BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia modern, peranan informasi menjadi sangat penting dan memiliki nilai guna yang tinggi, maka dari itu diperlukan pelayanan informasi yang cepat dan akurat. Manusia telah banyak memanfaatkan *website* sebagai sumber pencarian informasi. Pada perusahaan atau organisasi, informasi dan komunikasi mempunyai peranan yang sangat penting sebagai sumber informasi. *Website* merupakan komponen penting dalam berkembangnya teknologi informasi saat ini. *Website* merupakan salah satu media representasi yang diperlukan oleh suatu organisasi dalam hal ini adalah UPN "Veteran" Jawa Timur agar dapat berkembang secara luas. Dengan *website* tersebut seluruh informasi mengenai visi, misi, dan program kerja yang ingin ditampilkan akan dengan mudah sampai kepada pengguna melalui internet. Namun dengan kemajuan ini terdapat juga beberapa keresahan yang dirasakan baik dari sisi pengguna maupun pengembang suatu *website* sistem informasi.

Keresahan dalam teknologi informasi ini dapat berupa kerentanan keamanan yang dapat menimbulkan ancaman untuk mencari keuntungan finansial, merusak nama baik perusahaan/instansi tertentu dan lain sebagainya apabila ditemukan oleh para pelaku kriminal *cyber*/*cracker*. Namun pada umumnya tidak semua yang dapat menemukan celah keamanan ini adalah pelaku kriminal, adapun *ethical hacker* yang merupakan peretas yang bertujuan untuk memperkuat keamanan suatu sistem.

Penetration testing atau *pentest* adalah kegiatan di mana seseorang mencoba untuk melakukan serangan terhadap suatu jaringan organisasi/perusahaan untuk menemukan kelemahan pada sistem tersebut (Adetya Putra Dewanto, 2018). Hal ini umum dilakukan oleh seorang profesional atau *ethical hacker* untuk memperkuat keamanan suatu sistem. Dalam penelitian ini akan dilakukan sebuah *penetration testing* terhadap aplikasi berbasis *web* yang bertujuan untuk menemukan celah keamanan sebelum titik tersebut dieksploitasi oleh pihak yang tidak bertanggung jawab

serta membantu meningkatkan keamanan pada sistem. Dalam penelitian ini terdapat 5 tahap penerapan dari *ethical hacking* yaitu *reconnaisance*, *scanning* & *enumeration*, *gaining access* (exploitation), *maintaining access*, dan *covering tracks*.

Sebuah sistem pada umumnya memiliki mekanisme keamanan yang diterapkan oleh pihak pengembang. Namun pada beberapa keadaan atau situasi terdapat informasi yang dapat diakses tanpa izin akibat dari celah keamanan oleh sistem tersebut (Fauzan, 2019). Berdasarkan pendahuluan di atas, didapatkan beberapa masalah di antaranya adalah bagaimana cara menguji keamanan *domain* dan *subdomain* perusahaan/instansi pengguna sistem dan bagaimana cara melakukan pengujian terhadap sistem yang telah dikembangkan.

Adapun tujuan yang diharapkan dari penelitian pengujian celah keamanan ini adalah menguji keamanan sistem aplikasi berbasis *web* terhadap serangan eksternal oleh pelaku kriminal, melakukan pengujian terhadap sistem yang telah dikembangkan, dan membuat laporan hasil *pentest*/*pentest report*. *Pentest report* ini akan terdiri temuan yang didapat dari tahapan *reconnaisance* hingga *post exploitation*. Tujuannya laporan ini akan digunakan untuk menyajikan laporan dan hasil dari *pentest* yang telah dilakukan dengan tujuan untuk membantu perusahaan/instansi pengguna sistem. Dengan begitu saat melihat laporan *pentest*, klien dapat sepenuhnya menyadari seberapa aman produk dan area apa yang perlu ditingkatkan.

W*ebsite subdomain* upnjatim.ac.id UPN "Veteran" Jawa Timur merupakan situs yang memfasilitasi layanan dan informasi universitas seperti fakultas, UPT, dan layanan milik UPN "Veteran" Jawa Timur. Fitur yang ada dalam *website* ini antara lain adalah profil, layanan, koleksi, galeri, prosedur, unduhan, panduan, FAQ, *open access*, dan tautan sesuai dengan instansi terkait. Pada tahapan pengujian celah keamanan *website subdomain* upnjatim.ac.id dibutuhkan beberapa perangkat lunak guna membantu penelitian dan mencapai hasil yang terstruktur. Hal ini bertujuan untuk memudahkan *developer* dalam mengembangkan keamanan *website subdomain* upnjatim.ac.id UPN "Veteran" Jawa Timur.

Pada penelitian ini dilakukan pengujian celah keamanan pada *website subdomain* upnjatim.ac.id. Hal ini dilakukan karena *website subdomain* upnjatim.ac.id yang sedang digunakan memiliki kemungkinan kerentanan dalam aspek keamanan. Penelitian ini dilakukan guna membekali untuk mempersiapkan diri sebelum terjun ke dunia profesional untuk terlibat memberikan dampak sosial yang positif terhadap pendidikan di Indonesia dengan cara yang lebih kritis utamanya dalam keamanan *cyber*.

Dengan adanya kekurangan tersebut pada penelitian ini penulis melakukan pengujian celah keamanan *website subdomain* upnjatim.ac.id UPN "Veteran" Jawa Timur dengan menggunakan metode *penetration testing*. Keamanan *cyber* merupakan aspek penting dalam dalam dunia *digital*. Metode *penetration testing* dipilih karena merupakan metode untuk menguji celah keamanan yang efektif dan mengacu pada standar internasional OWASP TOP 10. Metode ini memiliki 5 tahapan yaitu *reconnaisance*, *scanning* & *enumeration*, *gaining access* (*exploitation*), *maintaining access*, dan *covering tracks*.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, berikut merupakan perumusan masalah yang akan dikaji dari pengujian celah keamanan *website subdomain* upnjatim.ac.id UPN "Veteran" Jawa Timur, yaitu :

1. Bagaimana cara menguji keamanan *subdomain* yang dapat merugikan perusahaan/instansi pengguna sistem?
2. Bagaimana solusi pencegahan preventif dalam keamanan *website subdomain* upnjatim.ac.id UPN "Veteran" Jawa Timur yang bermanfaat bagi instansi dan pengguna?

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah yang sudah dijelaskan di atas, maka terdapat batasan-batasan pada pengujian celah keamanan *website subdomain* upnjatim.ac.id, yaitu :

1. *Penetration testing* yang dilakukan mengacu pada OWASP TOP 10 2021
2. *Web* yang akan diuji adalah 10 web yang terdiri dari 6 fakultas universitas yang menggunakan domain upnjatim.ac.id.

1.4 Tujuan Penelitian

Adapun tujuan dari pelaksanaan penelitian ini sebagai berikut :

1. Melakukan pengujian celah keamanan dari *website* dengan *subdomain* upnjatim.ac.id yang ada terhadap kemungkinan serangan eksternal.
2. Mengidentifikasi hasil temuan dari pengujian *pentest* dan kemungkinan solusi preventif yang dapat digunakan.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari pelaksanaan Penelitian ini adalah sebagai berikut :

1. Masukan untuk meningkatkan kualitas keamanan *website subdomain* upnjatim.co.id dengan standar OWASP TOP 10.
2. Mampu meningkatkan kewaspadaan akan pentingnya *cyber security* dalam pengelolaan *website*.