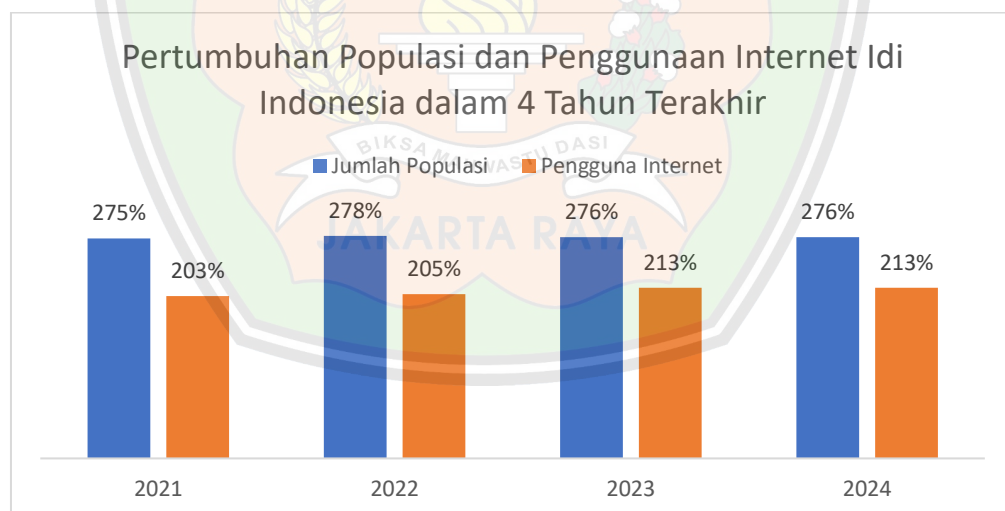


BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan informasi teknologi saat ini berlangsung sangat cepat dan dinamis. Hal ini terlihat dari meningkatnya jumlah pengguna situs web untuk berbagai keperluan, mulai dari lembaga pemerintahan, pendidikan, organisasi, hingga kebutuhan pribadi. Dalam perkembangan ini, keamanan menjadi hal yang sangat penting untuk diperhatikan. Semakin banyak pengguna yang terhubung ke internet, semakin tinggi pula risiko kejahatan siber yang bisa terjadi akibat ulah oknum yang tidak bertanggung jawab (Hidayatulloh and Saptadiaji 2021)



Gambar 1. 1 Pertumbuhan Populasi dan Penggunaan Internet di Indonesia dalam 4 Tahun Terakhir

Sumber : (Andi dwi riyanto 2024)

Menurut laporan digital yang dibuat oleh *We Are Social (Hootsuite)*, penggunaan internet di Indonesia dalam 4 tahun terakhir mengalami kenaikan 1% yang di mana pada tahun 2021 mencapai 275% , di 2022 mencapai 278%, dan di

tahun 2023 mencapai 276% akan tetapi jika dilihat dari data tersebut penggunaan internet pada bulan Januari 2024 sudah mencapai 276% juta pengguna yang dapat dipastikan pada awal Januari 2025 mendatang jumlah populasi dan penggunaan internet di Indonesia terus mengalami kenaikan angka yang signifikan. Dengan semakin bertambahnya penggunaan internet di Indonesia menandakan bahwa kini masyarakat Indonesia lebih banyak mendapatkan informasi melalui internet. *Website* merupakan salah satu tujuan utama bagi pengguna internet khususnya dalam memanfaatkannya untuk melakukan aktivitas baik untuk keperluan bisnis maupun mengakses sebuah informasi (Andi dwi riyanto 2024).

Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024, serangan siber terhadap instansi pemerintahan di Indonesia mengalami peningkatan yang signifikan. Salah satu ancaman yang paling umum adalah *web defacement*, di mana peretas mengubah tampilan halaman *website* untuk menyebarkan propaganda atau mencuri data sensitif. Selain itu, ancaman lain seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan *Broken Authentication* juga menjadi tantangan utama dalam menjaga keamanan sistem informasi berbasis web (BADAN SIBER DAN SANDI NEGARA RI 2023).

Dan dari hasil observasi yang dilakukan oleh peneliti terhadap domain *web.bnpp.go.id* melalui situs *zone-h.com* yang merupakan situs yang berisikan daftar laporan kerentanan yang pernah terjadi terhadap situs-situs alamat *website* yang terkena serangan. Dan peneliti mendapatkan hasil berupa adanya kasus yang terjadi pada domain *web.bnpp.go.id* yang telah terjadi sejak dua tahun terakhir ini seperti yang tersaji pada gambar 1.2

Total notifications: 1 of which 1 single ip and 0 mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H M R L ★ Domain	OS	View
2021/01/06	0x666cx	★ web.bnpp.go.id/hukum/artikel/d...	Linux	mirror

1

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Gambar 1. 2 Hasil observasi kerentanan domain target menggunakan Zone-H

Sumber : (Foundation 2024)

Dengan adanya data catatan kasus di atas, perlu dilakukan langkah antisipasi melalui pengujian sistem keamanan aplikasi berbasis *website*. Hal ini menjadi sangat penting untuk mencegah ancaman serangan siber yang semakin marak terjadi dalam beberapa tahun terakhir. Seiring dengan pesatnya perkembangan aplikasi berbasis web, jumlah kasus kejahatan siber juga meningkat dengan berbagai teknik serangan yang semakin canggih.

Sayangnya, keamanan sering kali ditempatkan di urutan kedua atau bahkan terakhir dalam daftar prioritas pengembangan sistem, sehingga meningkatkan risiko *eksploitasi* oleh pihak yang tidak bertanggung jawab. Selain itu, faktor kesalahan manusia (*human error*) dalam pemeliharaan maupun pengembangan aplikasi web juga menjadi penyebab utama timbulnya celah keamanan.

Oleh karena itu, diperlukan penelitian yang komprehensif untuk mengidentifikasi, menganalisis, dan memberikan solusi terhadap potensi kerentanan yang ada. Hasil penelitian ini diharapkan dapat menjadi referensi yang bermanfaat bagi para pengembang (*developer*) dalam mengimplementasikan langkah-langkah keamanan yang lebih baik guna melindungi sistem *website* dari berbagai ancaman siber. Dengan pendekatan yang tepat, keamanan aplikasi web

dapat ditingkatkan secara signifikan, sehingga memberikan perlindungan optimal bagi pengguna dan data yang dikelola oleh sistem tersebut (Foundation 2024).

Sejak diterbitkannya Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, informasi menjadi satu hal wajib yang harus disediakan oleh seluruh badan publik di Indonesia. Undang-Undang ini menjamin warga negaranya memperoleh informasi dan juga merupakan jawaban dari kebutuhan masyarakat akan informasi. Informasi bukan lagi menjadi satu hal yang rahasia atau ditutupi tetapi menjadi hal yang wajib dibuka karena menutupi suatu informasi berarti menyalahi Undang-Undang Keterbukaan Informasi Publik. Salah satu bagian penting dari domain *web.bnpb.go.id* adalah direktori/ppid atau layanan pejabat pengelola informasi dan dokumentasi yang berfungsi sebagai pintu informasi publik dan memiliki elemen autentikasi pengguna. Oleh karena itu direktori ini menjadi fokus utama dalam proses pengujian.

Untuk mengidentifikasi dan mengevaluasi tingkat kerentanan keamanan pada *website web.bnpb.go.id*, penelitian ini menggunakan standar *Open Web Application Security Project (OWASP) Top 10* sebagai referensi utama. OWASP Top 10 tahun 2024 merupakan daftar terbaru yang berisi sepuluh jenis ancaman keamanan web yang paling umum dan berbahaya. Dengan mengacu pada standar ini, penelitian akan melakukan uji penetrasi (*penetration testing*) untuk mengidentifikasi celah keamanan serta memberikan rekomendasi mitigasi guna meningkatkan ketahanan sistem terhadap serangan siber. Dikarenakan banyaknya subdomain yang ada, sehingga penulis dalam pengujian ini hanya memfokuskan pada tiga subdomain berdasarkan dari hasil pencarian informasi dan proses *vulnerability scanner* yang

telah dilakukan sebelum penyusunan laporan skripsi ini, ketiga subdomain tersebut yang dianggap bermasalah dan perlu untuk dilakukan pengujian serta memberikan rekomendasi yang dapat digunakan oleh BNPB dalam meningkatkan keamanan *website* mereka.

1.2 Identifikasi Masalah

Berdasarkan Latar belakang yang telah dijelaskan menunjukkan adanya indikasi kerentanan pada sistem, sehingga penting untuk mengidentifikasi inti permasalahan yang terjadi :

1. *Website web.bnpb.go.id* sebagai media informasi resmi yang menunjukkan adanya kerentanan pada beberapa subdomain. Hal ini menimbulkan risiko terhadap keamanan data dan layanan publik yang disediakan.
2. Berdasarkan hasil observasi melalui situs pemantau kerentanan, dilakukan serangan analisis terhadap domain *web.bnpb.go.id* yang berfokus pada direktori/ppid. Hal ini dilakukan untuk mencari celah keamanan yang perlu segera dijelaskan dan ditangani.
3. Tingginya ancaman siber terhadap situs instansi pemerintah, termasuk *web.bnpb.go.id* yang berfokus pada direktori/ppid, menunjukkan perlunya evaluasi keamanan menggunakan standar OWASP Top 10 untuk mencegah eksploitasi celah sistem.

1.3 Rumusan Masalah

Berdasarkan Identifikasi masalah yang telah diuraikan di atas maka dikembangkan suatu rumusan masalah pada penelitian ini yaitu:

1. Bagaimana cara melakukan pengujian analisis kerentanan keamanan *website* menggunakan *open web application security project (OWASP)* Top-10 studi kasus (*web.bnpb.go.id*)?
2. Bagaimana pendekatan OWASP Top-10 dapat digunakan untuk identifikasi dan mengatasi kerentanan pada *website web.bnpb.go.id* yang berfokus pada direktori/ppid ?
3. Bagaimana Jenis kerentanan yang paling kritis ditemukan pada *web.bnpb.go.id* yang berfokus pada direktori/ppid melalui pengujian menggunakan OWASP Top-10?
4. Bagaimana langkah-langkah yang diperlukan untuk mengurangi potensi risiko serangan siber pada *web.bnpb.go.id* yang berfokus pada direktori/ppid berdasarkan hasil pengujian?

1.4 Batasan Masalah

Melakukan pengujian analisis kerentanan keamanan *website* menggunakan *open web application security project (OWASP)* Top-10 studi kasus (*web.bnpb.go.id*) yang berfokus pada direktori/ppid.

1.5 Tujuan Penelitian

Adapun Tujuan Penelitian berdasarkan rumusan masalah yang diuraikan, maka tujuan penelitian ini adalah sebagai berikut:

1. Melakukan pengujian analisis kerentanan keamanan *website* menggunakan *open web application security project (OWASP)* Top-10 studi kasus (*web.bnpb.go.id*) yang berfokus pada direktori/ppid.

2. Menerapkan pendekatan OWASP Top-10 dapat digunakan untuk identifikasi dan mengatasi kerentanan pada *website web.bnpb.go.id* yang berfokus pada direktori/ppid.
3. Mengidentifikasi Jenis kerentanan yang paling kritis ditemukan pada *web.bnpb.go.id* yang berfokus pada direktori/ppid melalui pengujian menggunakan OWASP Top-10.
4. Menerapkan langkah-langkah yang diperlukan untuk mengurangi potensi risiko serangan siber pada *web.bnpb.go.id* yang berfokus pada direktori/ppid berdasarkan hasil pengujian.

1.6 Manfaat Penelitian

1.6.1 Bagi Peneliti

1. Sebagai salah satu syarat bagi peneliti untuk memenuhi syarat dalam mendapatkan gelar Sarjana Komputer (S. Kom).
2. Peneliti dapat memiliki ilmu dan pengalaman baru tentang menganalisa sebuah kerentanan sistem *Website* pada bidang Teknik Informatika.

1.6.2 Bagi Universitas

1. Sebagai tambahan referensi terhadap penelitian keamanan sistem selanjutnya.
2. Sebagai kontribusi karya ilmiah dalam disiplin ilmu di bidang Teknik Informatika.
3. Pihak Universitas dapat memanfaatkan hasil penelitian ini dalam mencegah terjadinya hal yang tidak diinginkan dan membantu mendapatkan terkait informasi kerentanan yang terdapat pada beberapa subdomain (*web.bnpb.go.id*)

1.6.3 Bagi Pembaca

1. Pembaca mendapatkan wawasan baru mengenai kerentanan terhadap sebuah sistem aplikasi *website* sebagai bagian dari ilmu pengetahuan tambahan tentunya dibidang Teknik Informatika.
2. Sebagai bahan referensi untuk penelitian selanjutnya dalam bidang Teknik Informatika pada topik yang berkaitan

1.7 Sistematika Penelitian

Sistematika penelitian skripsi ini terdiri dari 6 (enam) bab yang disusun meliputi dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang hal mendasar pada pelaksanaan penelitian ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan teori-teori dasar yang berkaitan dengan bahasan penelitian dalam membantu menyusun penulisan penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini berfokus pada penjabaran terkait metode penelitian yang digunakan meliputi metode pengumpulan data, data penelitian, dan skenario alur pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan pemaparan hasil serta analisis yang diperoleh dari pelaksanaan penelitian mengenai Analisis Kerentanan Keamanan *Website* Menggunakan *Open Web Application Security Project* (OWASP) Top-10 Studi Kasus *web.bnpb.go.id*.

BAB V PENUTUP

Bab ini memuat rangkuman kesimpulan berdasarkan hasil analisis pada bab-bab sebelumnya, serta memberikan saran yang dapat dijadikan acuan atau dikembangkan lebih lanjut untuk penerapan dalam komunitas di masa mendatang.

DAFTAR PUSTAKA

LAMPIRAN

