BAB I
PENDAHULUAN

1.1 Latar Belakang

Nikto adalah perangkat lunak open source yang digunakan untuk melakukan pengujian keamanan server web. Sullo mengembangkan perangkat ini pada tahun 2001. Nikto dirancang untuk melakukan pengujian keamanan pada server web dengan memindai semua direktori, file, dan objek di server web yang diujikan (Еременко & Кокоулин, 2016).

Universitas Esa Unggul, yang didirikan pada tahun 1993 di bawah naungan Yayasan Pendidikan Kemala Bangsa, adalah salah satu Pengguruan Tinggi Swasta terkemuka di Indonesia. E-Learning adalah salah satu fasilitas yang tersedia. E-Learning Universitas Esa Unggul menggunakan sistem informasi pendidikan dan pembelajaran digital. Pembelajaran digital berbasis web ini dapat diakses secara online, sehingga memudahkan siswa dan guru untuk belajar secara online. Ini juga mengurangi waktu yang dibutuhkan untuk belajar dan memungkinkan akses kapan saja dan di mana saja (Budiman et al., 2021). Kelas virtual yang nyata hanya dapat diakses melalui akun karena jenis informasi seperti e-learning memungkinkan metode belajar mengajar yang biasa digunakan di ruang kelas (Bhatia & Maitra, 2018). Sudah memiliki akun di Siakad dengan username dan password yang sama saat Anda membuat akun baru.

Gambar 1. Hasil Vulnerability Scanning terhadap web E-Learning Universitas Esa Unggul menggunakan Pentest-Tools

Dengan menggunakan website scanner Pentest-Tools, beberapa kerentanan pada web E-Learning Universitas Esa Unggul diidentifikasi, termasuk *fingerprinting* website, deteksi kerentanan berbasis versi, dan masalah konfigurasi umum. Kerentanan ini perlu ditinjau lagi untuk memastikan bahwa itu ada. Untuk memastikan bahwa informasi sensitif yang ada di web E-Learning Digital Universitas Esa Unggul dan keseluruhan web dilindungi sesuai dengan prinsip CIA Triad, diperlukan tindakan yang tepat.

Setiap situs web harus mempertimbangkan aspek keamanan datanya. Menurut badan pengawas lalu lintas internet, serangan pada aplikasi web yang dilakukan dengan menginjeksi basis data adalah yang paling umum pada tahun 2019, menyumbang 47,06% dari semua serangan siber. Kerentanan web seperti kasus ini dapat menyebabkan kebocoran data yang dapat merugikan banyak orang (Dias Utomo & Avorizano, 2017). Pengujian penetrasi atau kerentanan web adalah salah satu upaya pengamanan web yang dapat dilakukan. *Penetration Testing* mencari kelemahan sistem dan mengujinya untuk memperbaiki sistem untuk mencegah penyalahgunaan informasi (Shah & Mehtre, 2015). *Penetration Testing* membantu mengidentifikasi masalah keamanan internet.

Beberapa penelitian tentang Nikto yang telah dilakukan meliputi: **"Evaluation of Web Vulnerability Scanners: A Case Study on Nikto and W3AF"** oleh N. adalah salah satu dari banyak penelitian tentang Nikto yang telah dilakukan. Hasil penelitian Ahmad et al. menunjukkan bahwa Nikto dan W3AF efektif dan akurat. Hasil menunjukkan bahwa Nikto dapat menemukan kerentanan dengan baik, tetapi dia tidak dapat melakukan scanning yang menyeluruh (Ricardianto et al., 2022). **"Mengevaluasi Scanner Web Aplikasi: Hasil dan Implikasi"** oleh M. Hasil penelitian Jack et al. menunjukkan bahwa Nikto mendeteksi kerentanan dengan sangat baik, tetapi dia tidak memiliki waktu yang dibutuhkan untuk

melakukan scanning (Amankwah et al., 2020). **"Evaluation of Web Application Vulnerability Scanners: A Comparative Study"** oleh S. Hasil penelitian Soni et al. menunjukkan bahwa Nikto dapat mendeteksi kerentanan dengan baik, tetapi dia kurang mampu membedakan kerentanan yang sebenarnya dari yang palsu (Shahid et al., 2022).

Ada banyak framework yang dapat digunakan untuk menerapkan *Penetration Testing*, salah satunya adalah NIST SP 800-115. "*Technical Guide to Information Security Testing and Assesment*," yang diterbitkan oleh *National Institute of Standard and Technology*, mengandung framework ini. Satu keunggulan dari rangka kerja ini adalah dapat digunakan bersama dengan metode lain. *Planing*, *discovery*, *attack*, dan *reporting* adalah beberapa langkah yang diperlukan dalam metode ini. Parameter uji kerentanan dalam penelitian ini akan berasal dari daftar Scanner Kerentanan Nikto.

Walaupun Nikto dapat membantu handal keamanan meningkatkan keamanan aplikasi website, perlu diingat bahwa penyerang dapat menggunakannya untuk menemukan kerentanan pada aplikasi website yang belum dipatch atau dimaksimalkan. Oleh karena itu, memakai Nikto dengan hati-hati dan bertanggung jawab. Metode NIST SP 800-115 membantu Anda memahami cara terbaik untuk menerapkan keamanan web.

Penelitian ini menghasilkan daftar Scanner Vulnerability pada web E-learning digital Universitas Esa Unggul berdasarkan Nikto dan OWASP Top 10 2021. Daftar ini menawarkan rekomendasi untuk perbaikan yang dapat dilakukan untuk meningkatkan aspek keamanan web E-learning digital Universitas Esa Unggul. Dengan demikian, penelitian ini diharapkan menjadi pedoman untuk pengembangan aplikasi digital E-Learning Universitas Esa Unggul, yang akan membantu meningkatkan keamanan aplikasi dan mematuhi prinsip keamanan data CIA Triad.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana Universitas Esa Unggul dapat menggunakan metode NIST 800-115 untuk menguji kerentanan pada aplikasi E-learningnya berdasarkan penggunaan Nikto dan OWASP Top 10 2021?
2. Bagaimana cara menjaga aplikasi E-learning Universitas Esa Unggul aman?

1.3 Tujuan Tugas Akhir

Berikut ini adalah tujuan dari penelitian ini:

1. Berdasarkan penggunaan Nikto dan OWASP Top 10 2021, gunakan metode NIST 800-115 untuk mendeteksi keamanan sistem pada aplikasi E-learning Universitas Esa Unggul.
2. Rekomendasikan metode untuk meningkatkan keamanan platform E-learning Universitas Esa Unggul.

1.4 Manfaat Tugas Akhir

Manfaat penelitian ini meliputi:

1. Beri penjelasan tentang penggunaan metode NIST 800-115 untuk deteksi keamanan sistem pada aplikasi E-learning Universitas Esa Unggul berdasarkan Nikto dan OWASP Top 10 2021 pengguna tools.
2. Meningkatkan keamanan aplikasi E-learning di Universitas Esa Unggul untuk mencegah serangan siber.

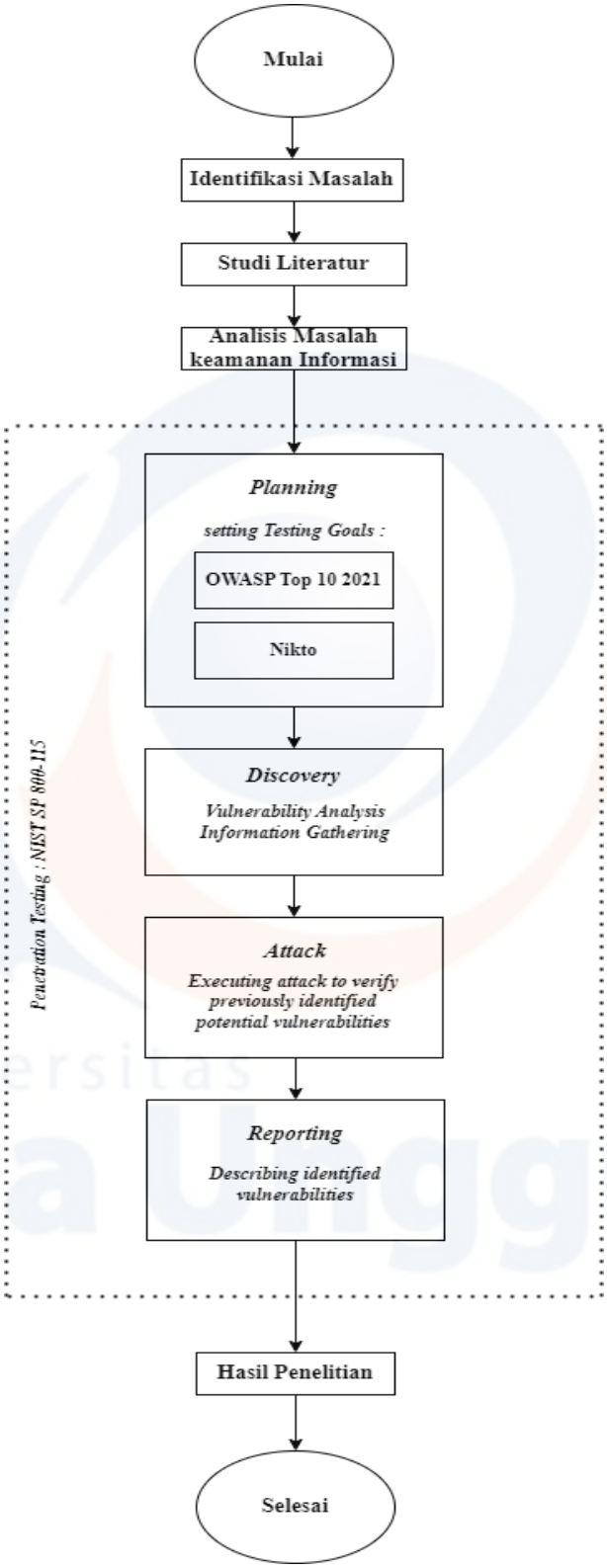
1.5 Lingkup Tugas Akhir

Dalam penelitian ini, terdapat beberapa batasan masalah dalam uji pendeteksi sistem keamanan informasi pada aplikasi E-Learning Universitas Esa Unggul, di antaranya adalah sebagai berikut:

1. Studi ini menyelidiki keamanan data di aplikasi E-Learning Universitas Esa Unggul. Metode yang disarankan oleh NIST 800-115 digunakan dalam penelitian ini.
2. Dengan menggunakan alat OWASP Top 10 2021 dan Nikto, penelitian ini menemukan domain yang akan datang.
3. Fokus penelitian adalah domain elearning.esaunggul.ac.id.

1.6 Kerangka Berpikir

Kerangka berpikir dari penelitian yang akan dilakukan adalah sebagai berikut :



Gambar 2. Kerangka Berpikir

Sebagai contoh, Gambar 2 menunjukkan struktur pemikiran :

1. Pada langkah ini, masalah untuk penelitian diidentifikasi.
2. Studi literatur: Pada tahap ini, literatur seperti jurnal dan buku dibaca untuk mencari dan membandingkan penelitian sebelumnya yang berkaitan dengan subjek penelitian ini, seperti deteksi keamanan sistem dengan menggunakan NIST 800-115, Nikto, dan OWASP Top 10 2021.
3. Analisa masalah keamanan data, pada tahap ini dilakukan analisis masalah keamanan data.
4. *Penetration Testing* : Pada tahap ini, NIST 800-115 melakukan pengujian identifikasi sistem keamanan informasi. Pengujian sistem ini mencakup sejumlah langkah, antara lain:
    a. ***Planning***, pada tahap ini, perencanaan dan persiapan dilakukan untuk melakukan uji pendeteksi sistem keamanan informasi. Parameter yang digunakan dalam penelitian ini didasarkan pada daftar panduan NIST 800-115 menggunakan alat OWASP Top 10 2021 dan Nikto.
    b. ***Discover***, pada tahap ini akan dilakukan dua hal yaitu *information gathering* dan *vulnerability analysis*. Pada *information gathering*, dilakukan dengan menggunakan berbagai alat. Setelah itu, dilakukan *vulnerability analysis* dilakukan dengan scanner untuk mengidentifikasi kerentanan sistem.
    c. ***Attack***, serangan akan dilakukan untuk memverifikasi kerentanan sistem yang ditemukan pada Kali Linux yang berjalan pada Virtual Box.
    d. ***Reporting***, hasil uji pendeteksi sistem keamanan data akan dilaporkan.
5. Pada tahap ini, hasil penelitian akan disajikan dan disarankan untuk meningkatkan aplikasi E-learning Universitas Esa Unggul.

1.7 Sistematika Penulisan Tugas Akhir

Proses penulisan penelitian ini dirancang untuk memberikan gambaran luas tentang penelitian yang sedang dilakukan. Secara keseluruhan, sistem yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN
Pada Bab I membahas latar belakang, identifikasi masalah, tujuan, keuntungan, lingkup, kerangka berpikir, dan sistem penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA
Pada Bab II memberikan penjelasan tentang teori yang digunakan untuk menyelesaikan masalah penelitian ini. Bagian ini membahas teori dasar serangan terhadap website dan Nikto serta NIST 800-115 sebagai metode.

BAB III METODOLOGI PENELITIAN
Pada Bab III memberikan penjelasan tentang metodologi penelitian, tahapan dan teknik pengumpulan data yang akan digunakan.

BAB IV HASIL DAN PEMBAHASAN
Pada Bab IV ini berisikan tentang hasil dari penelitian yang akan lakukan oleh peneliti.

BAB V KESIMPULAN DAN SARAN
Pada Bab V ini berisi kesimpulan dan saran terhadap penyusunan laporan kerja praktik.