BAB I
PENDAHULUAN

Bab pendahuluan ini bertujuan untuk memberikan gambaran singkat tentang pentingnya pengujian celah keamanan pada website Posketanmu. Di era digital saat ini, keamanan informasi pengguna menjadi krusial dalam menjaga integritas data. Oleh karena itu, penggunaan *Google Penetration Testing* dan metode OWASP TOP 10 - 2021 menjadi relevan dalam upaya ini.

1.1. Latar Belakang

Indonesia telah mengalami peningkatan yang signifikan dalam serangan siber. Pada tahun 2022, tercatat sebanyak 370,02 juta serangan siber terjadi, yang menunjukkan peningkatan sebesar 38,72% dibandingkan tahun sebelumnya(Febriani, 2023). Hal ini menyebabkan Indonesia berada di peringkat ketiga sebagai negara yang paling sering menjadi target serangan siber(Kominfo, 2018). Maka, diperlukan langkah-langkah keamanan siber yang kuat serta kepatuhan terhadap kebijakan keamanan (KOMINFO, 2016).

Melihat meningkatnya ancaman serangan siber di Indonesia, sebuah website perlu untuk melakukan pengujian keamanan, yang dikenal sebagai web *penetration testing.* Teknik ini melibatkan serangan yang ditargetkan untuk mengidentifikasi berbagai celah keamanan dan memberikan daftar lengkap celah-celah tersebut beserta saran perbaikan yang praktis(Gary Mcgraw Brad Arkin, 2005). Web *Penetration testing* perlu dilakukan secara teratur dan terstruktur untuk memastikan validitas hasil pengukuran dan penilaian(Deng et al., 2023).

Sebagai contoh konkret dari kebutuhan akan pengujian keamanan ini, Dispendukcapil Kabupaten Mojokerto adalah lembaga pemerintah yang berperan penting dalam administrasi kependudukan dan pencatatan sipil. Pada tahun 2023, Dispendukcapil meluncurkan website pelayanan *online* yang dikenal sebagai POSKETANMU(Thaoqid, 2023). Website ini dirancang untuk mempermudah proses administrasi kependudukan, sehingga masyarakat dapat mengurus berbagai dokumen seperti KIA, kartu keluarga, KTP, akta kelahiran, akta kematian, dan surat pindah secara online. Layanan ini diharapkan dapat menghemat waktu, biaya, dan tenaga. Website ini dapat diakses melalui https://posketanmu.mojokertokab.go.id/.

Namun, dengan meningkatnya penggunaan situs web ini, keamanan website menjadi aspek yang penting untuk mencegah serangan siber yang dapat membahayakan informasi pribadi masyarakat.

Untuk memastikan keamanan website seperti website Posketanmu, OWASP Top 10 adalah daftar yang dikeluarkan oleh Open Web Application Security Project (OWASP) yang mencakup sepuluh kerentanan keamanan web yang paling umum (*OWASP Top Ten*, n.d.). Dalam konteks pengujian penetrasi, OWASP Top 10 digunakan sebagai panduan untuk mengidentifikasi dan menguji kerentanan keamanan. Uji penetrasi ini fokus pada kerentanan seperti *injection, broken authentication, dan cross-site scripting.* Dengan menggunakan metode OWASP Top 10 sebagai pedoman, pengujian ini membantu memastikan bahwa kerentanan website dapat diidentifikasi dan diperbaiki, sehingga meningkatkan keamanan aplikasi web secara keseluruhan(Priambodo et al., 2023).

Penelitian sebelumnya oleh Febriyan Priambodo, Dadan Rifansyah, dan Hasbi (2023) dalam "*Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating*" menunjukkan proses uji penetrasi pada aplikasi web "XYZ". Penelitian yang telah dilakukan menggunakan kerangka kerja OWASP Top 10 - 2021 dan metode *black box testing* dengan alat seperti Vega dan OWASP ZAP. Penelitian ini merujuk pada *Web Security Testing Guide* (WSTG) versi 4.2 dan memberikan serangkaian rekomendasi kepada pengembang aplikasi web untuk mengatasi kerentanan yang ditemukan. Selain itu, penelitian yang dilakukan hanya menggunakan satu metode seperti OWASP dalam pengujian penetrasi, tetapi jarang menggabungkan metode lain untuk mendapatkan hasil yang lebih komprehensif.

Selain metode yang telah disebutkan, ada juga teknik lain yang mendukung pengujian keamanan, yaitu *Google Hacking*, atau dikenal juga sebagai *Google Dorking.* Metode ini digunakan dalam pengujian penetrasi untuk aplikasi web. Teknik ini melibatkan penggunaan operator pencarian khusus atau kueri pencarian lanjutan untuk mencari informasi yang rentan atau sensitif di internet(EITCA, 2023). *Google Hacking* memanfaatkan kemampuan Google dalam merayapi dan mengindeks informasi di web sehingga penyerang dapat menemukan informasi yang mungkin tidak terdeteksi melalui pencarian biasa(Long, 2004). Dengan menggabungkan *Google Penetration Testing* dan OWASP top 10 2021, penulis

berusaha untuk mengatasi kesenjangan tersebut dan memberikan gambaran yang lebih lengkap mengenai kerentanan keamanan website.

Maka, dalam penelitian yang dilakukan penulis, pengujian keamanan website Posketanmu dilakukan dengan metode *Google Penetration Testing* dan OWASP Top 10 2021. Dari penggabungan kedua metode ini, membantu meningkatkan kesadaran akan pentingnya keamanan web di kalangan pengelola situs serta implementasi langkah-langkah perbaikan yang konkret untuk mengatasi kerentanan yang ditemukan. Tanpa pengujian penetrasi, website akan tetap rentan terhadap serangan siber yang dapat menyebabkan pencurian data, gangguan operasional, dan kerugian finansial. Sebaliknya, pengujian ini akan meningkatkan keamanan web, yang akan menjaga data pengguna dan memastikan kontinuitas layanan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan yang dapat dirumuskan adalah sebagai berikut :

1. Bagaimana proses pengujian keamanan pada website posketanmu.mojokertokab.go.id dilakukan ?
2. Apa saja kerentanan keamanan yang ditemukan pada website posketanmu.mojokertokab.go.id ?
3. Bagaimana langkah – langkah yang dapat diambil untuk mengatasi dan mencegah kerentanan keamanan pada website posketanmu.mojokertokab.go.id?

1.3. Tujuan Penelitian

Tujuan yang ingin dicapai oleh penulis dari penelitian ini adalah sebagai berikut

1. Melakukan berbagai proses pengujian dengan melibatkan lima tahapan pengujian kerentanan dan melakukan analisis proses pengujian keamanan pada website posketanmu.mojokertokab.go.id dengan metode *Google Penetration Testing* dan metode OWASP top 10 - 2021.
2. Mengidentifikasi kerentanan yang ditemukan dan melakukan analisis kerentanan dengan uji penetrasi pada website Posketanmu apakah kerentanan tersebut berhasil diexploitasi atau tidak.

3. Memberikan rekomendasi dari kerangka OWASP top 10 - 2021 untuk mengatasi dan mencegah kerentanan keamanan pada website Posketanmu.mojokertokab.go.id yang berhasil ditemukan.

1.4. Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat, diantaranya:

1. Memahami implementasi uji penetrasi dalam pengujian keamanan web melibatkan proses identifikasi dan eksplorasi kerentanan sebelum dilakukan oleh penyerang yang tidak bertanggung jawab.
2. Meningkatkan keamanan website pelayanan Dispendukcapil Kabupaten Mojokerto.
3. Membantu Dispendukcapil Kabupaten Mojokerto dalam memprioritaskan aspek-aspek dalam pengembangan dan pengujian website berdasarkan OWASP top 10.

1.5. Batasan Masalah

Batasan masalah yang penulis gunakan untuk melakukan penelitian ini adalah sebagai berikut:

1. Penelitian ini menghasilkan rekomendasi perbaikan untuk kerentanan yang ditemukan, namun tidak mencakup dari rekomendasi tersebut.