BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Kemajuan *website* di Indonesia yang begitu cepat disebabkan oleh peningkatan jumlah pengguna internet yang terus bertambah seiring berjalannya waktu (Danang Prihanto, 2022). Ditambah lagi, adanya kebutuhan informasi dan layanan *online* yang cepat dan efisien turut mendorong pertumbuhan *website*. Penggunaan *website* memberikan kebebasan dalam mengakses informasi tanpa terikat oleh batas geografis atau waktu. Kemudahan ini telah mendorong hampir semua entitas, mulai dari perusahaan, industri, pemerintah, hingga lembaga pendidikan, untuk memiliki *website* guna mendukung proses bisnis dan berbagai aktivitas lainnya (Dewi et al., 2023). Penggunaan *website* di Indonesia dimanfaatkan pada berbagai bidang, contohnya adalah Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) yang memanfaatkan *website* sebagai sistem *e-learning* yang dikenal sebagai eling.fkes.unjaya.ac.id, *website e-learning* ini memberikan fleksibilitas bagi penggunanya untuk mengakses materi belajar tanpa dibatasi oleh ruang dan waktu (Budiman et al., 2021).

Namun, dengan pertumbuhan yang pesat ini, tantangan keamanan siber juga meningkat, membutuhkan upaya yang lebih besar untuk melindungi data dan privasi pengguna. Di Indonesia, selama lima tahun terakhir, mulai dari tahun 2020 hingga awal 2024, selalu terjadi serangan *web defacement*. *Web defacement* adalah jenis serangan yang merubah tampilan atau isi asli dari sebuah *website*. Orang yang melakukan serangan *web defacement* dikenal sebagai *defacer*. Serangan ini bisa terjadi dengan memanfaatkan kelemahan dalam sistem yang memungkinkan pelaku untuk mendapatkan akses ke server dan memiliki hak untuk mengubah atau menghapus isi dari *website* tersebut.

Pada tahun 2020, terdapat 9.749 kasus *web defacement* dengan serangan terbanyak pada bulan Juni sebanyak 1.967 kasus. Sektor Akademik, khususnya

perguruan tinggi, menjadi sektor dengan jumlah kasus terbanyak, yaitu 3.353 kasus (ID-SIRTII/CC, 2020). Pada tahun 2021, terdapat 5.940 kasus *web defacement*, dengan kasus terbanyak terjadi pada bulan Maret yang mencapai 727 kasus. Sektor Akademik dalam hal ini perguruan tinggi menjadi sektor dengan kasus terbanyak yaitu 2.217 serangan (ID-SIRTII/CC, 2021). Pada tahun 2022, terdapat 2.348 kasus *web defacement*, dengan kasus terbanyak terjadi pada bulan Januari dengan kasus sebanyak 416 kasus. Sepanjang tahun 2022, sektor Administrasi Pemerintahan menjadi sektor yang paling sering mengalami serangan *web defacement*, dengan total kasus mencapai 885 kasus (ID-SIRTII/CC, 2022). Pada tahun 2023, terdapat 189 kasus *web defacement*, dengan kasus terbanyak terjadi pada bulan Januari dengan jumlah kasus sebanyak 31 kasus. Sektor yang paling banyak terkena serangan *web defacement* adalah sektor Administrasi Pemerintahan dengan jumlah kasus sebanyak 167 kasus (ID-SIRTII/CC, 2023).

Pada bulan Januari 2024, terdapat laporan Notifikasi sebanyak 45 kasus, jenis insiden yang paling sering diindikasikan dalam notifikasi yang dikirim adalah *Anomali Trafik*, *Data Breach* dan diikuti oleh *Sensitive Data Exposure*, *Web Defacement*, dan *Malicious Software*. Dengan sektor penerima terbanyak adalah sektor Administrasi Pemerintah dengan jumlah laporan sebanyak 22 kasus. Sementara itu, sektor Teknologi Informasi dan Komunikasi berada pada urutan ke-dua, dengan jumlah laporan sebanyak 7 kasus, Pendidikan berada pada urutan ke-tiga, dengan jumlah laporan sebanyak 5 kasus (ID-SIRTII/CC Januari, 2024).

Pada bulan Februari 2024, terdapat laporan Notifikasi sebanyak 56 kasus, jenis insiden yang paling sering diindikasikan dalam notifikasi yang dikirim adalah *Anomali Trafik*, *Data Breach*, APT, Trojan, *Malicious Software*, Peringatan Keamanan, *Cryptoc urrency*, *Sensitive Data Exposure*, *Malicious Activity*, dan *Web Defacement.* Dengan sektor penerima terbanyak adalah sektor Administrasi Pemerintah dengan jumlah laporan sebanyak 40 kasus. Sementara itu, sektor Teknologi Informasi dan Komunikasi berada pada urutan ke-dua, dengan jumlah laporan sebanyak 7 kasus, sektor ‘Lainnya’ berada pada urutan ke-tiga, dengan jumlah laporan sebanyak 5 kasus (ID-SIRTII/CC Februari, 2024). Sementara itu,

dalam periode bulan Januari hingga Maret 2024, tercatat ada 138 insiden serangan siber yang menargetkan domain perguruan tinggi “ac.id” (zone-h.org, 2024).

Untuk memastikan keamanan *website* dalam jangka panjang dan mencegah serangan siber, sangat penting untuk melakukan evaluasi dan analisis kerentanan *website* secara rutin. Oleh karena itu, analisis terhadap celah keamanan *website* sangat penting. Dengan adanya analisis keamanan *website*, diharapkan dapat menjadi solusi untuk meningkatkan proteksi keamanan pada *website* Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA).

Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) menaungi Fakultas Ilmu Kesehatan (FKES) yang dahulu bernama Fakultas Ilmu Kesehatan (Stikes) Jenderal Achmad Yani. Lembaga ini didirikan pada tanggal 15 Juni 2006 berdasarkan Keputusan Menteri Pendidikan Nasional (No. 084/DE/0/2006). FKES Universitas Jenderal Achmad Yani Yogyakarta menawarkan beragam program studi dan program studi terbaru yang didukung oleh dosen-dosen berkualitas dan 2 terakreditasi oleh Badan Akreditasi Independen Perguruan Tinggi Indonesia (LAM PTKes) (https://fkes.unjaya.ac.id/, 2024).

Berdasarkan data-data di atas, keamanan informasi sangatlah penting dalam lingkungan *website* Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Kekurangan dalam aspek keamanan pada *website* termasuk pada *website e-learning*, dapat membuka peluang bagi risiko yang dapat merugikan elemen-elemen dalam lingkungan Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) itu sendiri. Beberapa bentuk penyalahgunaan yang bisa terjadi dalam lingkungan *website e-learning* antara lain yaitu mengakses, mengubah, atau menghapus data yang tidak berhak atau tanpa izin, mencuri pekerjaan tugas mahasiswa lain dan mengklaimnya sebagai hasil kerja sendiri, serta mendapatkan akses ilegal ke database nilai tugas dan mengubah nilai tugas sendiri atau mahasiswa lain.

Pada tahap awal telah dilakukan observasi pada bulan Maret, dan ditemukan bahwa *website e-learning* Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) belum menerapkan HTTPS (*Hypertext Transfer Protocol Secure*), kemudian observasi dilakukan kembali pada bulan April

yang pada *website e-learning* tersebut dengan hasil telah diterapkan HTTPS pada alamat domiannya. Atas observasi awal tersebut perlu dilakukan penilaian secara menyuluruh dengan menggunakan metode penilaian kerentanan (*Vulnerability Assessment*) dan pengujian pada *website e-learning* Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA), menggunakan alat seperti NsLookup, Nmap, dan Nessus. Penelitian ini untuk menghasilkan output yang dapat menunjukkan ada atau tidaknya celah keamanan pada *website* dan mencari solusi untuk *website* tersebut, serta penilaian diperlukan untuk meningkatkan keamanan sistem.

1.2 PERUMUSAN MASALAH

Penelitian ini dilakukan untuk mengevaluasi dan menganalisis *website e-learning* di Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Dari data yang ada menunjukkan bahwa sektor Akademik masih berpotensi menghadapi serangan siber. Kekurangan dalam aspek keamanan *website* dapat menciptakan peluang bagi risiko yang dapat merugikan komponen-komponen dalam lingkungan Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA).

1.3 BATASAN MASALAH

Penelitian ini berfokus pada identifikasi kerentanan tanpa melakukan eksploitasi terhadap celah keamanan pada *website* target. Proses melakukan pemindaian pada target dengan rentang waktu 10 Juni 2024 sampai dengan 27 Juni 2024.

1.4 PERTANYAAN PENELITIAN

Berikut adalah pertanyaan-pertanyaan yang muncul terkait dengan tantangan dalam penelitian ini:

1. Bagaimana langkah-langkah melakukan *vulnerability assessment* pada *website e-learning* FKES UNJAYA?
2. Apa saja celah keamanan yang ditemukan pada *website e-learning* FKES UNJAYA saat melakukan analisis?

3. Apa dampak dari celah keamanan yang ditemukan, serta solusi yang dapat diberikan terhadap *website e-learning* FKES UNJAYA?

1.5 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk dapat menemukan dan mengetahui potensi kerentanan yang ada pada *website e-learning* Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Berdasarkan hasil analisis yang telah diperoleh, nantinya perlu menyampaikan laporan kepada pengelola *website* Fakultas Kesehatan (FKES).

1.6 MANFAAT HASIL PENELITIAN

Penelitian ini diharapkan memiliki manfaat sebagai berikut:

1. Pada Peneliti:
   a. Mampu menerapkan bidang pengetahuan yang sudah dipelajari sewaktu pada saat perkuliahan.
   b. Mendapatkan pengetahuan dan pengalaman dalam mendeteksi dan menilai kerentanan suatu *website*.
2. Pada FKES Unjaya:
   a. Dapat mengetahui jenis, deskripsi, dan nilai kerentanan keamanan pada *website e-learning*.
   b. Melindungi *website e-learning* terhadap celah resiko keamanan dari hasil identifikasi informasi yang didapatkan selama penelitian.