BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era digital yang telah sangat berkembang, tidak dipungkiri lagi bahwa perkembangan digitalisasi sangat dibutuhkan dalam berbagai aspek. Contoh salah satunya yang dibutuhkan yaitu website. Website kini telah meraja lela ke berbagai bidang, baik itu perusahaan, perbelanjaan, dan tidak lupa dari lingkup pendidikan sendiri. Berbagai bentuk kreatifitas dan kemampuan dalam perancangan website telah banyak dikuasai oleh *programmer*. Namun, perlu kita sadari bahwa semakin berkembangnya era digital, juga semakin berkembangnya kejahatan *cyber* pada dunia maya, termasuk kejahatan *cyber* pada website.(Alanda et al., n.d.)

Perlu diketahui bahwa jumlah domain website yang terdapat di dunia telah mencapai ratusan juta. Menurut Verisign Domain Name Industry Brief edisi ke-4 tahun 2021, terdapat sekitar 367,3 juta nama domain terdaftar di seluruh dunia pada akhir Juni 2021. Jumlah ini meningkat 3,8 juta atau 1,1% dibandingkan dengan kuartal sebelumnya. Sedangkan, menurut data yang dikeluarkan oleh Verisign pada akhir kuartal pertama 2021, jumlah total domain TLD atas (Top-Level Domain) yang terdaftar di Indonesia adalah sekitar 775 ribu. Namun, ini hanya mencakup domain TLD atas seperti .com, .net, .org, dan lain-lain, dan tidak termasuk domain TLD atas negara Indonesia yaitu .id. Jumlah total domain .id terdaftar di Indonesia saat ini tidak saya ketahui secara pasti. Namun, data dari PANDI (Pengelola Nama Domain Internet Indonesia) pada Agustus 2021 menunjukkan bahwa terdapat lebih dari 114 ribu domain .id terdaftar di Indonesia.(fr, n.d.)

Dengan banyaknya jumlah domain website, tidak dipungkiri bahwa kejahatan *cyber* juga meningkat. Menurut Badan Siber dan Sandi Negara mencatat serangan siber di 2022 berjumlah 976.429.996 dengan anomali trafik paling banyak masih berasal dari aktivitas malware. Untuk menghindari kerugian yang disebabkan oleh serangan siber, perusahaan dan organisasi harus memiliki sistem keamanan informasi yang kuat. Penetration testing adalah salah satu metode yang

digunakan untuk menguji keamanan sistem informasi. Penetration testing atau pen testing adalah proses menguji sistem keamanan dengan mencoba menembus sistem tersebut dan mengidentifikasi kelemahan yang ada. Hal ini bertujuan untuk membantu mengidentifikasi risiko keamanan yang ada dalam sistem, sehingga dapat diambil tindakan pencegahan yang tepat.(Fachri et al., 2021)

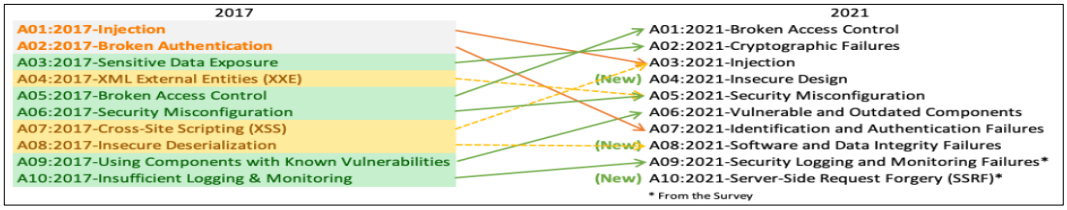
Salah satu aturan dasar dalam menentukan keamanan suatu jaringan ada tiga yang disebut CIA TRIAD.

1. Confidentiality(kerahasiaan) yaitu aspek yang berisi tentang menjamin kerahasiaan data atau informasi, dan memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
2. Integrity(integritas) yaitu aspek yang menjamin bahwa data tidak ada perubahan tanpa ijin dari pihak yang berwenang, menjaga keakuratan dan keutuhan data atau informasi.
3. Availability(ketersediaan) yakni aspek yang menjamin bahwa data tersedia Ketika dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Apabila ketiga faktor dasar keamanan jaringan tersebut tidak dapat dipenuhi maka suatu jaringan dapat dikategorikan tidak aman dan rawan akan celah, tidak menutup kemungkinan akan disusupi oleh pihak yang tidak bertanggung jawab.(Harahap et al., n.d.)

Terdapat sebuah organisasi nirlaba yang fokus pada keamanan aplikasi web yang bernama OWASP (Open Web Application Security Project). OWASP banyak menyediakan sumber daya mengenai keamanan aplikasi web, yang mana salah satunya yaitu OWASP Top 10 – 2021. OWASP Top 10 adalah sebuah panduan dan penjelasan terkait kelemahan kelemahan pada web pada tingkat 10 besar terbanyak.

Yang mana OWASP pada tahun 2017 telah mengeluarkan OWASP Top 10:2017, dan kini pada tahun 2021 OWASP mengeluarkan OWASP Top 10 terbarunya.(*Willberg_Mikael*, n.d.)



Gambar 1. 1 OWASP TOP 10 : 2021

Perlu diketahui bahwa pentingnya sadar akan pencegahan kejahatan *cyber* perlu ditingkatkan. Pada penelitian ini akan menguraikan cara untuk mengetahui kerentanan celah yang ada pada website, melakukan *penetration testing* untuk membuktikan kerentanan celah, dan membuat laporan terhadap celah tersebut, yang mana memilih studi kasus pada website Lembaga Penelitian dan Pengabdian kepada Masyarakat - UPN Veteran Jatim, Lembaga Pengembangan Pembelajaran dan Penjaminan Mutu – UPN Veteran Jatim, Pejabat Pengelola Informasi dan Dokumentasi – UPN Veteran Jattim, Kantor Urusan Internasional & Sekretariat Eksekutif – UPN Veteran Jatim, Sistem Informasi Riset Dan Pengabdian Masyarakat (SIMARIS) – UPN Veteran Jatim.

Sistem website pada lingkup pendidikan menjadi salah satu target kejahatan siber. Oleh karena itu, skripsi ini ditulis dengan latar belakang untuk mengevaluasi tingkat keamanan website menggunakan metode Black Box dengan Teknik Penetration Testing Execution Standard (PTES) pada studi kasus terkait dengan domain yang akan diuraikan pada bagian batasan masalah. Yang mana website tersbebut sangat berguna untuk mahasiswa terkait perkuliahan. Alasan penelitian ini menggunakan metode Black Box yaitu karena pada kasus ini metode yang paling cocok untuk Penetration Testing yaitu Black Box, karena di setiap prosesnya yang akan dilalui masih sebuah misteri dan tanpa memiliki akses apapun ke sistem, dan juga mendapatkan hasil yang lebih akurat daripada menggunakan metode White Box maupun Grey Box. Dapat dikatakan bahwa tingkat urgensi pada penelitian ini cukup penting.(Althunayyan et al., 2022)

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka penelitian ini memiliki beberapa rumusan masalah sebagai berikut :

1. Bagaimana mencari kelemahan keamanan pada website yang menjadi studi kasus.
2. Bagaimana website pada poin 1 (satu) memiliki celah keamanan terkait pada daftar OWASP Top 10.
3. Bagaimana cara melakukan pengujian *penetration testing* terhadap kelemahan keamanan website yang telah ditemukan berdasarkan CIA TRIAD.
4. Bagaimana cara menangani kelemahan keamanan website yang ditemukan.

1.3. Tujuan

Pada penelitian ini memiliki beberapa tujuan yang mengacu pada latar belakang dituliskan penelitian ini, yang tertera pada bawah ini.

1. Mengetahui kelemahan keamanan yang dimiliki oleh website studi kasus dengan *Vulnerability Scan Tools*.
2. Menguji keamanan website studi kasus dengan metode Web Penetration Testing.
3. Melakukan percobaan *exploitation* terhadap kelemahan website.
4. Memberikan rekomendasi kepada website studi kasus terkait hasil pengujian.

1.4. Manfaat

Penelitian yang menggunakan Teknik Penetration Testing ini diharapkan dapat mengevaluasi keamanan website yang menjadi studi kasus pada penelitian ini. Dengan rincian manfaat sebagai berikut.

1. Mengetahui kelemahan kelemahan yang dimiliki oleh website.
2. Mendapatkan hasil eksploitasi website sesuai dengan kelemahan sesuai kelemahan yang ada.
3. Mendapatkan rekomendasi yang sesuai dengan hasil eksploitasi.

1.5. Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, maka terdapat batasan masalah yang ditentukan pada :

1. Website sub-domain upnjatim.ac.id yang akan diuji adalah lppm.upnjatim.ac.id, lp3m.upnjatim.ac.id, ppid.upnjatim.ac.id, io.upnjatim.ac.id, home.upnjatim.ac.id/simaris.
2. Penelitian ini beroperasi menggunakan sistem operasi Windows 10 dan Kali Linux.
3. Penelitian ini menerapkan metodologi PTES (Penetration Testing Execution Standard).
4. Eksploitasi akan dilakukan dengan menggunakan lab website tersendiri, jika pada website studi kasus tidak dapat dieksploit, menggunakan aplikasi Burpsuite.