BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi saat ini, teknologi berkembangan pesat karena adanya kebutuhan akan sarana informasi[1]. Percepatan perkembangan teknologi informasi di berbagai bidang memerlukan kepekaan teknologi informasi terhadap situasi kehidupan masyarakat. Dari harapan tersebut, teknologi informasi menghadirkan kecepatan dan efisiensi dalam kehidupan masyarakat[2]. Tidak boleh dilupakan bahwa lembaga pendidikan memanfaatkan teknologi web sebagai sarana untuk mengkomunikasikan informasi terkini dan menginformasikan kepada masyarakat umum tentang penerimaan peserta didik baru atau beasiswa yang tersedia dalam bentuk saran, kritik atau pertanyaan mengenai lembaga pendidikan tersebut[3]. Namun, ancaman digital adalah masalah tersendiri yang mempengaruhi sistem seperti situs web. Halaman web adalah halaman informasi online yang menyediakan berbagai informasi, dokumen atau link yang menghubungkan satu halaman informasi dengan halaman informasi lainnya dan dapat kita gunakan ketika kita terhubung ke Internet kapan saja dan dimana saja melalui browser.[1] Namun seiring berkembangnya teknologi, seringkali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab sehingga dapat menimbulkan ancaman terhadap penggunaan teknologi. *Webiste* harus menjamin keamanan, privasi, dan integritas data yang diproses. Kinerja Website juga menjadi bagian penting yang harus diperhatikan agar Website dapat digunakan secara optimal dan aman[2].

Pada penelitian ini mengkaji sebuah website polbeng.ac.id yang merupakan Website Profile Institusi dan Portal Berita Kampus Politeknik Negeri Bengkalis, Yang mana Dari hasil analisis belakangan ini website Polbeng.ac.id memiliki kerentanan Missing Headers dan Clickjacking tentunya ini akan berdampak terbukanya celah bagi seorang *hacker* atau oknum yang tidak bertanggung jawab untuk melakukan peretasan website demi kepentinggan pribadinya. Berdasarkan

permasalahan tersebut maka keamanan *Website* harus lebih ditingkatkan lagi, dan untuk memperbaikinya maka peneliti berencana melakukan Evaluasi dan Mitigasi Kerentanan website Politeknik Negeri Bengalis pada Domian Polbeng.ac.id dan tidak terhituung subdomainnya. Tujuannya untuk mengetahui celah mana yang terbuka dan memberikan solusi juga melakukan pencegahan untuk mencegah serangan *hacker*.

Sebelum peneliti melaksanakan pengujian keamanan aplikasi berbasis website ini, peneliti melakukan tinjauan literatur dan menemukan beberapa penelitian terkait. Utoro dkk. dalam penelitiannya menganalisis keamanan website *e-learning* SMKN 1 Cibatu menggunakan metode Penetration Testing Execution Standard (PTES). Hasil penelitian menunjukkan temuan kerentanan kritis seperti *Web Server Transmits Cleartext Credentials*, *Cross-Site Scripting (XSS)*, dan *Cross-Site Request Forgery (CSRF).* Penelitian ini merekomendasikan implementasi protokol *HTTPS*, mekanisme validasi input, dan penggunaan token anti-*CSRF* untuk meningkatkan tingkat keamanan sistem informasi sekolah[4]. Burhani dan Priyawati mengevaluasi keamanan website pengelolaan internet Desa Kragan dengan metode yang sama, yaitu PTES. Mereka berhasil mengidentifikasi 14 celah keamanan, di antaranya *Absence of* Anti-*CSRF Tokens, SQL Injection*, dan Missing Anti-clickjacking Header. Eksploitasi terhadap beberapa celah berhasil dilakukan, sementara *SQL Injection* gagal dieksploitasi karena adanya proteksi *Web Application Firewall (WAF)* dan SSL. Sebagai rekomendasi, penelitian ini mengusulkan penambahan header keamanan dan pembaruan library yang rentan [5]. Tahir dan Risky juga menerapkan metode PTES untuk mengaudit keamanan website Dinas Pemerintahan Yogyakarta. Dengan bantuan *tool Nessus*, mereka menemukan kerentanan seperti *Browsable Web* Directories dan kerentanan terhadap serangan Clickjacking yang masuk dalam kategori risiko menengah. Solusi yang ditawarkan berfokus pada perbaikan konfigurasi *server* dan implementasi header keamanan yang lebih ketat [6].

Dari penelitian di atas dapat di simpulkan analisis kerentanan dapat meminimalisir kerentanan pada website. *Evaluasi dan Mitigas kerentanan* sangat membantu mencegah kerentanan pada website. Implementasi Evaluasi dan Mitigasi

kerentanan pada website Polbeng.ac.id di harapkan dapat bermanfaat seperti meminimalisir kerentanan yang ada pada *website* Polbeng.ac.id. Sehinggah Evaluasi dan Mitigasi kerentanan menggunakan *OWASP, WPSCANN*, kemudian melakkukan Mitigas dari hasil scanning kerentanan yang didapatkan. Mitigasi yang belum diterapkan pada penliti terhadulu. Menurut Depdagri (2003) mitigasi adalah segala upaya dan kegiatan yang dilakukan untuk mengurangi dan memperkecil akibat-akibat yang ditimbulkan oleh bencana, yang meliputi kesiapsiagaan serta penyiapan kesiapan fisik, kewaspadaan, dan kemampuan mobilisasi.[7] Selain itu, peneliti penelitian ini juga mengidentifikasi setiap masalah pada setiap peringatan yang ditampilkan menggunakan hasil pemindaian otomatis *OWASP ZAP* dan menjelaskannya sesuai dengan hasil rekaman. Untuk melakukan penelitian ini, peneliti menggunakan Metode *Penetration Testing Execution Standard* (PTES) adalah sebuah standar metodologi pengujian penetrasi yang dikembangkan oleh para praktisi keamanan informasi pada tahun 2010 oleh colaborasi para praktisi keamanan informasi international, Standar ini di kembangkan oleh para pakar dari organisasi seperti Lares Consulting, TrusedSec, Offensive Security dokumentasi resmi di publikasikan pada situs http;//www.pentest-standard.org/ Metode ini dirancang untuk memberikan panduan yang terstruktur dan dapat diulang dalam melakukan penilaian keamanan sistem informasi, PTES terdiri dari 7 tahapan utama yang saling terkait[4]. Salah satu referensi penting yang berkaitan dengan praktik *penetration testing* adalah buku berjudul *Metasploit*: *The Penetration Tester's Guide*, buku ini ditulis oleh David Kennedy, Jim O'Gorman, Devon Kearns, dan Mati Aharoni, serta diterbitkan oleh No Starch Press pada Juli 2011, David Kennedy dikenal sebagai pendiri dan CEO *TrustedSec*, sebuah perusahaan keamanan siber *internasional*, Mati Aharoni merupakan pendiri *Offensive Security*, organisasi yang mengembangkan berbagai pelatihan dan sertifikasi di bidang keamanan siber, Sementara itu, Jim O'Gorman dan Devon Kearns merupakan praktisi dan peneliti keamanan informasi yang memiliki pengalaman profesional dalam bidang *penetration testing* dan pengembangan keamanan sistem, Buku tersebut membahas implementasi teknis pengujian penetrasi menggunakan framework *Metasploit* yang relevan dengan tahapan metodologi seperti PTES[8].

Standar pelaksanaan uji penetrasi terdiri dari tujuh bagian utama, Bagian-bagian ini mencakup segala hal yang berkaitan dengan uji penetrasi mulai dari komunikasi dan penalaran awal di balik uji penetrasi, melalui fase pengumpulan intelijen dan pemodelan ancaman di mana penguji bekerja di balik layar untuk mendapatkan pemahaman yang lebih baik tentang organisasi yang diuji, melalui riset kerentanan, eksploitasi, dan pascaneksploitasi, di mana keahlian keamanan teknis para penguji berperan dan berpadu dengan pemahaman tentang keterlibatan, dan akhirnya hingga pelaporan, Standar pelaksanaan uji penetrasi terdiri dari tujuh bagian utama. Bagian-bagian ini mencakup segala hal yang berkaitan dengan uji penetrasi mulai dari komunikasi dan penalaran awal di balik uji penetrasi, melalui fase pengumpulan intelijen dan pemodelan ancaman di mana para penguji bekerja di balik layar untuk mendapatkan pemahaman yang lebih baik tentang organisasi yang diuji, melalui riset kerentanan, eksploitasi, dan pascaneksploitasi, di mana keahlian keamanan teknis para penguji berperan dan berpadu dengan pemahaman bisnis tentang keterlibatan, dan akhirnya hingga pelaporan(, metode Action Research yang berfokus pada hasil pemindaian terkait celah keamanan website. Pengujian dilakukan dengan menggunakan kerangka OWASP yang berfokus pada pengujian otentikasi, pengujian otorisasi, dan manajemen sesi. OWASP *(Open WebApplication Security Project)* adalah organisasi amal nirlaba yang didirikan pada tahun 2001 oleh OWASP Foundation[1]. Hasil dari penelitian ini sendiri yakni meng Evaluasi dan Mitigasi berupa solusi untuk meminimalisir terjadinya Attack yang dilakukan oleh Hacker.

1.2 Permasalahan

Dalam era digital yang semakin pesat, website institusi pendidikan seperti Politeknik Negeri Bengkalis (Polbeng) menjadi media utama dalam menyampaikan informasi akademik, layanan mahasiswa, dan interaksi dengan publik. Namun, semakin banyaknya informasi sensitif yang disimpan di dalam website—seperti data pribadi mahasiswa, dosen, serta sistem administrasi akademik—meningkatkan risiko terjadinya ancaman keamanan siber. Salah satu tantangan utama yang dihadapi adalah kurangnya penerapan standar keamanan yang memadai dalam

pengelolaan website institusi. Hal ini membuat website rentan terhadap berbagai jenis serangan web, termasuk *SQL Injection, Cross-Site Scripting (XSS),* dan *brute-force authentication attacks*. Melihat hal tersebut, evaluasi dan mitigasi kerentanan keamanan terhadap website Polbeng menjadi sangat penting untuk dilakukan, guna menjaga integritas, kerahasiaan, dan ketersediaan data yang ada. Penelitian ini menggunakan metodologi *Penetration Testing Execution Standard* (PTES) untuk memberikan pendekatan sistematis dalam mengevaluasi celah keamanan dan memberikan rekomendasi mitigasi berdasarkan temuan aktual yang diperoleh dari pengujian terhadap website https://www.polbeng.ac.id.

1.3 Batasan Masalah

Penelitian ini dibatasi pada evaluasi dan mitigasi kerentanan keamanan pada website resmi Politeknik Negeri Bengkalis yang dapat diakses melalui https://www.polbeng.ac.id, Pengujian keamanan dilakukan menggunakan metodologi Penetration Testing Execution Standard (PTES) dengan fokus pada identifikasi kerentanan pada aplikasi web, Penelitian ini hanya mencakup tahap pengujian kerentanan dan pemberian rekomendasi mitigasi tanpa melakukan eksploitasi yang dapat merusak sistem.

1.4 Tujuan

Melakukan evaluasi kerentanan yang ada pada website polbeng.ac.id dengan menggunakan metode PTES untuk mebncari kerentanan pada website tersebut.

1.5 Manfaat

Manfaat penelitian dari judul "Evaluasi Kerentanan Website Polbeng Menggunakan Metode Penetration Testing Execution Standard (PTES)" adalah

a. Menemukan kerentanan website Polbeng.
b. Mengetahui dampak resiko yang terjadi seperti *brute force* login yang dapat menyeababkan user bukan admin login dan mengakses halaman admin.
c. Menjadi referensi bagi peneliti di masa depan.