

# **BAB 1**

## **PENDAHULUAN**

### **1.1 LATAR BELAKANG**

Perkembangan teknologi informasi di era globalisasi saat ini menjadi perhatian besar (Juardi, 2017), terutama pada sistem informasi. Sistem informasi saat ini menjadi komponen yang penting diseluruh aspek bidang (Rahardjo, 2005), (Wahyudin & Rahayu, 2020), (Mayasari et al., 2021) (Novita Sari, 2023). Disisi lain kebutuhan akan informasi memberikan peran kepada siapapun untuk mengaksesnya (Sudiarto et al., 2017). Dengan adanya hal tersebut, setiap perusahaan atau organisasi berkeinginan membuat sistem informasi dan selalu mengevaluasi supaya memberikan informasi yang kompleks, akurat dan bermanfaat untuk proses bisnis mereka (Pricher & Nirwanto, 2013), (Nurfitriana et al., 2020), (Putri Primawanti & Ali, 2022). Peran sistem informasi adalah memberikan cara terorganisir untuk mengumpulkan, mengakses, mengelola dan menyimpan informasi, sehingga perusahaan atau organisasi dapat mencapai tujuan yang ditetapkan (Fahrozi et al., 2013), (Yulia & Ratnawati, 2020), (Mohd Lokman et al., 2007), (Oktavianti, 2019), (E. Novianto, 2023), (Pardede et al., 2017), (Utami et al., 2020).

Peran lain sistem informasi saat ini memainkan peran strategis dalam menghadapi persaingan, dimana sistem informasi dan teknologi informasi digabungkan dengan komponen lain seperti prosedur proses, struktur organisasi dan komponen terkait untuk membantu membentuk sistem informasi manajemen yang baik, hal itu merupakan salah satu kunci keberhasilan sebuah perusahaan atau organisasi (Sidh, 2013), (Ikhwan & Hendri, 2020), (Suzanto & Sidharta, 2015), (Arifudin, 2021). Hal ini ada hubungannya jika dikaitkan dengan sistem informasi akademik (SIA). Sistem informasi akademik dirancang untuk memenuhi kebutuhan perusahaan atau universitas yang menginginkan layanan pendidikan atau jasa secara sistem untuk meningkatkan efisiensi, mengedepankan kualitas layanan, kualitas produksi sumber daya manusia

(Arifudin, 2021). Selain untuk penyelenggaraan suatu instansi atau universitas sistem informasi akademik juga bermanfaat untuk mendukung produktivitas dosen dan mahasiswa dalam proses pengajaran, penelitian dan pengabdian kepada masyarakat(Ikhwan & Hendri, 2020),(Panday & Purba, 2015), (Wahyu Sholeha et al., 2018).

Pada tahun 2021 Badan Siber Dan Sandi Negara melalui direktorat operasi keamanan siber melakukan evaluasi, dan pada hasil evaluasi tersebut menunjukkan bahwa keamanan suatu sistem informasi terkhusus dibidang instansi pendidikan diindonesia menjadi target terbesar dibandingkan sektor lain (Hariyadi & Nastiti, 2021), (BSSN “ *Laporan Tahunan Monitoring Keamanan Siber*” 2021, 2022) . Pada laporan tersebut menunjukkan kasus *defacement* mencapai sebanyak 5.490 kasus dan dalam satu tahun kasus terbanyak terjadi pada bulan Maret yang mencapai 727 kasus. *Defacement website* atau perusakan *website* adalah serangan pada *website* yang mengubah tampilan visual situs atau laman *web*. Saat mendapat laporan adanya kasus kasus *defacement* di indonesia, Direktorat Operasi Keamanan Siber akan melakukan analisis celah keamanan untuk mengetahui apa saja yang memungkinkan *defacer* lakukan. Kemudian pada laporan tersebut juga menunjukkan ada 10 sektor yang menjadi target serangan *web defacement*, dan sektor pendidikan atau akademik hal ini perguruan tinggi menjadi sektor dengan kasus terbanyak pada tahun 2021 yang mencapai 2.217 kasus. Maka dari itu dalam pengembangan sistem informasi pada keamanan informasi merupakan aspek penting yang harus diperhatikan dalam hal membangun sistem (Riadi et al., 2020). Universitas Jenderal Achmad Yani Yogyakarta adalah perguruan tinggi yang menggunakan *website* untuk menunjang kegiatan perkuliahan. Semua informasi yang berkaitan dengan perkuliahan dimuat dalam *website* Sistem Informasi Akademik atau Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta. Hal ini tentunya sangat efektif dalam melakukan proses kegiatan perkuliahan. Namun, jika *web server* yang digunakan oleh Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta tidak memiliki atau memenuhi keamanan yang baik maka akan beresiko. Disisi lain,

dikhawatirkan ada oknum yang tidak bertanggung jawab yang akan memanfaatkan celah keamanan untuk merugikan sivitas akademika Universitas Jenderal Achmad Yani Yogyakarta.

Menurut G.J simmons, keamanan informasi mengacu pada bagaimana upaya untuk mencegah penipuan(*cheating*). Aspek yang harus dipenuhi oleh sistem yang menyediakan keamanan informasi adalah informasi yang diberikan akurat dan lengkap(*right information*), informasi tersebut disimpan oleh orang yang berwenang (*right people*) dan memberikan informasi pada format yang tepat(*right form*) (Raharjo, 2022). Diantara berbagai aspek keamanan siber, keamanan perangkat lunak juga memiliki peran penting(Riadi et al., 2020). Untuk melindungi *web server* dari serangan pihak yang tidak bertanggung jawab, sebaiknya dilakukan pengujian *web server* dengan menguji sistem *web server* itu sendiri melalui metode *penetration testing* (Burato & Spoto, 2019).

Di sisi lain *penetration testing* memerlukan analisis menyeluruh tentang kerentanan sistem yang sedang dieksploitasi guna mencari celah keamanan dalam sistem (Pangalila et al., 2015), (Burato & Spoto, 2019). Semua analisis data yang telah dilakukan akan didokumentasikan dan diserahkan kepada *owner* atau pemilik sistem, serta memberitahukan dampak kerentanan atau celah keamanan serta solusi yang diketahui dari seorang *pentester* (Pangalila et al., 2015). *Penetration testing* atau *pentesting* melibatkan simulasi serangan nyata yang tujuan utamanya berfokus menganalisa potensi pelanggaran keamanan pada sistem, lalu pada saat melakukan *pentesting* seorang *pentester* tidak hanya menemukan kerentanan yang dapat dieksploitasi oleh seorang *pentester*, tetapi juga melakukan evaluasi dari apa yang diperoleh setelah proses eksploitasi berhasil (Azis & Fattah, 2019). Berdasarkan penelitian sebelumnya mengenai *analysis* kerentanan menggunakan *vulnerability assement* pada *website* Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta yang dimana hasilnya menampilkan teknologi atau arsitektur yang sama, pada objek penelitian ini yaitu Sistem Informasi Portal Akademik Universitas Jendral Achmad Yani Yogyakarta. Pada penelitian tersebut memberikan data bahwa pada objek penelitian tidak ditemukan *config backup*

yang artinya tidak beresiko. Namun, tetap memunculkan kerentanan pada *website*. Pada penelitian ini penulis sudah melakukan tahap *reconnaissance* menggunakan metode *PTES (Penetration Testing Execution Standard)* untuk melihat arsitektur yang ada pada Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta. Pada tahapan *reconnaissance* ditemukan Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta menggunakan WordPress dan ditemukan celah keamanan yang dapat diserang oleh *hacker*. Jadi melihat adanya fenomena antara realita dan ideal yang terjadi pada kasus tersebut, maka penulis mengambil topik mengenai Pengujian Keamanan Sistem Informasi Studi Kasus: Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta Dengan Metode *PTES (Penetration Testing Execution Standard)*.

#### **1.1.1 Perumusan Masalah**

Berdasarkan latar belakang yang telah dikemukakan, rumusan masalah dalam penelitian ini adalah kasus *defacement* tertinggi itu ada pada web dan pada instansi pendidikan pada tahun 2021. Tingginya kasus *defacement* pada instansi pendidikan akan mengancam keamanan pada *website*.

#### **1.1.2 Manfaat Hasil Penelitian**

- a. Bagi penulis:
  1. Menambah pengetahuan terhadap standarisasi keamanan suatu sistem
  2. Menjadi acuan untuk pandangan karir di dunia *cyber security*
- b. Bagi Developer :
  1. Menjadi perhatian khusus dalam penanggulangan yang dapat mengurangi ancaman terhadap sistem jika terjadi kerentanan, tujuannya untuk meningkatkan keamanan pada sistem web Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta
  2. Mempermudah perbaikan jika ditemukan *bug* pada Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta.

c. Bagi pembaca:

Menambah literasi mengenai kerentanan suatu sistem informasi yang ada di sektor pendidikan.

d. Bagi pengguna sistem:

Meningkatkan kewaspadaan dan keamanan terhadap data yang ada di Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta.

## **1.2 TUJUAN PENELITIAN**

Penelitian ini bertujuan untuk mengukur keamanan Sistem Informasi pada Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta yang berguna menjadi bahan evaluasi terkait keamanan Sistem Informasi pada Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta.

PEPUSTAKAAN  
UNIVERSITAS JENDERAL ACHMAD YANI  
YOGYAKARTA