BAB I

PENDAHULUAN

1.1 Latar belakang

Pemerintah Indonesia di bawah kepemimpinan Presiden Joko Widodo menaruh perhatian besar terhadap ekosistem keamanan siber di Indonesia. Pemerintah telah menerbitkan Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara dengan pertimbangan bahwa pembentukan dan optimalisasi organisasi Badan Siber dan Sandi Negara yang lebih efektif dan efisien dalam melaksanakan tugas dan fungsi di bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya mewujudkan keamanan, perlindungan, dan kedaulatan siber nasional serta meningkatkan pertumbuhan ekonomi nasional (BSSN, 2021).

(ID-SRTII/CC) Indonesia *Security Incident Response Team on Internet Infrastructure/Coordination Center* Bersama dengan (Badan Siber dan Sandi negara) BSSN menerbitkan hasil monitoring keamanan siber periode agustus 2022. Pada laporan tersebut ID-SRTII/CC mengatakan ada 44.776.891 anomali trafik pada bulan Agustus 2022. Jumlah anomali tertinggi terjadi pada 3 Agustus 2022 mencapai 3.103.770 anomali trafik (BSSN, 2022). Terdapat 148 kasus peretasan situs yang ada di Indonesia. Diketahui juga aktivitas peretasan tertinggi terjadi pada tanggal 5 & 9 Agustus 2022 yang mencapai 18 kasus.

Berdasarkan sebaran kasus per-sektor bahwa sektor Pemerintah Daerah menjadi sektor yang paling banyak terjadi peretasan selama bulan Agustus 2022. Namun, tidak menutup kemungkinan pada sektor lain untuk tetap perlu mendapatkan perhatian terkait keamanan situs yang dimiliki. Tak terkecuali sektor pendidikan, pada laporan bulanan publik hasil monitoring keamanan siber bulan agustus 2022 yang dilakukan oleh (Badan Siber dan Sandi negara) BSSN pada sektor pendidikan terdapat 54 kasus peretasan dan menempati posisi kedua setelah pemerintahan daerah yang terdapat 62 kasus. (BSSN, 2022)

Universitas Pendidikan Ganesha sebagai salah satu lembaga pendidikan yang ada di Indonesia tepatnya di Singaraja, Bali dalam menjalankan seluruh aktifitas kampus sudah memanfaatkan sistem informasi berbasis Teknologi Informasi dan Komunikasi (TIK). Untuk melaksanakan pengembangan, pengelolaan, dan pelayanan teknologi informasi dan komunikasi serta pengelolaan sistem informasi dan jaringan Universitas Pendidikan.

Dari hasil penelitian awal yang dilakukan, yaitu melakukan *vulnerability scanning* pada sistem ABC dan sistem XYZ dengan menggunakan *tool ZAP*. ditemukan beberapa celah kerentanan yang memiliki tingkat risiko medium-high yang paling mungkin untuk dieksploitasi oleh pihak yang tidak bertanggung jawab pada dua sistem yang akan diuji, yakni sistem ABC dan sistem XYZ. Pada sistem ABC teridentifikasi *sensitive information disclosure, cloud metadata potentially exposed, hidden file found, sql injection*, sementara pada sistem XYZ terdapat *cross site scripting reflected, cloud metadata potentially exposed, sql injection, hidden file found* dan *arbitrary file upload*. Secara umum Universitas Universita Pendidikan Ganesha memenuhi hal-hal dasar yang harus diamankan.

Keamanan situs web penting untuk melindungi informasi yang ada. Situs web dapat diakses oleh banyak orang, tetapi juga berisi informasi sensitif, seperti data pengguna dan informasi pribadi, yang harus dilindungi. Jika keamanan situs web tidak diperhatikan, kerentanan akan dimanfaatkan oleh pihak yang tidak bertanggung jawab. *Vulnerability* adalah suatu point kelemahan dimana suatu sistem rentan terhadap serangan (Kamilah & Hendri Hendrawan, 2019).Terdapat beberapa Jenis kerentanan yang dapat terjadi, untuk itu perlu dilakukan pencarian celah kerentanan dengan melakukan *vulnerability scanning* dan melakukan *Proof of Concept (PoC)* yaitu suatu cara untuk membuktikan bahwa suatu kerentanan atau celah benar-benar dapat dieksploitasi, dengan menggunakan contoh yang dapat direplikasi untuk menunjukkan dampak yang mungkin terjadi pada sistem yang rentan(Sirait, dkk., 2018).

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas maka rumusan masalah pada penelitian ini adalah sebagai berikut.

a. Bagaimana melakukan pengujian kerentanan yang ditemukan?
b. Bagaimana analisis dari hasil pengujian kerentanan tersebut?
c. Bagaimana solusi dari celah kerentanan yang ditemukan?

1.3 Tujuan

Berdasarkan uraian latar belakang diatas, adapun tujuan dari penelitian ini adalah sebagai berikut.

a. Mengidentifikasi kelemahan dalam sistem elektronik bertujuan untuk mengatasi potensi kerentanan yang dapat dieksploitasi oleh pihak

eksternal maupun internal untuk melanggar kebijakan keamanan atau merusak sistem pada sistem ABC dan sistem XYZ.

b. Melakukan uji penetrasi, eksploitasi, dan validasi atas kerentanan yang telah teridentifikasi.
c. Melakukan penilaian tingkat risiko kerentanan yang ditemukan.
d. Memastikan kerahasiaan, integritas, dan ketersediaan data dan layanan dalam sistem elektronik.

1.4 Batasan Masalah

Agar penelitian ini tetap terarah dan tidak menyimpang dari tujuan awal penelitian maka perlu adanya batasan masalah, yaitu sebagai berikut.

a. Sistem informasi yang di analisis sistem ABC dan sistem XYZ.
b. Pengujian celah dilakukan pada celah yang memiliki tingkat risiko *medium* sampai *high* dan memiliki informasi yang jelas seperti misalnya memiliki lokasi kerentan yang jelas.
c. Dalam penelitian ini, diberikan rekomendasi mengenai cara menutup celah yang telah ditemukan, namun peneliti tidak melakukan perbaikan langsung.
d. Identifikasi kerentanan dan uji Penetrasi dilakukan pada jaringan eksternal dan internal.
e. Teknik pengujian menggunakan *grey box testing.*

1.5 Manfaat

Adapun manfaat yang didapat dari hasil penelitian ini adalah sebagai berikut.

a. Manfaat Umum

Penelitian ini diharapkan dapat memberikan *benefit* dalam bentuk *profit* kepada masyarakat umum serta dapat memberikan manfaat bagi dunia pendidikan dalam mempelajari keamanan sistem informasi.

b. Manfaat Khusus

Penelitian bisa dijadikan acuan untuk bahan evaluasi keamanan sistem informasi oleh Universitas Pendidikan Ganesha. Selain itu penelitian ini dapat meningkatkan keamanan sistem informasi serta dapat mencegah serangan yang dapat merugikan.