BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan informasi menjadi salah satu tantangan utama yang dihadapi saat ini, seiring dengan meningkatnya kejahatan siber dan perkembangan teknologi yang berdampak pada keamanan siber [1]. Berdasarkan laporan tahunan Honeynet Project tahun 2023 Badan Siber dan Sandi Negara (BSSN), tercatat bahwa Indonesia mengalami 603 juta serangan siber dari 1,7 juta alamat IP penyerang dengan berbagai metode serangan [2]. Jumlah tersebut bertambah dari tahun sebelumnya yakni sebanyak 370 juta serangan siber dari 1,1 juta alamat IP penyerang [3]. Sebanyak 1,6 juta data dari 429 instansi terekspos berdasarkan laporan tahunan Lanskap Keamanan Siber Indonesia Tahun 2023 dari 103 dugaan insiden kebocoran data [4]. Jumlah ini bertambah dari tahun sebelumnya yakni sebanyak 27,9 ribu data dari 427 instansi terekspos dengan 311 dugaan pada 248 *stakeholder* [5]. Sebanyak 1,4 ribu aduan siber diterima pada tahun 2023 dari berbagai sektor, aduan tersebut kemudian dikategorikan menjadi 15 kategori dengan tiga kategori tertinggi adalah *Cybercrime*, *Vulnerable Indicator*, dan *Web Defacement* [4]. Berdasarkan hasil *Information Technology Security Assessment* (ITSA) tahun 2023 pada 138 instansi dengan jumlah 586 sistem elektronik, ditemukan sebanyak 2,8 ribu celah keamanan yang memiliki tingkat risiko yang beragam, diantaranya adalah *Insecure Direct Object Reference* (IDOR), *Broken Access Control* (BAC), SQL *Injection*, *File Upload Vulnerability*, dan *Privege Escalation* [4]. Menurut hasil survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2024, tercatat peningkatan jumlah pengguna internet, mencapai 221 juta pengguna atau 79,5% dari total populasi penduduk Indonesia [6]. Mengacu pada hasil survei yang diperoleh, APJII memprediksi jumlah pengguna internet di Indonesia akan terus mengalami peningkatan setiap tahun. Dengan bertambahnya jumlah pengguna layanan internet, maka akan banyak informasi yang bisa didapat melalui internet termasuk melalui aplikasi web.

Aplikasi web banyak digunakan dalam aktivitas sehari-hari, termasuk untuk layanan seperti *e-governance*, belanja, dan komunikasi [7]. Sebagian besar organisasi dan institusi menggunakan aplikasi web yang menyediakan kegiatan operasional penting dan menyimpan data sensitif. Dengan banyaknya penggunaan aplikasi web telah menarik perhatian peretas [7], yang ingin memanfaatkan kerentanan untuk melakukan tindakan kejahatan. Sekolah XYZ merupakan sekolah berprestasi yang menjadi salah satu dari institusi yang pernah mengalami peretasan pada aplikasi web mereka. Kegiatan peretasan dapat diminimalisasi dengan cara melakukan peningkatan keamanan melalui penilaian kerentanan terhadap aplikasi web secara berkala [8]. Terdapat beberapa metodologi yang dapat digunakan dalam kegiatan penilaian kerentanan, salah satu yang sangat direkomendasikan adalah *Open Web Application Security Project* (OWASP) *Testing Guides* [9]. OWASP *Testing Guides* dibagi menjadi tiga kategori bergantung pada jenis aplikasi yang digunakan, diantaranya adalah Web *Security*, *Mobile Security*, dan *Firmware Security*. Penggunaan metode OWASP dapat memberikan petunjuk dan penjelasan yang kompleks, dalam membantu pengembang menentukan langkah preventif pengambilan keputusan mengenai keamanan informasi pada aplikasi web [10]. OWASP juga terbukti efektif dan efisien dalam mengukur tingkat kerentanan aplikasi web, berdasarkan 10 kerentanan teratas OWASP sebagai tolok ukur dalam penentuan tingkat keparahan dan peringkat kerentanan [11]. Alat yang umum digunakan untuk menilai kerentanan aplikasi web pada metode OWASP adalah OWASP Zed *Attack Proxy* (ZAP), yang mendapatkan skor tertinggi pada kategori alat non-komersial ketika dibandingkan dengan alat pengujian penetrasi yang lain dalam hal pendeteksian kerentanan aplikasi web [12][13]. Validasi terhadap kerentanan yang telah di identifikasi penting dilakukan untuk mengurangi kemungkinan *false* positif dari hasil penilaian kerentanan yang telah dilakukan sebelumnya.

1.2. Rumusan Masalah

Berdasarkan latar belakang penelitian diatas, rumusan masalah pada penelitian ini ditentukan dari permasalahan mengenai keamanan informasi aplikasi web, dikarenakan banyaknya penggunaan aplikasi web oleh organisasi

maupun institusi sehingga menarik perhatian peretas yang ingin memanfaatkan kerentanan untuk melakukan tindakan kejahatan, ditambah aplikasi web Sekolah XYZ sebelumnya pernah mengalami peretasan. Sehingga dari masalah tersebut didapatkan rumusan masalah sebagai berikut:

1. Bagaimana hasil pengujian kerentanan pada aplikasi web Sekolah XYZ?
2. Bagaimana hasil analisis terhadap hasil temuan kerentanan pada aplikasi web Sekolah XYZ?
3. Bagaimana upaya mitigasi terhadap kerentanan yang ditemukan pada aplikasi web Sekolah XYZ?

1.3. Tujuan dan Manfaat

Tujuan dari penelitian ini diangkat dari rumusan masalah pada aplikasi web Sekolah XYZ, dengan melakukan analisis terhadap aplikasi web Sekolah XYZ dan menentukan upaya mitigasi terhadap kerentanan yang ditemukan. Maka didapatkan tujuan penelitian ini sebagai berikut:

1. Mengetahui hasil pengujian kerentanan terhadap aplikasi web Sekolah XYZ menggunakan metode OWASP
2. Mengetahui hasil analisis yang diperoleh dari hasil pengujian kerentanan aplikasi web Sekolah XYZ
3. Mengetahui upaya mitigasi yang dapat dilakukan terhadap kerentanan yang ada pada aplikasi web Sekolah XYZ

Penelitian ini diharapkan dapat memberikan dampak yang baik secara teoritis maupun praktis dalam bidang keamanan aplikasi web. Secara khusus, manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi Sekolah XYZ

   Memberikan informasi yang komprehensif terkait kerentanan keamanan pada aplikasi web, sehingga dapat membantu dalam meningkatkan keamanan aplikasi dan melindungi data pengguna dari potensi ancaman.
2. Bagi Pengembang

   Memberikan wawasan teknis terkait kelemahan yang ditemukan, serta memberikan panduan mitigasi yang dapat diimplementasikan untuk mengurangi risiko keamanan di masa depan.

3. Bagi Dunia Pendidikan

   Menambah literatur mengenai penerapan metode OWASP dalam pengujian keamanan aplikasi web, khususnya pada sektor pendidikan.

4. Bagi Peneliti atau Praktisi Keamanan Siber

   Memberikan referensi atau studi kasus nyata terkait pengujian kerentanan dan penerapan upaya mitigasi, yang dapat menjadi dasar untuk penelitian lanjutan atau praktik profesional.

5. Bagi Pengguna Aplikasi Web Sekolah XYZ

   Menjamin perlindungan data dan meningkatkan kepercayaan terhadap aplikasi yang digunakan, karena langkah-langkah mitigasi yang diambil dari penelitian ini diharapkan dapat mengurangi potensi ancaman keamanan.

1.4. Batasan Masalah

Terdapat beberapa batasan yang ditetapkan pada penelitian ini, agar fokus penelitian tetap terarah dan efisien. Batasan masalah ini ditujukan untuk membatasi ruang lingkup pekerjaan sehingga solusi yang dihasilkan dapat lebih mendalam dan relevan. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pengujian dilakukan terbatas pada aplikasi web milik Sekolah XYZ dengan domain XYZ.sch.id.
2. Pengujian dilakukan menggunakan metode *black box*, dimana penguji tidak memiliki akses ke kode sumber dan hanya berperan sebagai pengguna eksternal.
3. Pengujian berfokus pada 10 kerentanan teratas yang diidentifikasi oleh OWASP tahun 2021.
4. Analisis hasil pengujian serta rekomendasi upaya mitigasi didasarkan pada standar OWASP dan praktik terbaik yang berlaku pada saat pengujian dilakukan.

1.5. Jadwal Pelaksanaan

Berikut pada tabel 1.1 merupakan diagram batang dari jadwal pelaksanaan kegiatan penilitian ini:

Tabel 1.1 Jadwal Kegiatan

Kegiatan	Bulan					
	1	2	3	4	5	6
Analisa						
Pengumpulan Data						
Pengujian Situs Web						
Pengembangan Solusi						
Penulisan Laporan						