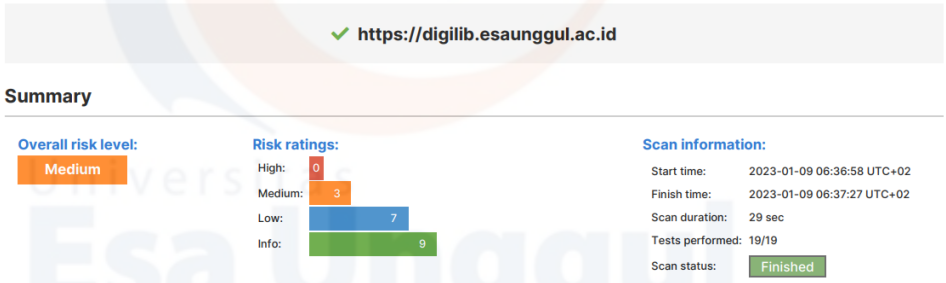
BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi internet oleh masyarakat Indonesia terus berkembang setiap tahunnya. Berdasarkan hasil laporan yang dikeluarkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyatakan bahwa tingkat penetrasi internet di Indonesia mencapai 77,02% untuk tahun 2021-2022 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2022). Perkembangan yang masif menunjukkan semakin banyaknya juga informasi yang dapat diperoleh dari internet. Hal ini menimbulkan kekhawatiran terhadap keamanan dari informasi tersebut. Keamanan informasi didefinisikan sebagai melindungi informasi dan sistem informasi dari akses, penggunaan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan (Nurul et al., 2022).

Keamanan informasi pada umumnya memiliki tiga aspek utama yang biasa disebut dengan CIA Triad. Aspek-aspek tersebut terdiri dari *confidentiality* (kerahasiaan) yang merupakan kerahasiaan informasi dari orang yang tidak berwenang, *integrity* (integritas) yang merupakan menjaga perubahan informasi dari orang-orang yang tidak berwenang, dan *availability* (ketersediaan) yaitu menjaga agar informasi agar selalu dapat diakses (Izumi & Widiasari, 2022). Jika aspek-aspek tersebut tidak terpenuhi, sistem atau aplikasi tersebut dapat tergolong tidak aman dan rawan serangan oleh pihak yang tidak bertanggung jawab.

Universitas Esa Unggul merupakan salah satu perguruan tinggi swasta terkemuka di Indonesia. Salah satu layanan yang disediakan adalah perpustakaan. Perpustakaan Universitas Esa Unggul memiliki sistem informasi perpustakaan dan repositori digital. Repositori digital ini berbasis web dan dapat diakses secara online sehingga memudahkan baik mahasiswa ataupun dosen dalam penelusuran informasi dan akses di mana pun dan kapan pun. Beberapa informasi seperti jurnal atau skripsi yang berada dalam web ini hanya dapat diakses dengan menggunakan akun. Dalam pembuatan akun, pendaftar diminta untuk mengisi beberapa data seperti alamat surel, nama lengkap, alamat tinggal, dan kata sandi, yang merupakan data sensitif.



Gambar 1. Hasil Vulnerability Scanning terhadap web Perpustakaan Digital Universitas Esa Unggul menggunakan Pentest Tools

Melalui pengamatan menggunakan *website scanner* Pentest-Tools, didapatkan beberapa kerentanan pada web Perpustakaan Universitas Esa Unggul seperti *website fingerprinting*, *version-based vulnerability*, dan *common configuration issues*. Kerentanan ini perlu ditinjau lagi lebih jauh untuk memastikan apakah kerentanan tersebut benar-benar ada. Berdasarkan wawancara yang telah dilakukan dengan pihak pengelola perpustakaan, ditemukan juga bahwa aplikasi sebelumnya pernah terkena serangan spam. Sehingga, diperlukan sebuah langkah baik untuk mengamankan informasi sensitif yang terdapat pada web Perpustakaan Digital Universitas Esa Unggul maupun mengamankan keseluruhan web secara umum untuk memastikan bahwa informasi yang berada pada web tersebut memenuhi prinsip CIA Triad.

Setiap web perlu diperhatikan aspek dari keamanan informasinya. Badan pengawas lalu lintas internet menyebutkan bahwa serangan siber yang paling populer pada tahun 2019 adalah serangan pada aplikasi web yang dilakukan dengan cara menginjeksi basis data yang mencapai 47,06% total serangan (Kusuma, 2022). Kebocoran data yang diakibatkan oleh serangan karena adanya kerentanan pada web seperti kasus tersebut dapat merugikan berbagai pihak. Salah satu dari upaya dari pengamanan web yang dapat dilakukan adalah pengujian kerentanan web atau *Penetration Testing*. *Penetration Testing* merupakan sebuah langkah yang dilakukan untuk mengidentifikasi kelemahan pada sistem dengan cara menemukan dan menguji kerentanan yang ditemukan sehingga dapat dilakukan perbaikan pada sistem untuk meminimalisir risiko terjadinya penyalahgunaan informasi (Suprianto, 2022). Dengan *Penetration Testing*, celah dari keamanan yang terdapat pada web dapat diamati dengan baik (Goutam & Tiwari, 2019). *Penetration Testing* juga dapat diartikan sebagai serangan siber secara legal dan etis bagi organisasi untuk mengidentifikasi dan menangani kerentanan dalam sebuah sistem teknologi informasi sebelum kerentanan tersebut dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dengan melakukan *Penetration Testing*, dapat dilakukan peninjauan keamanan informasi yang terdapat pada sistem. Setelah itu, hasil yang didapatkan dapat dijadikan pertimbangan untuk meningkatkan keamanan yang ada pada sistem tersebut.

Terdapat beberapa penelitian terdahulu yang serupa yang telah dilakukan. Pada penelitian dengan judul "*Vulnerability Assesment Website E-Government* dengan NIST SP 800-115 dan OWASP Menggunakan *Web Vulnerability Scanner*". Pada penelitian ini, dilakukan *Vulnerability Assesment* (VA) dengan melakukan pengujian celah keamanan untuk mengetahui seluruh potensi kelemahan kritis dari *website e-government* berdasarkan metode NIST SP 800-115 dan OWASP menggunakan dua alat *web vulnerability scanner*. Pemindaian dilakukan pada dua jenis web berbeda yaitu web *e-government* milik pemerintah daerah dan milik pemerintah desa. Hasil menunjukkan bahwa ditemukan penilaian kategori level ancaman dan jumlah *vulnerability* yang mirip antara keduanya (Darojat et al., 2022).

Penelitian terkait lainnya dengan judul "*Vulnerability Assessment of Angolan University Web Applications*". Aplikasi web universitas di Angola menyimpan informasi sensitif mahasiswa dan staf universitas, yang jika informasi tersebut bocor dapat mengancam kredibilitas universitas tersebut. Pada penelitian ini, dilakukan peninjauan keamanan terhadap aplikasi web yang dimiliki oleh beberapa universitas di Angola. Pengidentifikasian kerentanan keamanan yang dilakukan menggunakan acuan OWASP Top 10 untuk mencari serta memvalidasi penemuan dari tinjauan yang dilakukan. Hasil dari penelitian menunjukkan bahwa aplikasi web beberapa universitas di Angola tergolong tidak aman. Sekitar 70% aplikasi berkomunikasi melalui saluran yang tidak aman karena tidak adanya sertifikat keamanan (dan oleh karena itu tanpa SSL/TLS) dan menggunakan pustaka JavaScript dengan kerentanan yang diketahui, sehingga terkena serangan *cross-site scripting*. Terdapat juga kerentanan berupa *Injection, Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration,* dan *Vulnerable and Outdated Components* (Mateus & Serrão, 2021).

Penelitian terkait lainnya dengan judul "Analisis Kualitas Keamanan Sistem Informasi *E-Office* Berbasis Website Pada STMIK ROSMA Dengan Menggunakan OWASP Top 10". Pada penelitian ini, dilakukan pengujian pengamanan yang bertujuan untuk mengetahui tingkat kerentanan yang terdapat pada sistem informasi *e-office* berbasis web STMIK ROSMA Karawang menggunakan metode OWASP Top 10. Hasil pengujian menunjukkan bahwa terdapat 4 kerentanan yang terdapat sistem informasi berbasis web STMIK ROSMA Karawang yang diantaranya adalah *Sensitive Data Exposure, Security Misconfiguration, Cross-site Scripting,* dan *Insecure Deseralization* (Yudiana et al., 2021).

Dalam implementasi *Penetration Testing,* terdapat beberapa *framework* yang dapat diterapkan. Salah satunya adalah NIST SP 800-115. *Framework* ini termasuk pada dokumen yang berjudul "*Technical Guide to*

Information Security Testing and Assesment" yang dikeluarkan oleh *National Institute of Standard and Technology*. Salah satu keunggulan dari *framework* ini adalah dalam implementasinya, metode ini dapat digabungkan dengan metode lain (Hout, 2019). Dalam metode ini, terdapat beberapa tahapan yang harus, yaitu *planning*, *discovery*, *attack*, dan *reporting*. Dalam penelitian ini, daftar *Open Web Application Security Project* (OWASP) Top 10 2021 akan dijadikan parameter uji kerentanan.

Hasil dari penelitian ini adalah daftar kerentanan pada web Repositori Digital Universitas Esa Unggul berdasarkan OWASP Top 10 2021 dan rekomendasi perbaikan yang dapat dilakukan untuk meningkatkan aspek keamanan pada web Repositori Digital Universitas Esa Unggul. Dengan begitu, diharapkan hasil dari penelitian ini dapat dijadikan pedoman bagi pihak pengembang aplikasi Repositori Digital Universitas Esa Unggul dalam meningkatkan keamanan agar aplikasi dapat lebih aman serta memenuhi prinsip keamanan informasi CIA Triad.

1.2 Rumusan Masalah

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

1. Bagaimana menerapkan metode NIST 800-115 untuk mendeteksi keamanan pada aplikasi Repositori Digital Universitas Esa Unggul berdasarkan OWASP Top 10 2021?
2. Bagaimana cara meningkatkan keamanan pada aplikasi Repositori Digital Universitas Esa Unggul?

1.3 Tujuan Tugas Akhir

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan metode NIST 800-115 untuk mendeteksi keamanan pada aplikasi Repositori Digital Universitas Esa Unggul berdasarkan OWASP Top 10 2021.
2. Memberikan rekomendasi untuk meningkatkan keamanan pada aplikasi Repositori Digital Universitas Esa Unggul.

1.4 Manfaat Tugas Akhir

Manfaat dari penelitian ini adalah sebagai berikut:

1. Memberikan gambaran mengenai penerapan metode NIST 800-115 untuk mendeteksi keamanan pada aplikasi Repositori Digital Universitas Esa Unggul berdasarkan OWASP Top 10 2021.
2. Meningkatkan keamanan pada aplikasi Repositori Digital Universitas Esa Unggul sehingga dapat terhindar dari ancaman serangan siber.

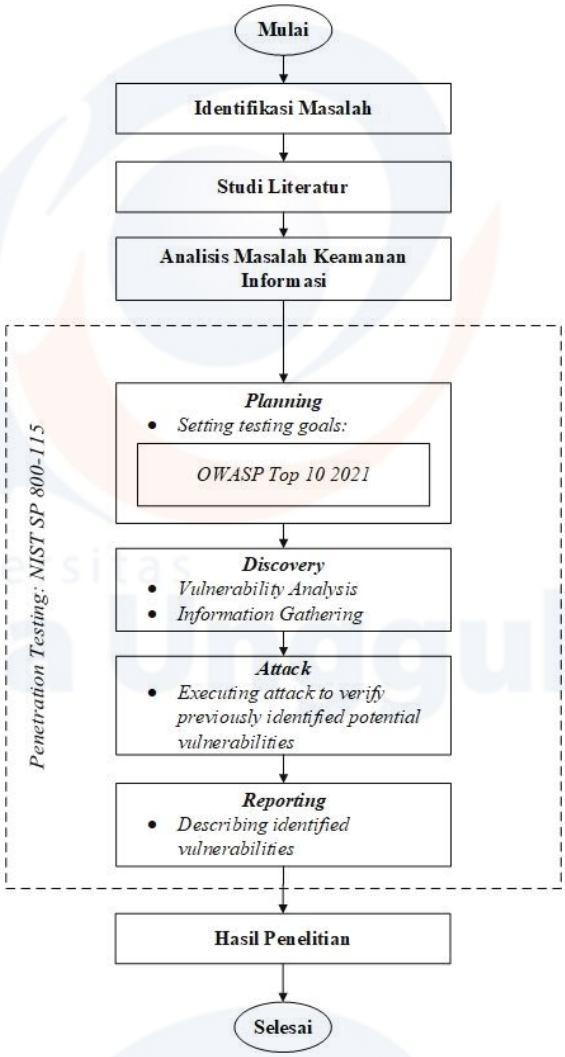
1.5 Lingkup Tugas Akhir

Dalam penelitian ini, terdapat beberapa batasan masalah dalam uji kerentanan pada aplikasi Repositori Digital Universitas Esa Unggul yang diantaranya adalah sebagai berikut:

1. Penelitian ini dalam mendeteksi keamanan informasi yang terdapat pada aplikasi Repositori Digital Universitas Esa Unggul menggunakan metode yang disarankan oleh NIST 800-115.
2. Penelitian ini menguji kerentanan menggunakan daftar kerentanan yang tercantum pada OWASP Top 10 2021 sebagai acuan parameter tes yang akan dilakukan.
3. Penelitian ini hanya berfokus pada domain digilib.esaunggul.ac.id.

1.6 Kerangka Berpikir

Kerangka berpikir dari penelitian yang akan dilakukan adalah sebagai berikut:



Gambar 2. Kerangka Berpikir

Kerangka berpikir berdasarkan Gambar 2 dijelaskan sebagai berikut:

1. Identifikasi masalah, pada tahap ini dilakukan identifikasi masalah untuk penelitian yang akan dilakukan.
2. Studi literatur, pada tahap ini dilakukan studi literatur dengan membaca literatur seperti jurnal dan buku untuk mencari dan membandingkan penelitian terdahulu yang berhubungan dengan tema dan topik penelitian, yaitu mendeteksi keamanan pada sistem dengan menerapkan NIST 800-115 dan OWASP Top 10.
3. Analisis masalah keamanan informasi, pada tahap ini dilakukan analisis terhadap masalah keamanan informasi.
4. *Penetration Testing:* NIST 800-115, pada tahap ini dilakukan pengujian kerentanan pada sistem. Terdapat beberapa langkah yang dilakukan dalam pengujian sistem ini, yaitu:
    a) *Planning,* pada tahap ini dilakukan persiapan untuk melakukan uji kerentanan pada sistem. Persiapan ini berupa menyiapkan perangkat yang dibutuhkan, serta menentukan parameter tes untuk uji kerentanan. Dalam penelitian ini, parameter yang digunakan berdasarkan pada daftar kerentanan OWASP Top 10 2021.
    b) *Discover*, pada tahap ini akan dilakukan dua hal yaitu *information gathering* dan *vulnerability analysis*. Pada *information gathering*, dilakukan pengumpulan informasi mengenai sistem menggunakan beberapa *tools*. Setelah itu, dilakukan *vulnerability analysis* menggunakan scanner untuk mengetahui apa saja kerentanan yang ada pada sistem.
    c) *Attack*, pada tahap ini akan dilakukan serangan untuk memvalidasi kerentanan yang telah ditemukan pada sistem pada tahap sebelumnya menggunakan tools *penetration testing* yang terdapat pada Kali Linux yang berjalan pada Virtual Box.
    d) *Reporting,* pada tahap ini akan dilakukan pelaporan hasil uji kerentanan yang telah dilakukan.
5. Hasil penelitian, pada tahap ini akan dilakukan penyajian hasil penelitian serta rekomendasi untuk perbaikan pada aplikasi Repositori Digital Universitas Esa Unggul.

1.7 Sistematika Penulisan Tugas Akhir

Sistematika penelitian ini terdiri dari 5 (lima) bab yang diantarnya adalah sebagai berikut:

BAB I PENDAHULUAN

Pada BAB I ini meliputi Latar Belakang, Identifikasi Masalah, Tujuan Penelitian, Ruang Lingkup, Manfaat Penelitian dan Sistematika Penelitian.

BAB II TINJAUAN PUSTAKA

Pada BAB II ini menjelaskan tentang Studi Literatur Jurnal dan Teori Umum Pendukung Penelitian.

BAB III METODOLOGI PENELITIAN

Pada BAB III Ini berisikan tentang Rencana Penelitian, Kerangka Berpikir/Tahapan Penelitian dan Teknik Pengumpulan Data yang akan digunakan.

BAB IV RENCANA HASIL PENELITIAN

Pada BAB IV ini berisikan tentang rencana hasil dari penelitian yang akan lakukan oleh peneliti.

BAB I KESIMPULAN SEMENTARA

Bab ini berisi kesimpulan sementara yang diperoleh dalam penelitian ini serta saran untuk penelitian berikutnya.