari scope yang dimasukkan, jika scope dari serangan itu bernilai changed atau unchanged. Rumus atau formula yang digunakan telah ditentukan oleh CVSS Special Interest Grub (SIG) yang melakukan pencarian dan menetapkan nilai metric kedalam tingkat keparahan yang ada[13].