BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet menjadi teknologi terbesar yang terus berkembang penggunanya di Indonesia. Jumlah pengguna internet saat ini telah mencapai 213 juta orang per Januari 2023. Jumlah ini setara 77% dari total populasi Indonesia sebanyak 276,4 juta orang [1]. Aktifitas pengguna internet yang digunakan adalah *browser* untuk menjelajahi dunia maya serta mencari informasi. Saat ini, informasi dapat ditemukan pada halaman website sebagai sarana media informasi. Website dapat mencakup berbagai jenis informasi, mulai dari artikel hingga produk atau layanan yang sangat mudah terjangkau oleh konsumen yang lebih luas melalui akses internet[2].

Selain mudah diakses dan digunakan, website juga menampilkan halaman yang *user-friendly* bagi pengguna yang menggunakan internet untuk menemukan informasi. Tak kalah penting, website harus memiliki pertahanan keamanan yang kuat agar terhindar dari tindakan kebocoran, pencurian data dan manipulasi[3]. Secara umum keamanan dinilai secara tiga faktor utama yang disingkat yaitu CIA atau *Confidentiality*, *Integrity* dan *Availability*. Ketiga faktor utama tersebut saling mengikat satu sama lain untuk melindungi informasi dari tiga sisi faktor yang berbeda sehingga disebut dengan segitiga CIA[4].

Pengelola Website Launchinpad atau disebut Launchinpad Repository Management Project adalah suatu penyimpanan projek mahasiswa/i dari launchinpad.com. Launchinpad dikembangkan oleh dosen prodi informatika Universitas Amikom Yogyakarta yang mengembangkan serta merancang tampilan landingpage website yang bertujuan untuk mengapresiasi mahasiswa/i dalam menyelesaikan projek mata kuliah dan hasil projeknya akan diterbitkan di halaman website launchinpad.com.

Berdasarkan hasil observasi dan wawancara yang telah dilakukan peneliti terkait dengan keamanan website launchinpad.com ditemukan bahwa jenis vulnerability atau kerentanan yang memiliki jenis tipe ancaman yang berbeda dalam melakukan penyerangan pada website launchinpad.com. Pada proses ini peneliti melakukan uji penyerangan tahapan awal untuk mengenal pola atau alur kerja sistem website dengan metode scanning dalam mengumpulkan informasi website launchinpad.com terlebih dahulu. Setelah melewati proses tersebut dapat terlihat kurangnya keamanan aplikasi website untuk menjaga kredensial informasi pengguna pada sistem keamanan yang digunakan oleh website[5].

Hasil pengujian penyerangan tahapan awal peneliti mengidentifikasi beberapa celah keamanan yang memungkinkan penyerang untuk mendapatkan informasi webserver yang digunakan dalam mengembangkan aplikasi website. Penemuan tampilan informasi webserver merupakan kesalahan yang terjadi disisi direktori info.php merupakan lokasi webserver yang berisi file PHP untuk memberikan informasi tentang konfigurasi server, versi PHP, ekstensi yang diaktifkan, dan informasi penting lainnya terkait dengan lingkungan server[6].

Solusi dalam permasalahan keamanan website aplikasi mengacu pada penerapan teknik dan prinsip pengembangan perangkat lunak yang aman, seperti penggunaan validasi input, menghindari SQL dan XSS serta penggunaan library dan framework yang aman. Penelitian keamanan webserver dan SSL telah dilakukan pada penelitian sebelumnya. Diantaranya penelitian yang oleh nazwita dan ramadhani. Dalam penelitian menganalisis keamanan web server dan SSL telah dilakukan penyerang mencoba untuk menyusup melalui port yang telah discanning[7]. Penelitian dalam menerapkan keamanan terhadap kerentanan SQL Injection yang dilakukan oleh Asnawi, Dedy, Ulfi, Puji. penelitian yang diusulkan untuk berkolaborasi penanganan serangan menggunakan struktur alur NIST (*National Institute of Standards and Technology*) SP 800-53 sebagai fundamental penanganan pelaku attacker (penyerang)[8]. Melalui penelitian yang menggunakan konsep analisis kerentanan aplikasi web menggunakan kombinasi *tool* yang dilakukan oleh Moh Yunus. Masalah kerentanan dapat berupa serangan *Malware, Eksploitasi* dan *infeksi database.* Solusi pengamanan web dari gangguan atau penyerang dapat dilakukan dengan *self test* yaitu pengujian yang dilakukan terhadap website secara legal dengan aktivitas menyerupai penyerang atau hacker[9].

Untuk menemukan dan mengidentifikasi suatu kerentanan, dengan melakukan analisis kerentanan website menjadi tujuan penelitian dalam memahami potensi ancaman celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, sehingga dapat diambil langkah-langkah pencegahan yang tepat untuk meningkatkan keamanan dan integritas website launchinpad.com[10].

Langkah-langkah yang dilakukan merupakan output dari penelitian. Proses tersebut akan dilaporkan secara etis kepada pihak narasumber atau pengelola website launchinpad.com. Dengan melihat hasil perbandingan yang dilakukan, setelah mengirimkan laporan dokumentasi dan melakukan penyerangan kembali dalam bentuk analisis untuk mencoba membandingkan setelah mengirimkan laporan ke pihak launchinpad.com.

Dampak dari ancaman kerentanan tentunya berkaitan dengan pelaku kejahatan dalam mengurangi resiko pencurian data pengguna seperti data diri, email, dan lainnya. Pernyataan ini dapat diuji kebenarannya dengan melakukan simulasi penyerangan dan analisis terhadap

keamanan website. Hal ini mengacu pada dua sosok yang ekpert (pakar) dalam pengelolahan website dan penetration tester. Peran penetration tester dan developer tidak hanya merancang dan deploy website aplikasi, juga harus memperhatikan keamanan dari aplikasi, maka pernyataan tersebut dapat dianggap benar[11]. Peneliti melakukan tindakan dalam evaluasi keamanan website launchinpad.com, aplikasi atau infrastruktur untuk mengidentifikasi potensi kerentanan dan mengevaluasi kesiapannya dalam menghadapi serangan. Peran peneliti melakukan simulasi serangan sebagai *penetration tester* merupakan aktivitas profesional keamanan informasi yang bertanggung jawab untuk melakukan uji penetrasi. Dengan memiliki keahlian dan pengetahuan mendalam dalam mengidentifikasi, mengeksploitasi, dan memberikan solusi untuk kerentanan keamanan[12]. Aktivitas ini dilakukan secara resmi dan telah mendapatkan izin untuk melakukan kegiatan *Penetration Testing*. Hal ini dilakukan untuk menguji dan melihat hasil perspektif penyerangan eksternal (serangan luar) yang tidak memiliki pengetahuan terhadap gambaran aplikasi yang akan diserang[13] dan akan berdampak dengan kondisi yang dimiliki oleh launchinpad.com.

Aplikasi website repository atau penyimpanan yang merujuk pada literature review terdahulu penelitian yang dilakukan oleh Aditya Wibisono Kuncoro untuk menguji apakah metode yang diterapkan keamanan *OWASP* (*Open Web Aplication Security Project*) digunakan untuk mendeteksi celah keamanan pada sistem aplikasi web dan melakukan perbandingan hasil penemuan[14]. Penelitian ini menerapkan aplikasi scanner *Vulnerability* untuk mengetahui bagian dari struktur development (pengembangan) yaitu *Simple Object Access Protocol* (SOAP) merupakan pembahasan kerentanan yang sering terjadi dalam development (pengembangan) SOAP[15].

Kelebihan melakukan *Penetration Testing* yaitu melibatkan peneliti dalam melakukan proses pengujian sistem dari luar tanpa pengetahuan yang mendalam tentang struktur internal atau kode sumber aplikasi. Dan mengungkapkan hasil penemuan celah kerentanan yang tidak terlihat atau tidak diketahui secara keseluruhan pada sistem[16].

Oleh karena itu, *Penetration Testing* memberikan fakta yang dapat dijelaskan. Dengan alasan yang jelas peneliti telah memutuskan untuk memilih judul skripsi "Analisis Kerentanan Website Launhcinpad Repository Management Project".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas maka, rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana menemukan kerentanan pada website launchinpad.com dengan melakukan *Penetration Testing*?
2. Bagaimana pengujian kerentanan pada website launchinpad.com?
3. Bagaimana hasil dari metode *NIST* yang diterapkan pada *Penetration Testing* website launchinpad.com?
4. Apa saja ancaman utama terhadap keamanan website saat ini?

1.3 Batasan Masalah

Berdasarkan batasan masalah yang telah diuraikan, maka peneliti melakukan batasan masalah terhadap masalah penelitian yang sedang dilakukan sebagai berikut:

1. Melakukan *Penetration Testing* pada website launchinpad.com.
2. Penelitian ini diawali dengan menggunakan sistem operasi *Windows 10* dan *Kali Linux* versi 2023.
3. Penelitian ini menggunakan beberapa tahapan utility dan *tools* yaitu *Whois, Ping, Host, scan SSL, Dirsearch, NMAP*, dan *Burp Suite*.
4. Peneliti akan memusatkan perhatian pada analisis dan implementasi secara teknis untuk mengungkap penemuan kerentanan seperti *SQL Injection*, *Cross-site scripting* (*XSS*), dan serangan lainnya.
5. Penelitian ini melibatkan *Penetration Tester* melakukan pengujian dengan menggunakan metode *NIST*, dan tindakan *Penetration Testing*.

1.4 Tujuan Penelitian

Tujuan penelitan yang ingin dicapai dalam penelitian adalah untuk menganalisis dan memahami dampak dari kerentanan keamanan website terhadap keberlangsungan projek dan integritas data serta mengidentifikasi strategi pencegahan dan mitigasi yang efektif dalam menghadapi pencegahan keamanan digital. Dengan tujuan mengidentifikasi potensi celah keamanan yang dapat dieksploitasi oleh penyerang. Selain itu, penelitian ini bertujuan untuk mengembangkan strategi perlindungan yang efektif dan praktis untuk mengurangi resiko keamnan website launchinpad.com serta memperkuat integritas, kerahasiaan, dan ketersediaan informasi yang disimpan dan diproses oleh website launchinpad.com.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah memberikan solusi dan masukan tentang faktor penyebab adanya celah kerentanan. Peneliti juga berkontribusi secara langsung terhadap Launchinpad, Universitas Amikom Yogyakarta.

a. Oleh Peneliti :
   1. Menjadi salah satu syarat peneliti untuk mendapatkan gelar Sarjana Komputer (S.Kom)
   2. Mendapatkan ilmu pengetahuan dan pengalaman dalam melakukan *Penetration Testing* dalam bidang Informatika
b. Oleh Lauchinpad :
   1. Menjalin hubungan yang dekat terhadap Launchinpad dan Universitas Amikom Yogyakarta yang telah memberikan ruang untuk penelitian program studi Informatika
   2. Launchinpad mendapatkan hasil penelitian yang akan diberikan kepada narasumber sebagai bahan pertimbangan dalam memperbaiki sistem keamanan
   3. Meningkatkan keamanan website Launchinpad
c. Oleh Pembaca :
   1. Pembaca dapat mengetahui serta mendapatkan wawasan secara teknis mengenai penetration testing untuk ilmu pengetahuan bidang Informatika.
   2. Menjadikan bahan referensi untuk melakukan pengujian penelitian di masa yang akan datang.

1.6 Sistematika Penulisan

Sistematika penulisan penelitian skripsi ini terdiri dari 5 (lima) bab yang disusun sebagai berikut:

BAB I Pendahuluan

Bab ini menjelaskan masalah yang menjadi landasan pelakasanaan penelitian ini yang diambil dari latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Bab ini menguraikan dasar teori yang terkait untuk digunakan selama melakukan penelitian yang membantu proses penyusunan penulisan dari informasi kerentanan, *Penetration Testing*, *Kali Linux*, *Tools*, *Burp Suite*, *dan Literatur*.

BAB III Metode Penelitian

Bab ini membahas dalam point terpenting dan menjelaskan tahapan metode pengumpulan data, pengujian, dan data penelitian yang dilakukan untuk analisis kerentanan website.

BAB IV Hasil Dan Pembahasan

Bab ini memberikan hasil implementasi tentang analisis dan pembahasan dari penelitian dengan menggunakan beberapa alat scaning dan *Burp Suite* untuk melakukan analisis kerentanan website.

BAB V Penutup

Bab ini mengenai kesimpulan hasil penelitian yang didapat dan saran yang diberikan untuk melakukan tahapan metode pengujian penetration testing yang lebih baik.