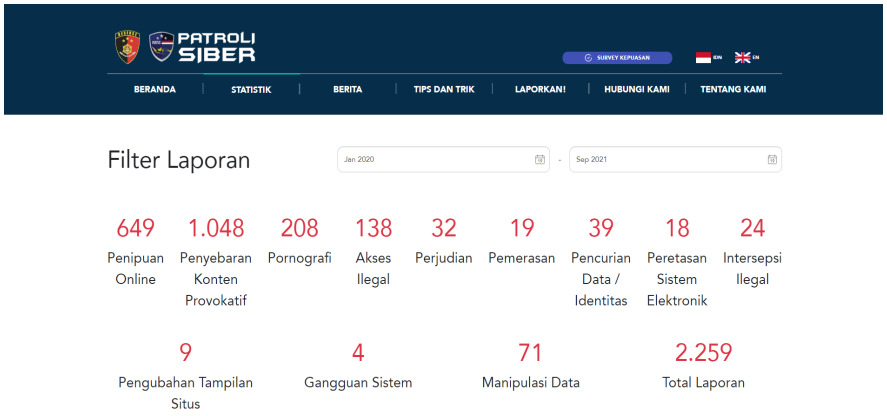
BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini perkembangan teknologi semakin maju dan canggih, mulai dari sistem penyimpanan yang tidak lagi membutuhkan sebuah perangkat keras seperti *harddisk*, *flashdisk*, dll. Sehingga semua data penting yang kita miliki dapat disimpan secara *online*. Namun perkembangan teknologi juga memiliki dampak negatif seperti data yang dicuri pada situs yang kita gunakan untuk menyimpan data oleh peretas atau *hacker* yang tidak bertanggung jawab. Namun setiap data yang dicuri tidak selalu data yang penting, hal ini dikarenakan peretas tidak pandang bulu dalam melakukan peretasan. Alasan peretas yang mencuri segala jenis data karena selama data tersebut memiliki sebuah nilai dan dapat menghasilkan, maka peretas akan mencoba untuk mencuri data tersebut demi keuntungannya sendiri atau orang lain yang membutuhkan data tersebut. Selain itu masih banyak lagi jenis kasus kejahatan yang dilakukan oleh para *hacker* tersebut. Berdasarkan data yang dirangkum dari patroli siber pada bulan Juni 2020 sampai dengan bulan September 2021 terdapat 2.259 laporan yang diajukan dan tercatat pada situs patroli siber, pada gambar 1.1merupakan infografis dari laporan tersebut (PatroliSiber, 2021).



Gambar 1. 1 Statistik Laporan Tindak Kejahatan Online

Dengan adanya tindak kejahatan online atau biasa disebut dengan *cybercrime,* maka diperlukan sebuah sistem keamanan yang dapat mencegah terjadinya tindak kejahatan tersebut. Salah satu tindakan yang dapat diambil dalam melakukan pencegahan *cybercrime* pada suatu situs dengan melakukan *Vulnerability Scanning,* hal ini bertujuan untuk mengetahui celah keamanan pada suatu situs yang rentan untuk diserang oleh peretas. Selain itu juga dilakukan *Penetration Testing* yaitu proses simulasi penyerangan yang dilakukan terhadap suatu sistem untuk memastikan apakah benar-benar ada kerentanan pada suatu sistem dan dapat merusak sistem tersebut.

Pada penulisan skripsi ini, akan dilakukan *Penetration Testing* terhadap *Buggy Web Application* (bWAPP). Hal ini dilakukan untuk analisis terhadap dampak yang ditimbulkan jika suatu situs terinfeksi oleh serangan yang memanfaatkan kerentanan atau *vulnerability* berupa *Insecure Design,* dan *Server Side Request Forgery* (SSRF). Adapun dua jenis kerentanan yang akan dianalisis dipilih berdasarkan jenis kerentanan atau risiko yang baru ditambahkan pada OWASP Top Ten 2021.

Adapun metode yang akan digunakan adalah *Penetration Testing Execution Standard* (PTES). Metode ini memiliki 5 (lima) tahapan yaitu *Intelligence Gathering, Vulnerability Analysis, Exploitation, Pos-Exploitation,* dan *Report*. Di dalam metode tersebut terdapat beberapa skenario serangan yang kemungkinan dapat terjadi pada suatu situs. Namun

penulis tidak akan menjalankan semua skenario yang ada, melainkan hanya dua kategori risiko atau kerentanan yang baru ditambahkan pada OWASP Top Ten 2021.

1.2. Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka identifikasi masalah adalah sebagai berikut:

1. Ditambahkannya dua kategori risiko atau kerentanan baru pada OWASP Top Ten 2021.
2. Risiko atau kerentanan *Insecure Design* yang baru ditambahkan menempati peringkat 4 dari 10 kerentanan.
3. Risiko atau kerentanan *Server Side Request Forgery* (SSRF) yang baru ditambahkan sebelumnya termasuk ke dalam salah satu kategori tertentu, namun saat ini memiliki kategori tersendiri.

1.3. Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dijelaskan sebelumnya, maka diperoleh rumusan masalah:

1. Apa saja dampak yang ditimbulkan oleh kerentanan *Insecure Design* dan *Server Side Request Forgery* (SSRF) (terhadap objek kasus penelitan bWAPP 2.2)?
2. Bagaimana cara untuk mengatasi kerentanan dan risiko tersebut (terhadap objek kasus penelitan bWAPP 2.2)?

1.4. Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, maka diperoleh Batasan masalah:

1. Aplikasi yang akan digunakan untuk melakukan pengujian kerentanan, yaitu *Buggy Web Application* (bWAPP).
2. Penelitian ini menggunakan Sistem Operasi Windows 10 untuk pembutan laporan dan Kali Linux untuk pengujian serangan.
3. Pengujian kerentanan dilakukan berdasarkan metode PTES.
4. Tahapan *Vulnerability Analysis* tidak akan dilakukan, karena tidak dibutuhkan *scanning vulnerability* pada penelitian ini.

5. Tahapan *Post Exploitation* tidak akan dilakukan, karena tidak dibutuhkan mempertahankan akses dalam penelitian ini.
6. Jenis kerentanan yang akan diuji berdasarkan dengan OWASP Top Ten 2021 adalah *Insecure Design* dan *Server Side Request Forgery* (SSRF).

1.5. Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut:

1. Melakukan pengujian dan analisis terhadap kerentanan *Insecure Design* dan *Server Side Request Forgery* (SSRF).
2. Menjabarkan hasil pengujian dan analisis serta memberikan solusi yang dapat dilakukan untuk memperbaiki celah kerentanan tersebut.

1.6. Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Bagi Penulis

a. Untuk memenuhi salah satu syarat kelulusan Strata Satu (S1), Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
b. Mendapatkan pengetahuan dan pemahaman mengenai dampak terjadinya penyerangan atau peretasan pada suatu situs.
c. Mendapatkan pengetahuan dan pemahaman mengenai bagaimana cara menangani suatu serangan dan peretasan pada suatu situs.

2. Bagi Universitas

a. Sebagai kontribusi karya ilmiah dalam disiplin ilmu Informatika.
b. Sebagai tambahan referensi terhadap penelitian keamanan sistem selanjutnya.

3. Bagi Masyarakat

a. Menambah pengetahuan mengenai sistem keamanan suatu situs.
b. Menambah pengetahuan mengenai dampak terjadinya suatu serangan atau peretasan pada suatu situs.
c. Menambah pengetahuan mengenai cara menangani suatu serangan atau peretasan pada suatu situs.
d. Sebagai acuan untuk referensi terhadap penelitian dengan topik serupa.

1.7. Sistematika Penulisan

Sistematika penulisan skripsi ANALISIS KERENTANAN *INSECURE DESIGN* DAN *SERVER SIDE REQUEST FORGERY* DENGAN METODE PTES (STUDI KASUS *BUGGY WEB APPLICATION*) sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan secara singkat dan jelas mengenai latar belakang permasalahan, identifikasi masalah, rumusan masalah, Batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan

BAB II LANDASAN TEORI

Bab ini berisi uraian mengenai berbagai literatur yang berkaitan dengan teori/konsep/prosedur/metode/proses yang berkaitan dengan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan langkah-langkah penelitian yang digunakan untuk pemecahan permasalahan penelitian dan mencapai tujuan penelitian. Metodologi harus diuraikan tahap demi tahap secara rinci.

BAB IV PEMBAHASAN

Bab ini berisi pembahasan hasil penelitian yang memuat objek penelitian, analisis, desain dan implementasinya.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran. Kesimpulan memuat hal-hal yang sudah dibahas pada bab-bab sebelumnya mulai dari permasalahan, analisis sampai dengan hasil penelitian. Saran memuat hal-hal yang perlu dilakukan oleh peneliti selanjutnya (dapat berupa hal-hal yang belum dilakukan oleh penulis dalam penelitian).