BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengujian sistem keamanan aplikasi berbasis web sangat penting saat ini dan perkembangan aplikasi web yang cepat. Semakin berkembangnya aplikasi web juga disertai dengan tingkat keamanan yang tinggi dari berbagai teknik ancaman dan serangan [1]. Meskipun organisasi memiliki banyak tindakan pencegahan seperti firewall, hal itu tidak cukup untuk melindungi sebuah aplikasi . Karena firewall tidak dapat melindungi aplikasi dari ancaman eksternal, tetapi firewall masih tetap diperlukan sebagai bagian dari keamanan jaringan [2]. Oleh karena itu, organisasi harus melakukan penilaian aplikasi web sehingga mereka dapat mendeteksi kerentanan dan memahami risiko yang mereka hadapi. Salah satu metode untuk menilai risiko kerentanan keamanan aplikasi berbasis web adalah Metode Penetration Testing [3].

OWASP Zed Attack Proxy adalah alat berbasis Java yang hadir dengan GUI intuitif yang memungkinkan penguji keamanan aplikasi web untuk melakukan serangan fuzz, script, spider, dan proxy terhadap aplikasi web [4]. Dari masing-masing faktor akan terdapat 3 resiko yang ditemukan diantaranya risk severity High, risk severity Medium dan risk severity Low [5]. Selain OWASP ZAP Acunetix adalah salah satu tools pemindai keamanan pada website. Acunetix Web Vulnerability Scanner adalah suatu layanan aplikasi internet yang berfungsi secara otomatis untuk melakukan pengujian keamanan pada aplikasi web Anda. Alat ini melakukan audit terhadap aplikasi internet dengan mendeteksi kerentanan seperti SQL Injection, Cross-Site Scripting, dan lainnya. Acunetix merupakan suatu alat otomatis yang membantu perusahaan dalam melakukan pemindaian terhadap aplikasi web mereka, dengan tujuan mengidentifikasi dan mengatasi kerentanan yang mungkin dapat dieksploitasi oleh pihak yang tidak berwenang atau hacker. Penulis menggunakan metode Penetration Testing dari Open Web Application Security Project (OWASP) dan analisa berdasarkan OWASP Top 10 2021. Penetration Testing adalah teknik yang dipakai untuk mengevaluasi kelemahan dalam sistem komputer, jaringan, atau aplikasi web. Ada tiga pendekatan yang

umum digunakan dalam pengujian penetrasi, yaitu Black Box Testing, White Box Testing, dan Gray Box Testing. Penetration Testing termasuk ke dalam White box Testing , juga dikenal sebagai "pengujian kotak putih," merujuk pada metode pengujian perangkat lunak yang menginvestigasi dan menganalisis struktur internal serta kode perangkat lunak. White box testing lebih menekankan pada pemahaman aliran input dan output yang terjadi dalam perangkat lunak dengan memeriksa secara detail elemen-elemen internalnya.Pengujian penetrasi bertujuan untuk mengidentifikasi dan mengumpulkan data terkait kerentanan atau celah keamanan sebagai dasar untuk perbaikan dan peningkatan keamanan pada server web.

Sebagai salah satu website ecommerce YAS-ID telah menerapkan sistem informasi yang berbasis Web. Namun, hingga saat ini, sistem informasi yang digunakan belum pernah diuji keamanannya. Sistem informasi berbasis web memiliki kerentanan keamanan yang dapat dieksploitasi melalui penggunaan akses Internet, menimbulkan kekhawatiran tentang eksploitasi kerentanan keamanan dalam sistem informasi tersebut. Pada penelitian ini peneliti menggunakan OWASP Top 10 2021 serta didukung oleh tools OWASP ZAP dan Security Headers untuk menganalisa kerentanan yang ada pada website YAS-ID dengan menggunakan metode Penetration Testing.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka dapat dirumuskan beberapa masalah yang akan dijawab dalam penelitian ini, yaitu:

1. Apakah OWASP ZAP dan Security Headers dapat menemukan kerentanan pada YAS-ID?
2. Kerentanan apa yang ditemukan pada domain YAS-ID dengan menggunakan OWASP ZAP dan Security Headers?
3. Apakah penambahan script dapat untuk meminimalisir kerentanan Content Security Policy, Cross Domain Misconfiguration, dan Anti Clickjacking Header?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan, maka dapat dirumuskan beberapa batasan masalah yang ada dalam penelitian ini, yaitu:

1. Penelitian dilakukan pada website YAS-ID .
2. Penelitian dilakukan berdasarkan metode OWASP TOP 10 2021
3. Penelitian ini dilakukan untuk meminimalisir kerentanan Content Security Policy, Cross Domain Misconfiguration, dan Anti Clickjacking Header

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan dari penelitian ini adalah :

1. Dapat mengetahui risiko celah keamanan pada domain YAS-ID menggunakan OWASP ZAP dan Security Headers
2. Dapat mengidentifikasi jenis kerentanan yang ditemukan dengan OWASP ZAP pada YAS-ID.
3. Dapat memberikan solusi terkait kerentanan Content Security Policy, Cross Domain Misconfiguration, dan Anti Clickjacking Header pada website tersebut.

1.5 Manfaat Penelitian

1. Meminimalisir resiko eksploitasi pada website YAS-ID dan dapat membantu dalam mengevaluasi dari perspektif keamanan nya.
2. Sebagai bahan pertimbangan dalam pengembangan institusi terkait keamanan website baik secara teknis maupun non teknis.

3. Menjadi acuan penelitian selanjutnya tentang keamanan jaringan atau keterkaitan dengan tema penelitian bagi mahasiswa maupun pembaca.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang digunakan.

BAB III METODE PENELITIAN, berisi metode dan proses yang diterapkan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN, berisi tentang pembahasan terkait penelitian yang sedang dilakukan berdasarkan metode yang diterapkan.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.