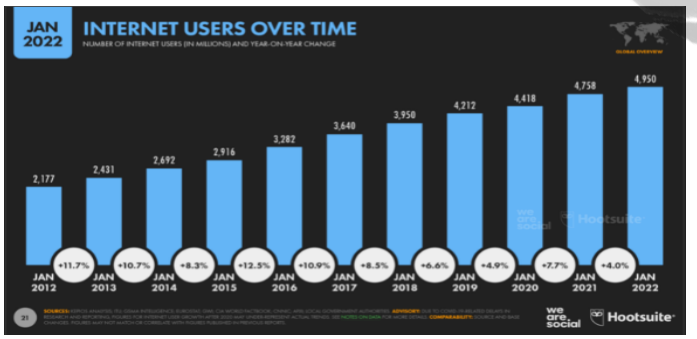
BAB 1

PENDAHULUAN

1.1 Latar Belakang

Selama beberapa dekade terakhir, teknologi informasi telah membuat lompatan besar. memberikan dampak positif yang signifikan bagi kehidupan manusia. Internet merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. [Ari Muzakir, A., 2022]. OWASP Zed Attack Proxy adalah alat berbasis Java yang hadir dengan antarmuka grafis intuitif, memungkinkan penguji keamanan aplikasi web untuk melakukan fuzzing, scripting, spidering, dan proxy untuk menyerang aplikasi web. [Obbayi, L. 2018]. ZAP dirilis pada 6 September 2010. Pada titik tertentu di bulan Desember, ZAP diterima sebagai proyek OWASP dan pada 1 Januari 2011 unduhan melonjak dari hampir tidak ada menjadi 433. [Simon Bennetts. 2021]. OWASP bertujuan untuk meningkatkan keamanan perangkat lunak, [BasuMallick, C. 2022]. Disini peneliti manjadikan website jamas sebagai bahan penelitian uji coba, celah keamanan dapat dijumpai dalam sebuah sistem maupun jaringan. [Dewi, B.T.K. and Setiawan, M.A., 2022]. Situs jamas merupakan website e-commerce berfokus pada masakan rumahan yang berdiri pada tahun 2021. Alasan peneliti menggunakan situs ini agar dapat membantu website jamas untuk meningkatkan keamanan sehingga dapat beroperasi dengan lebih aman tanpa takut dengan adanya serangan dari orang yang tidak bertanggung jawab.



Gambar 1.1 *GLOBAL OVERVIEW REPORT*

Data terbaru menunjukkan bahwa pengguna internet tumbuh 192 juta selama 12 bulan terakhir, menghasilkan pertumbuhan tahunan hanya 4,0 persen pada tahun 2021. Namun, kami sangat menduga bahwa angka pertumbuhan yang lebih rendah ini kemungkinan besar merupakan konsekuensi dari tantangan yang terkait dengan pengumpulan dan pelaporan data selama pandemi COVID-19 yang sedang berlangsung, dan bahwa angka-angka ini tidak mencerminkan pertumbuhan aktual pengguna internet selama setahun terakhir. Akibatnya, ada

peluang yang sangat bagus bahwa kami akan melaporkan angka pertumbuhan yang lebih tinggi antara tahun 2021 dan 2022 setelah data yang lebih baru tersedia. (Kemp, S. 2022).

Saat ini, aplikasi web memainkan peran penting dalam membuat hidup manusia lebih mudah. Mereka membuat kehadiran yang mulia di bidang-bidang seperti pendidikan, perbankan, hiburan, pemasaran, dan komunikasi. Beberapa contoh penting adalah belanja online, perbankan online, jejaring sosial, pengeditan dokumen online, pengeditan media online, layanan peta online, kamus online, layanan pencarian online, dan game.

Aplikasi ini memberikan layanan kepada orang-orang sesuai dengan kebutuhan mereka secara efisien dan hemat biaya. Namun, hanya menjadi efisien dan hemat biaya saja tidak cukup. Aplikasi ini harus aman dan dapat diandalkan juga. Penggunaan aplikasi yang tidak aman dan tidak dapat diandalkan mungkin selalu berdampak serius karena dapat membuat perusahaan gulung tikar. Seiring dengan meningkatnya ketergantungan hidup manusia pada layanan web. Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi dan perusahaan. [Dina, D., Dedy, S. and Yesi Novaria, K., 2020]., Selama dekade terakhir, seiring dengan perkembangan teknologi web, teknik menyerang baru juga muncul. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbabagai teknik ancaman. [Ghozali, B., Kusrini, K. and Sudarmawan, S., 2019]. Sebelum menyerang, penyerang terlebih dahulu mencoba mengetahui kerentanan dalam aplikasi yang ingin mereka serang, dan kemudian menggunakan kemampuan kerentanan yang mereka temukan untuk melakukan serangan yang diinginkan. Hacker merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan computer. [Yunanri, Y., Riadi, I., & Yudhana, A. 2017]. Dalam hitungan detik, seorang pencuri virtual dapat mengakses sistem dan mencuri informasi penting, seperti password. [Ilman, Z.Y. and MM, M., 2022]. Teknologi informasi merupakan salah satu aset yang sangat berharga baik itu bagi perusahaan atau instansi yang telah menerapkan teknologi informasi dalam proses bisnisnya. [Kurnia, R. and Suryayusra, S., 2021]. Penggunaan aplikasi yang rentan selalu berbahaya bagi semua pemangku kepentingan. Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak resiko yang ditemukan pada sistem. [Listartha, I.M.E., Mitha, I.M.A.P., Arta, M.W.A. and Arimika, I.K.W.Y., 2022]. aplikasi harus selalu diuji secara menyeluruh untuk segala jenis kerentanan yang mungkin terjadi. Banyak alat tersedia untuk menguji kerentanan dalam aplikasi web. Beberapa dari mereka gratis, dan yang lainnya komersial. Mereka memindai aplikasi dengan keduanya cara otomatis dan manual. OWASP Zed Attack Proxy (ZAP), pemindai open source

yang mudah digunakan untuk menemukan kerentanan dalam aplikasi web. Ini adalah salah satu proyek unggulan OWASP yang direkomendasikan oleh OWASP untuk pengujian kerentanan aplikasi web. [Mburano, B. and Si, W., 2018]. Untuk penelitian ini akan melakukan scanning dengan alat pengujian penetrasi aplikasi web dari OWASP, yang disebut Zed Attack Proxy.

1.2 Rumusan Masalah

Perkembangan teknologi yang pesat membuat banyaknya tindakan kejahatan di dunia internet dan website atau aplikasi memiliki kemungkinan di serangn oleh orang yang tidak bertanggung jawab seperti hacker untuk kepuasan diri mereka sendiri.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini antara lain:

- Melakukan pemeriksaan kerentanan atau celah yang ada pada website agar dapat mengurangi dan mencegah terjadinya serangan yang di lakukan oleh pihak yang tidak bertanggung jawab
- Agar dapat mengetahui tingkat keparahan berupa skor pada kerentanan yang ditemukan
- Dan dapat di gunakan sebagai bahan pertimbangan untuk dapat membantu meningkatakan keamanan pada website

1.4 Ruang Lingkup Penelitian dan Batasan Masalah

Dalam penyusunan dan penulisan tugas akhir ini perlu adanya pengertian pada pembahasan yang terfokus sehingga permasalahan tidak melebar. Untuk mempermudah pemahaman dan memberikan gambaran serta menyamakan persepsi antara penulis dan pembaca, maka dikemukakan penjelasan yang sesuai dengan variabel dalam penelitian ini. Adapun batasan dalam penelitian ini adalah:

1. Uji coba *penetrasi testing* dilakukan hanya pada situs jago masak.
2. Hasil yang di peroleh hanya di tunjukan kepada pihak koding terkait tentang jago masak.

1.5 Manfaat Penelitian

Pada Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Agar dapat mengurangi dan mencegah terejadinya kehilangan, pencurian data dan lain lain yang di sebabkan oleh orang yang tidak bertanggung jawab seperti hacker.
2. Pengguna atau *client* yang menggunakana website dapat berselancar dengan nyaman tanpa takut terjadinya pencurian data dan dapat membuat pengguna merasa lebih yakin dengan website yang mereka gunakan.

1.6 Metodologi Penelitian

1.6.1 Waktu Penelitian

Waktu penelitian ini dimulai dari bulan Desember sampai dengan April 2022 mencakup kegiatan dalam Langkah-langkah penelitian hingga pelaksanan penelitian.

1.6.2 Alat dan Bahan

Pada Penelitian ini menggunakan alat dan bahan sebagai berikut :

a. Hardware (Perangkata Keras), yang terdiri dari :
- Laptop dengan *processor* Intel Core i5, 8GB RAM, dan VGA Nvidia GeForce MX130
- Modem Indihome

b. Software (Perangkat Lunak), yang terdiri dari :
- Sistem Operasi Windows 11.
- Kali Linux digunakan untuk melakukan uji coba penyerangan terhadap situs jago masak.
- OWASP ZAP adalah alat yang akan di gunakan untuk uji coba penyerangan situs jago masak.
- Nmap digunakan untuk mengetahui port bepara saja yang sedang terbuka.
- Who.is digunakan untuk mengetahui apakah aplikasi yang di tuju aktif atau tidak dan menunjukan alamat ip pada situs tersebut.
- CVSS digunakan untuk menampilkan tingkat kelemahan berupa angka.
- Wappalayzer digunakan untuk mengetahui teknologi apa saja yang digunakan di dalam website tersebut.

1.6.3 Metode Pengumpulan Data

Berikut merupakan metode pengumpulan data yang dilakukan dalam penelitian ini :

a. Observasi

Observarsi adalah kegiatan mengamati objek penelitian secara langsung guna untuk mengumpulkan data. Pada penelitian ini peneliti melakukan observasi pada website jago masak untuk mendapatkan informasi yang dibutuhkan untuk melakukan uji coba.

b. Studi Pustaka

Studi Pustaka merupakan Teknik pengumpulan data dengan cara membaca buku, jurnal, serta sumber lain yang sesuai dengan data yang di perlukan dalam penelitian. Studi Literatur pada penelitian kali ini yaitu dengan mencari referensi dari internet yang berkaitan dengan judul penelitian serta jurnal yang memiliki kemiripan dengan judul penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi yang digunakan, dapat diluraikan sebagai berikut:

BAB I PENDAHULUAN

Di Bab ini, berisi tentang penjelasan mengenai latar belakang, perumusan masalah, tujuan penelitian, ruang lingkup dan Batasan masalah, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Di Bab ini, berisi tentang penjelasan terkait *Penetrasi Testing* serta uraian mengenai teori-teori yang digunakan sebgai landasan atau acuan dalam melaksanakan penelitian.

BAB III ANALISA DAN KEBUTUHAN

Di Bab ini, berisi tentang analisa perancangan dan kebutuhan dalam uji coba *penetrasi testing* pada situs jago masak.

BAB IV HASIL DAN PEMBAHASAN

Di Bab ini, berisi tentang penjelasan hasil uji coba beserta penjelasan terkait penggunaan OWASP ZAP dan fitur-fitur di dalamnya.

BAB V KESIMPULAN DAN SARAN

Bagian terakhir yang berisi kesimpulan dan juga saran dari peneliti untuk situs jago masak.