BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kemanan sistem informasi saat ini sangat penting karena diiringi majunya teknologi informasi dan banyaknya kebutuhan orang yang menggunakannya untuk mendukung operasi dan manajemen sehingga dapat menimbulkan banyaknya serangan yang terjadi. Mulai 1 Januari 2020 sampai 12 April 2020 Badan Siber dan Sandi Negara (BSSN) telah mencatat 88.414.296 serangan siber. Jumlah serangan siber paling besar terjadi pada tanggal 12 Maret 2020 yang mencapai angka 3.344.470 serangan. Namun, setelah mencapai angka itu jumlah serangan mengalami penurunan cukup signifikan saat diberlakukannya kebijakan *Work From Home* (WFH) di berbagai tempat (BSSN, 2020). Kegiatan *Work From Home* yang dilakukan secara massal telah menyadari tingkat kekhawatiran dan tantangan keamanan dunia maya yang belum pernah dihadapi oleh industri dan warga negara (Lallie dkk, 2020:1). Contoh serangan siber yang paling sering terjadi dan sudah banyakw dijelaskan dan dipelajari adalah *Man in the middle attack, Brute force attack, Distributed Denial of Service (DDoS), Malware, Phising, dan social engineering* serta serangan berbasis *web.* (Bendovschi, 2015). Serangan berbasis *web* pun memiliki berbagai jenisnya dan serangan yang sering dilancarkan untuk merusak infrastruktur adalah *Cross Site Scripting (XSS) dan Structured Querry Language (SQL) Injection* (Muammar, 2013). Contoh lain serangan berbasis *web* adalah *Unauthorized Access, Phising, dan Malware.* (Kaur dan Kaur, 2016 hlm 300).

Setelah mengetahui jenis dan jumlah serangan yang telah terjadi, maka keamanan sistem informasi juga harus menjadi perhatian berbagai pihak. Salah

satu cara meningkatkan keamanan sistem informasi adalah dengan mengetahui celah keamanan sistem informasi itu sendiri. Salah satu cara untuk mengetahui celah keamanan adalah dengan melakukan *Penetration Testing (pentest).* Adapun salah satu metode yang akan digunakan di penilitian ini yaitu *Zero Entry Hacking* (ZEH). Metode *Zero Entry Hacking* (ZEH) merupakan metode yang memungkinkan semua orang dapat mengimplementasikannya karena metode ini dirancang untuk digunakan dengan mudah (Engrebetson, 2013).

Keamanan jaringan sendiri memiliki 3 dasar untuk menentukan jaringan tersebut aman yang biasa disebut CIA TRIAD. *Confidentiality* (kerahasiaan) kerahasiaan yang dijamin dari pihak luar yang tidak memiliki hak, *Integrity* (integritas) menjaga agar informasi tidak berubah dari pihak luar dan *Availability* (ketersediaan) menjaga agar informasi selalu tersedia untuk diakses. Jika melihat dari konsep tersebut, nampak bahwa ketiga bertujuan sebagai keamanan mendasar untuk kedua data dan informasi serta layanan komputasi, sehingga konsep tersebut dapat menjadi acuan untuk terhindar dari serangan yang ada (Yuliansyah, 2014 hlm 1). Dalam mengatasi masalah tersebut salah satu langkahnya adalah dengan melakukan *penetration testing* guna mencari kelemahan terhadap web *Damn Vulnerable* (DVWA). Penelitian ini berfokus pada *penetration testing (pentest)* dengan menggunakan metodologi *Zero Entry Hacking* (ZEH) dan *Open Web Application Sercurity* (OWASP).

1.2 Rumusan Masalah

1. Bagaimana cara untuk mengetahui kondisi serta tingkat keamanan sistem *website* DVWA?
2. Apa saja celah keamanan yang di lakukan eksploit pada website DVWA?
3. Apa saja solusi yang bisa diberikan terhadap celah keamanan dari *website* DVWA?

1.3 Ruang Lingkup

1. Aplikasi berbasis *web* yang akan diuji adalah aplikasi *web Damn Vulnerable Web App* (DVWA) melalui *localhost*.
2. Proses eksploitasi kerentanan yang dilakukan hanya *cross site scripting* (XSS), *command injection, file inclusion, file upload, brute force attack, SQL Injection*
3. Pengujian kerentanan dengan menggunakan metodologi *Zero Entry Hacking* (ZEH) dan solusi yang diberikan berdasarkan *Open Web Application Security Project* (OWASP)

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah

1. Melakukan pengujian kerentanan untuk mengetahui kondisi keamanan *website* DVWA
2. Menjabarkan celah keamanan yang perlu untuk diperbaiki.

1.5 Manfaat Penelitian

Manfaat penelitian ini bagi pengembangan IPTEK dapat menambah pengetahuan dalam bidang teknologi, khususnya bidang keamanan tentang sistem informasis berbasis website serta bisa diharapkann menjadi referensi u ntuk penelitian terkait pada penelitian mendatang.

1.6 Luaran yang Diharapkan

Luaran yang diharapkan berupa hasil laporan kerentanan aplikasi *web Damn Vulnerable Web App* (DVWA) dengan penjabaran yang dapat dimengerti semua orang.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini sebagai berikut:

BAB 1 PENDAHULUAN

Pada Bab 1 Pendahuluan, menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, luaran yang diharapkan, dan sistematika penulisan dalam Menyusun skripsi ini.

BAB 2 LANDASAN TEORI

Pada Bab 2 Landasan Teori, menjelaskan teori- teori mendasar yang mendukung dan berkaitan dengan penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Pada Bab 3 Metodologi Penelitian, menjelaskan metode yang digunakan dalam penelitian sehingga penelitian ini dapat mencapai tujuan.

BAB 4 HASIL DAN PEMBAHASAN

Pada Bab 4 Hasil dan Pembahasan, menjelaskan bagaimana tahapan proses yang dilakukan dalam penelitian dari masalah yang terkait sehingga mencapai hasil dan tujuan sesuai dengan yang diteliti.

BAB 5 PENUTUP

Pada Bab 5 Penutup, menjelaskan mengenai kesimpulan dari hasil penelitian yang diteliti, serta saran sebagai sarana pemecahan masalah untuk penelitian berikutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN