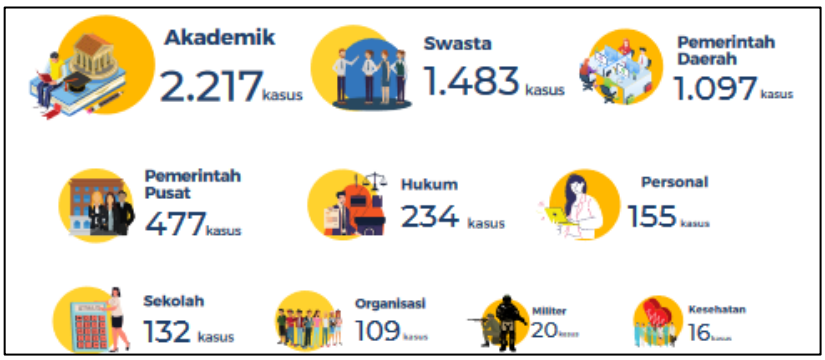
BAB 1 PENDAHULUAN

1.1 Latar Belakang

Politeknik Negeri Bengkalis merupakan salah satu perguruan tinggi di Indonesia yang menyelenggarakan pendidikan vokasi dan teknologi. Sebagai institusi pendidikan, Politeknik Negeri Bengkalis memiliki *website* yang digunakan untuk memfasilitasi kegiatan akademik dan non-akademik seperti pendaftaran, pengumuman, dan informasi mengenai kegiatan kampus. Dalam era *digital* yang semakin berkembang saat ini, keamanan *website* sangat penting untuk menjaga kerahasiaan data, mencegah penyalahgunaan *data*, dan melindungi website dari serangan *hacker*. Oleh karena itu, diperlukan analisis keamanan *website* Politeknik Negeri Bengkalis untuk mengetahui apakah *website* tersebut rentan terhadap serangan atau tidak.

Evaluasi keamanan sistem informasi pada instansi pendidikan menjadi sangat penting karena adanya ancaman serangan siber yang semakin meningkat. Menurut Badan Siber dan Sandi Negara, Selama tahun 2021, sektor yang paling banyak terkena serangan *web defacement* adalah sektor Akadmin dengan jumlah kasus sebanyak 2.217 kasus[1].

Berikut merupakan Sektor Terdampak *Web Defacement*, dan sektor Akademik dalam hal ini perguruan tinggi menjadi sektor dengan kasus terbanyak pada Tahun 2021.



Gambar 1. 1 Sektor Terdampak *Web Defacement*
(Sumber:[1])

Oleh karena itu, perlu dilakukan evaluasi keamanan sistem informasi pada instansi pendidikan untuk mencegah dan mengurangi risiko terjadinya serangan *web defacement*. Evaluasi keamanan sistem informasi pada instansi pendidikan meliputi identifikasi kelemahan atau kerentanan pada sistem informasi, dan memberikan rekomendasi untuk meningkatkan keamanan sistem informasi pada instansi pendidikan. Evaluasi keamanan sistem informasi menjadi sangat penting untuk melindungi data dan informasi penting pada instansi pendidikan serta menjaga reputasi dan kepercayaan masyarakat terhadap instansi tersebut.

Politeknik Negeri Bengkalis memiliki *website* dengan nama *domain* http://polbeng.ac.id/ yang di mana didalamnya memeiliki fitur yaitu, *Website* polbeng, Siakad, Mahasiswa baru, Jurusan, Layanan, Informasi Public, Literasi, Karir, Hubungi Kami, Kantor Urusan Internasional, semakin banyaknya layanan yang diberikan atau peluang resiko terhadap kerentanan terhadapa ancaman keamaannn juga semakin terbuka ditambah lagi dengan tidak adanya laporan kerentanan secara berkala pada *website* yang dikelola oleh Politeknik Negeri Bengkalis.

Vulnerability Assessment (Penilaian Kerentanan) dan *Penetration Testing* (Pengujuan Penetrasi) adalah dua metode penting yang digunakan dalam pengujian keamanan *website*. *Vulnerability Assessment* digunakan untuk mengidentifikasi kerentanan potensial dalam sistem, aplikasi, atau infrastruktur *website*. Hal ini dilakukan dengan menganalisis kode sumber, *konfigurasi server*, serta teknologi yang digunakan dalam pengembangan *website*. Hasil dari *Vulnerability Assessment* membantu para pengembang dan administrator untuk mengenali titik lemah dalam sistem dan mengambil langkah-langkah untuk memperbaikinya.

Disisi lain, *Penetration Testing* merupakan proses yang aktif untuk mengevaluasi kekuatan dan kelemahan *website* melalui serangkaian tes yang mencoba menembus lapisan keamanan yang ada. *Penetration Tester* (Penguji Penetrasi) akan mencoba memanfaatkan kerentanan yang ditemukan untuk mendapatkan akses tidak sah ke dalam sistem. Dengan melakukan Penetration Testing, pemilik *website* dapat menilai keefektifan mekanisme keamanan yang

telah diimplementasikan dan mengidentifikasi langkah-langkah perbaikan yang diperlukan.

Mengkombinasikan *Vulnerability Assessment* dan *Penetration Testing* dalam analisis keamanan website memberikan manfaat yang signifikan.*Vulnerability Assessment* adalah metode yang kuat untuk mengidentifikasi kerentanan umum pada *website*, sementara *Penetration Testing* membantu mencoba memanfaatkan kerentanan yang ditemukan untuk mendapatkan akses tidak sah ke dalam website.

Dengan menggabungkan kedua metode ini, kita dapat memperoleh pemahaman yang lebih mendalam tentang *website*, menerapkan pendekatan serangan yang lebih realistis, dan melakukan analisis keamanan yang lebih komprehensif. Kombinasi ini memungkinkan untuk mengidentifikasi kerentanan yang mungkin terlewatkan dan menyusun rekomendasi perbaikan yang tepat.

Dari permasalah di atas maka perlu dilakukan penelitian untuk menguji keamanan pada *website* polbeng dengan alamat domain http://polbeng.ac.id/official menggunakan *Vulnerability Assessment* dan *Peneration Testing* untuk menguji tingkat keamanan dan memberikan rekomendasi perbaikkan agar celah keamanan dapat ditutup.

1.2 Permasalahan

Berdasarkan latar belakang yang telah dijelaskan, perumusan masalah yang dapat diajukan adalah bagaimana menganalisis keamanan *website* Politeknik Negeri Bengkalis dengan menggunakan *Vulnerability Assessment dan Peneration Testing.*

1.3 Tujuan

Berdasarkan permasalahan, tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Melakukan analisis kerentanan pada *website* Politeknik Negeri Bengkalis.
2. Melakukan pengujian dari kerentanan yang ditemukan.
3. Membuat rekomendasi perbaikkan pada *website* Politeknik Negeri Bengkalis.

Dengan mencapai tujuan-tujuan ini, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan *website* instansi perguruan tinggi dari ancaman keamanan yang semakin kompleks dan canggih.

1.4 Manfaat

Penelitian analisis keamanan *website* Politeknik Negeri Bengkalis menggunakan *Vulnerability Assessment* dan *Peneration Testing* diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan informasi mengenai tingkat keamanan *website* Politeknik Negeri Bengkalis sehingga dapat meningkatkan kesadaran akan pentingnya menjaga keamanan *website*.
2. Memberikan kontribusi dalam bidang keamanan informasi terutama pada pengembangan teknologi keamanan *website*.