202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

BAB II

LANDASAN TEORI

2.1 Keamanan Aplikasi Web

Keamanan aplikasi web adalah disiplin yang dimaksudkan untuk melindungi aplikasi web dari serangan dan ancaman yang dapat menyebabkan kehilangan data, kehilangan ekonomi, atau kerusakan reputasi. Sehubungan dengan situs web negara, keamanan aplikasi web sangat penting karena situs web pemerintah sering menyimpan data sensitif dari warga seperti data populasi, informasi keuangan, dan layanan publik [16][17]. Serangan siber di situs web pemerintah dapat merusak kehilangan data, kegagalan layanan, dan bahkan panggilan dari lembaga nasional. Beberapa jenis serangan yang sering terjadi pada *website* pemerintah meliputi :

1. ***SQL Injection*** **:** Serangan yang memanfaatkan kerentanan dalam *query* SQL untuk mengakses atau memanipulasi *database*. Contohnya, pada tahun 2021, sebuah *website* pemerintah daerah di Indonesia mengalami kebocoran data akibat serangan SQL *Injection*, yang mengakibatkan ribuan data warga terekspos.
2. ***Cross-Site Scripting*** **(XSS) :** Serangan yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman *website* yang dilihat oleh pengguna lain. Serangan ini dapat digunakan untuk mencuri informasi sensitif pengguna, seperti kredensial *login*.
3. ***Distributed Denial of Service*** **(DDoS) :** Serangan yang bertujuan untuk membuat *website* tidak dapat diakses dengan membanjiri server dengan lalu lintas palsu. Pada tahun 2020, beberapa *website* pemerintah di Indonesia menjadi target serangan DDoS, yang mengakibatkan gangguan layanan publik.

4. ***Cross-Site Request Forgery*** **(CSRF) :** Serangan yang mengeksploitasi kepercayaan pengguna terhadap aplikasi web untuk melakukan tindakan yang tidak diinginkan, seperti mengubah data atau melakukan transaksi tanpa persetujuan.
5. ***Insecure Direct Object References*** **(IDOR) :** Kerentanan yang terjadi ketika aplikasi web memberikan akses langsung ke objek tanpa otorisasi yang tepat, memungkinkan penyerang mengakses data sensitif.

2.2 Penetration Testing

Penetration testing adalah teknik evaluasi keamanan yang melibatkan simulasi serangan terhadap sistem untuk menemukan kerentanan yang dapat digunakan oleh penyerang. Proses ini sangat penting untuk *website* pemerintah karena dapat membantu menemukan kerentanan sebelum mereka digunakan oleh pihak yang tidak bertanggung jawab [18][19]. Pemerintah dapat melindungi data warga, menjaga integritas layanan publik, dan mencegah kerugian finansial dan reputasi dengan melakukan *penetration testing*.

Tahapan dalam *penetration testing* meliputi :

1. **Perencanaan dan Pengumpulan Informasi :** Mengidentifikasi target dan mengumpulkan informasi yang relevan, seperti struktur *website* dan teknologi yang digunakan.
2. **Pemindaian :** Menggunakan alat untuk menemukan kerentanan yang ada dalam *system*.
3. **Eksploitasi :** Mencoba untuk mengeksploitasi kerentanan yang ditemukan untuk menentukan tingkat risiko yang sebenarnya.
4. **Pelaporan :** Menyusun laporan yang merinci temuan, kerentanan, dan rekomendasi perbaikan.

Penetration testing penting untuk situs web pemerintah, karena dapat membantu menentukan kerentanan mungkin tidak terdeteksi selama proses pengembangan atau pemeliharaan lokasi. Selain itu, tes penetrasi dapat memastikan bahwa situs web pemerintah memenuhi standar keamanan yang diperlukan [7][20].

2.3 OWASP (Open Web Application Security Project)

OWASP (Open Web Application Security Project) adalah organisasi nirlaba yang berfokus pada peningkatan keamanan perangkat lunak. Salah satu kontribusi terbesar dari OWASP adalah OWASP Top 10 *Publishing*, ini adalah daftar sepuluh risiko keselamatan aplikasi web terpenting [21][22]. Top 10 OWASP sangat cocok untuk situs web pemerintah, karena banyak lubang dicatat, seperti SQL *Injection* dan *Cross Script* (XSS), biasanya di situs web pemerintah. OWASP juga menyediakan banyak alat dan sumber daya yang berbeda untuk membantu pengembang dan pakar keselamatan meningkatkan keselamatan aplikasi web. Salah satu alat yang paling populer adalah OWASP ZAP (Zed Attack), yang dirancang khusus untuk tes penetrasi aplikasi web [23].

2.4 OWASP ZAP (Zed Attack Proxy)

OWASP ZAP adalah alat *open source* yang dirancang untuk membantu menembus tes pada aplikasi web [15]. Alat ini sangat cocok untuk digunakan untuk memeriksa keamanan situs web pemerintah karena kemampuan untuk melakukan pemindaian otomatis dan manual. Beberapa fitur utama OWASP ZAP meliputi :

1. **Pemindaian Otomatis :** ZAP dapat melakukan pemindaian otomatis untuk menemukan kerentanan umum dalam aplikasi web, seperti SQL *Injection* dan XSS.

2. ***Proxy Intercept :*** ZAP dapat berfungsi sebagai *proxy* untuk menganalisis dan memodifikasi permintaan dan respons HTTP, memungkinkan pengguna untuk melakukan pengujian yang lebih mendalam.
3. **API :** ZAP menyediakan API yang memungkinkan integrasi dengan alat lain dan otomatisasi pengujian.
4. **Dukungan untuk Pengujian Manual :** ZAP juga menyediakan alat untuk pengujian manual, memungkinkan pengguna untuk melakukan eksploitasi yang lebih mendalam.

Dengan fitur-fitur ini, OWASP ZAP menjadi alat yang efektif untuk mengidentifikasi kerentanan keamanan pada *website* pemerintah dan memberikan rekomendasi perbaikan. Sebuah studi literatur juga menemukan bahwa "OWASP ZAP efektif untuk identifikasi kerentanan kritis pada *website* pemerintah" [21][22][2].

2.5 Studi Terkait

Berikut adalah tabel studi literatur yang terkait dengan penelitian OWASP ZAP yang menggunakan tiga kriteria yang dapat dilihat di tabel 2.1 :

Tabel 2.1. Studi *Literature Review*

No.	Judul Penelitian	Tahun	Metode	Hasil	Kesimpulan
1	"Analysis of Web Application Vulnerabilities in Government Portal Using OWASP ZAP"	2023	PTES *Framework* + OWASP ZAP	Terdeteksi 5 kerentanan (3 *High Risk*: SQLi, XSS, CSRF)	OWASP ZAP efektif untuk identifikasi kerentanan kritis pada *website* pemerintah
2	OWASP ZAP efektif untuk identifikasi kerentanan kritis pada *website* pemerintah	2022	OWASP Top 10 + *Automated Scanning*	78% kerentanan terdeteksi sesuai OWASP Top 10	Perlunya integrasi OWASP ZAP dalam SDLC instansi pemerintah

3	"Comparative Analysis of Vulnerability Scanning Tools for E-Government Services"	2022	OWASP ZAP vs *Burp Suite*	ZAP lebih unggul dalam deteksi XSS (92% accuracy)	ZAP cocok untuk *website* pemerintah *karena open-source* dan komprehensif
4	"Enhancing Security of Public Sector Websites Through Automated Penetration Testing"	2021	OWASP ZAP + *SQLmap*	Validasi 100% SQL *Injection* yang terdeteksi ZAP	Kombinasi ZAP + *tools* validasi meningkatkan akurasi temuan
5	Kombinasi ZAP + *tools* validasi meningkatkan akurasi temuan	2021	PTES + *Manual Exploitation*	15 kerentanan (4 Critical) pada *login page*	Pentingnya *post-exploitation analysis* untuk mitigasi risiko
6	"OWASP ZAP for Detecting Security Flaws in Government Web Applications"	2020	ZAP API + *Custom Scripts*	62 *vulnerabilities* (termasuk IDOR & Broken Auth)	ZAP fleksibel untuk pengujian berulang dan otomasi
7	"Effectiveness of OWASP ZAP in Identifying OWASP Top 10 Vulnerabilities"	2020	*Benchmark* OWASP Top 10	Deteksi 89% XSS & 76% SQLi	ZAP memiliki *false positive rate* 12% (perlu validasi manual)