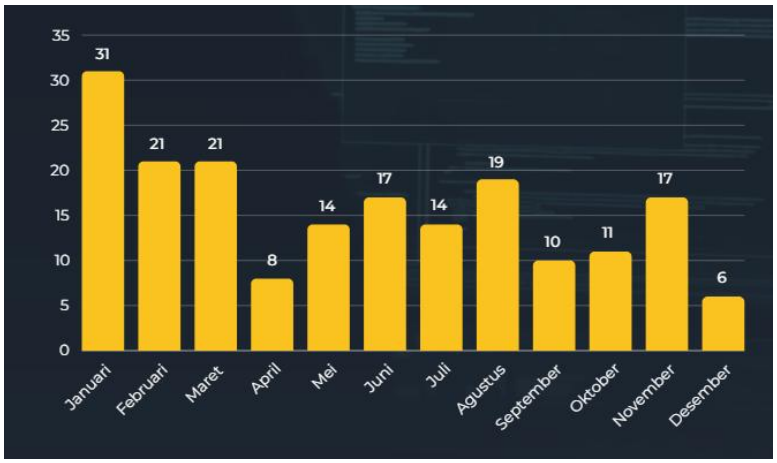
BAB I

PENDAHULUAN

1.1 Latar Belakang

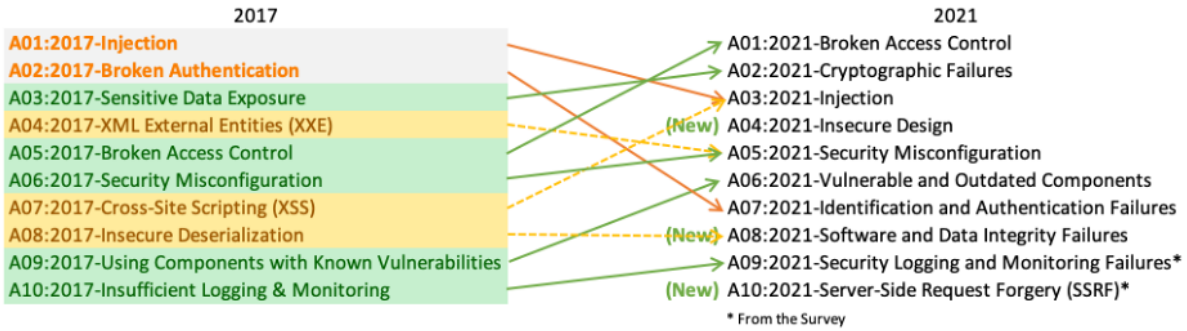
Era modern ini teknologi diciptakan untuk memudahkan kehidupan manusia. Seiring dengan berkembangnya teknologi tuntutan akan kehidupan yang efesien, praktis dan aman semakin meningkat. Kemajuan teknologi diti dengan semakin berkembang pesatnya pengguna internet hal ini dapat diketahui dari pengukuran pengguna internet yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet (APJII) tahun 2024. Penelitian ini menunjukan jika pengguna internet di Indonesia telah mencapai 79,5% dengan jumlah total pengguna internet 221.563.479 jiwa dari jumlah total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023[1]. Dengan adanya kemudahan internet menjadi bagian penting dari dunia nyata sekarang, dimana menyediakan berbagai macam layanan informasi yang dapat memberikan dampak positif maupun *negative* pada kehidupan manusia, contohnya seperti website. Website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna dalam dunia teknologi informasi yang terhubung ke internet[2]. Salah satu dampak *negative* dari website yaitu serangan *web defacement*, dimana serangan ini mengeksploitasi baik situs maupun server web dengan memanfaatkan kerentanan dari website tersebut. Menurut data dari Badan Siber dan Sandi Negara Republik Indonesia pada tahun 2023 menyatakan peretasan web di Indonesia mencapai 189 Kasus *Web Defacement* [3], hal ini menunjukan bahwa keamanan siber khususnya website di Indonesia begitu lemah ,seperti pada Gambar 1.1.



Gambar 1.1 - Kasus Web Defacement menurut Data Badan Siber dan Sandi Negara Republik Indonesia

Keamanan siber menjadi isu krusial bagi berbagai instansi dan organisasi, termasuk instansi pemerintah seperti Pengadilan Negeri Purwokerto www.pn-purwokerto.go.id. Website Pengadilan Negeri Purwokerto mempunyai peran penting sebagai portal utama untuk publikasi informasi pelayanan masyarakat dan interaksi dengan publik. Perlindungan terhadap ancaman siber menjadi sangat penting. Serangan siber terhadap aplikasi web terus berkembang, baik dari sisi teknik maupun kompleksitas serangan. Beberapa serangan yang umum meliputi *SQL Injection*, *Cross-Site Scripting (XSS)*, dan serangan lainnya yang dapat mengekspos data sensitif atau mengganggu layanan. Kerentanan keamanan ini tidak hanya dapat menyebabkan kerugian materil tetapi juga dapat merusak reputasi institusi serta mengancam keamanan publik.

OWASP (*Open Web Application Security Project*) merupakan organisasi non profit yang bertujuan untuk membantu *cyber security enthuasiast* untuk belajar mengenai web security untuk terhindar dari serangan-serangan *cyber.* Salah satu inisiatif utamanya adalah OWASP Top Ten, yang merupakan daftar sepuluh ancaman keamanan web paling kritis [4], seperti yang ditunjukan pada Gambar 1.2



Gambar 1.2 - TOP 10 Risiko Keamanan Aplikasi Web Teratas
Menurut OWASP Foundation

OWASP Top Ten memberikan panduan bagi pengembang dan administrator system untuk memahami, mengidentifikasi, dan mengatasi ancaman dengan cara yang efektif. Dalam pendekatan website Pengadilan Negeri Purwokerto penerapan OWASP Top Ten sangat relevan, sebagai portal yang sering diakses oleh publik dan mengelola berbagai data sensitif dari informasi pribadi hingga data operasional Pengadilan Negeri Purwokerto, keberadaan kerentanaan keamanan dapat memberikan dampak signifikan. Oleh karena itu, analisis kerentanan berdasarkan OWASP Top Ten dan implementasi Upaya mitigasi yang tepat sangat diperlukan untuk memastikan intergritas, kerahasiaan, dan ketersediaan informasi yang dikelola oleh website Pengadilan Negeri Purwokerto.

Penelitian ini berfokus pada kerentanan dan Upaya mitigasi pada website Pengadilan Negeri Purwokerto dengan pendekatan OWASP Top Ten. Dengan melakukan analisis terhadap 10 ancaman utama yang dirangkum oleh OWASP, ini bertujuan untuk memberikan gambaran mengenai kondisi keamanan website Pengadilan Negeri Purwokerto dan menyusun rekomendasi mitigasi yang efektif. Dengan mengindentifikasi dan memahami kerentanan yang ada, pengelola website Pengadilan Negeri Purwokerto dapat mengambil langkah proaktif untuk memperbaiki dan memperkuat sistem mereka. Upaya ini dapat meningkatkan tingkat keamanan website Pengadilan Negeri Purwokerto untuk melindungi data, informasi penting dan memastikan layanan yang lebih aman bagi Masyarakat. Penelitian ini tidak hanya bermanfaat bagi Pengadilan Negeri Purwokerto, tetapi

juga dapat menjadi referensi bagi institusi pemerintah lainya untuk meningkatkan keamanan pada web mereka.

1.2 Perumusan Masalah

Dalam penelitian ini, rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Apa saja kerentanan keamanan yang terdapat pada website Pengadilan Negeri Purwokerto berdasarkan pendekatan OWASP top ten?
2. Bagaimana upaya yang dapat dilakukan untuk mengatasi kerentanan tersebut?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengidentifikasi kerentanan keamanan pada website Pengadilan Negeri Purwokerto berdasarkan pendekatan OWASP Top Ten.
2. Menganalisis kerentanan keamanan website Pengadilan Negeri Purwokerto.

1.4 Batasan Masalah

Pada penelitian ini diketahui beberapa batasan masalah yang akan diselesaikan pada penelitian ini sebagai berikut :

1. Data yang digunakan merupakan data yang dapat diakses secara publik atau melalui izin resmi dari pengelola website Pengadilan Negeri Purwokerto.
2. Penemuan kerentanan pada website Pengadilan Negeri Purwokerto
3. Penelitian ini tidak mencakup analisis terhadap serangan siber yang lebih kompleks atau jenis kerentanan yang tidak tercakup dalam panduan OWASP TOP TEN.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Manfaat Bagi Peneliti

   Studi ini memberikan kesempatan bagi peneliti untuk memperdalam pemahaman mereka tentang keamanan jaringan, khususnya daftar 10 ancaman teratas *OWASP*. Selain itu, hasil penelitian ini melengkapi literatur ilmiah, memperkaya pengetahuan di bidang keamanan siber.

2. Manfaat bagi Universitas Telkom Purwokerto

   Penelitian ini dapat meningkatkan profil Universitas Telkom Purwokerto sebagai lembaga penelitian keamanan siber yang aktif dan membangkitkan minat calon mahasiswa dan peneliti. Hasil penelitian ini juga dapat digunakan untuk memperbarui dan memperkaya bahan kajian kurikulum terkait teknologi informasi dan keamanan siber, serta membuka peluang kerjasama dengan lembaga pendidikan lain.

3. Manfaat Pengadilan Negeri Purwokerto

   Implementasi rekomendasi penelitian ini dapat membantu meningkatkan dan memperkuat sistem keamanan situs web dan melindungi informasi sensitif. Website yang lebih aman meningkatkan efisiensi operasional dan kepercayaan masyarakat terhadap layanan yang diberikan oleh Pengadilan Negeri Purwokerto. Dengan memahami dan memperbaiki kesenjangan keamanan, pengadilan dapat mengurangi risiko serangan dunia maya yang dapat mengganggu pemberian layanan dan merusak reputasi Pengadilan Negeri Purwokerto

1.6 Metode Penelitian

Metode uji penetrasi (*penetration testing*) sebagai teknik utama untuk mengidentifikasi dan mengevaluasi potensi kerentanan pada sistem target. Proses penelitian dilaksanakan melalui lima tahapan sistematis sebagai berikut:

1. *Planning*

   Tahap awal ini bertujuan untuk menentukan ruang lingkup pengujian, sistem atau aplikasi target, serta teknik pengujian yang akan digunakan. Dalam tahap ini, peneliti akan berkoordinasi dengan pemilik sistem untuk memperoleh persetujuan formal, menetapkan tujuan pengujian, dan menentukan batasan-batasan teknis maupun etis. Dokumentasi dan perencanaan strategi dilakukan untuk memastikan bahwa proses pengujian berjalan aman dan tidak mengganggu layanan operasional sistem.

2. *Information Gathering*

   Pada tahap ini dilakukan proses pengumpulan data mengenai sistem target, baik dari sisi infrastruktur, layanan yang berjalan, alamat IP, hingga kemungkinan konfigurasi sistem. Pengumpulan informasi dilakukan melalui dua metode, yaitu passive information gathering (tanpa menyentuh sistem secara langsung) dan active information gathering (melibatkan interaksi langsung dengan sistem). Tools seperti *ping, whatweb, whois* dan lainya guna digunakan untuk mendukung proses ini..

3. *Vulnerability Identification*

   Pada tahap ini dilakukan *identifikasi* terhadap potensi kerentanan yang mungkin dimiliki oleh sistem berdasarkan hasil pengumpulan informasi sebelumnya. Tools seperti *Nikto, Xray* atau *Zap* digunakan untuk menganalisis celah keamanan pada port, layanan, atau aplikasi web. Hasil identifikasi digunakan untuk menentukan potensi ancaman yang mungkin dieksploitasi oleh penyerang.

4. *Penetration Test*

   Pada tahap ini dilakukan *eksploitasi* terhadap celah keamanan yang telah ditemukan untuk mengetahui sejauh mana dampak dari kerentanan tersebut terhadap sistem. Pengujian dilakukan secara terkendali dan bertanggung jawab, dengan tetap memperhatikan batasan yang telah ditetapkan pada tahap perencanaan. Tools seperti

Metasploit Framework, SQLmap, atau Burp Suite digunakan untuk mendukung eksploitasi dan pengujian.

5. Reporting

   Pada tahap ini dilakukan penyusunan laporan hasil dari seluruh proses pengujian, mulai dari identifikasi celah hingga dampak yang ditemukan. Laporan ini juga memuat dokumentasi teknis, analisis risiko, serta rekomendasi langkah mitigasi yang dapat diambil oleh pengelola sistem. Selain itu, hasil pengujian dibahas secara mendalam untuk memberikan pemahaman teknis serta relevansi terhadap teori yang digunakan dalam penelitian.