BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan siber merupakan aspek penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data, terutama bagi organisasi yang menggunakan sistem informasi dalam operasionalnya. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2022, Indonesia mengalami 370,02 juta serangan siber, meningkat sebesar 38,72% dibandingkan tahun sebelumnya yang mencapai 266,74 juta serangan [1]. Kondisi tersebut menempatkan Indonesia berada pada urutan ketiga dengan tingkat frekuensi serangan siber yang sangat tinggi [2].

Berdasarkan Global Cybersecurity Index (GCI) 2020 oleh International Telecommunication Union (ITU), Indonesia tercatat mengalami peningkatan peringkat keamanan siber, dengan posisi ke-24 dari 194 negara, naik dari peringkat ke-41 pada tahun 2018 [3]. Selain itu, berdasarkan lanskap keamanan siber Indonesia tahun 2023, sektor administrasi pemerintahan tercatat sebagai sektor dengan jumlah insiden siber terbanyak. Berbagai ancaman siber teridentifikasi dalam insiden tersebut, antara lain kebocoran informasi digital, serangan ransomware, gangguan pada tampilan situs web, serta indikasi serangan DDoS, yang disertai dengan upaya pemantauan proaktif terhadap potensi kejadian siber. [4].

Seiring dengan meningkatnya ancaman siber di Indonesia, pengujian keamanan pada website menjadi kebutuhan yang penting, salah satunya melalui metode web penetration testing. Metode ini dilakukan dengan mensimulasikan serangan yang terarah untuk menemukan berbagai celah keamanan pada sistem, sekaligus menghasilkan daftar kerentanan yang disertai rekomendasi perbaikan yang dapat diterapkan [5]. Penetration testing merupakan aktivitas pengujian keamanan berupa upaya penyerangan terkontrol terhadap sistem, yang bertujuan untuk mengidentifikasi kerentanan pada aplikasi maupun jaringan sebagai dasar dalam perbaikan keamanan secara berkelanjutan [6]. Oleh karena itu, web penetration testing perlu dilaksanakan secara berkala dan terstruktur agar hasil pengukuran serta penilaian tingkat keamanan yang diperoleh tetap valid [7].

Rumah Potong Hewan (RPH) Surabaya merupakan instansi yang berperan penting dalam pengelolaan dan distribusi daging serta tengah melakukan digitalisasi

untuk mendukung efektivitas operasional dan peningkatan layanan informasi kepada masyarakat. Seiring dengan penerapan sistem digital, aspek keamanan informasi menjadi semakin penting, mengingat potensi ancaman siber dapat mengganggu kelancaran layanan maupun menimbulkan kerugian bagi instansi. Berdasarkan informasi dari pihak RPH, website RPH Surabaya yang berfungsi sebagai sarana penyedia informasi publik pernah mengalami insiden peretasan, di mana halaman web menampilkan konten promosi yang tidak relevan seperti promosi obat kuat dan robot trading. Kasus tersebut mencerminkan adanya kerentanan keamanan yang berisiko disalahgunakan pihak tidak berwenang. Oleh karena itu, diperlukan langkah pengamanan dari berbagai ancaman siber untuk mendukung operasional website secara optimal.

Pada penelitian ini, pengujian kerentanan website RPH Surabaya dilakukan dengan menerapkan standar OWASP Top 10 dan NIST sebagai dasar. OWASP Top 10 adalah daftar yang mencakup sepuluh kerentanan web yang paling umum dan berbahaya yang sering dijadikan acuan dalam pengujian keamanan web [8]. Pedoman OWASP Top 10 2021 dimanfaatkan sebagai landasan pengujian untuk mengidentifikasi serta mengatasi kerentanan pada aplikasi web, sehingga website yang diuji dapat memiliki tingkat keamanan yang lebih baik secara keseluruhan [9].

Selain OWASP Top 10, penelitian ini juga mengacu pada standar lain, yaitu NIST SP 800-115. NIST SP 800-115 merupakan panduan teknis untuk pengujian dan penilaian keamanan informasi yang bertujuan untuk membantu organisasi dalam melakukan perencanaan pengujian keamanan informasi. Metodologi ini mencakup empat tahap utama, yaitu *planning* (perencanaan), *discovery* (penemuan), *attack* (serangan), dan *reporting* (pelaporan), yang digunakan untuk mengidentifikasi serta mengevaluasi kerentanan dalam sistem informasi [10].

Melalui penelitian ini, diharapkan tercapai peningkatan aspek keamanan website RPH Surabaya terhadap potensi ancaman siber, serta tersedianya dasar penguatan sistem keamanan siber yang dapat menunjang kinerja operasional secara berkelanjutan. Dengan menerapkan metode OWASP Top 10 2021 dan NIST SP 800-115, penelitian ini bertujuan untuk meningkatkan kesadaran pengelola situs mengenai pentingnya keamanan web sekaligus memberikan rekomendasi langkah-langkah perbaikan dalam mengatasi celah keamanan yang teridentifikasi. Tanpa adanya pengujian, website berisiko rentan pada serangan siber yang berujung pada kebocoran

data hingga potensi yang merugikan. Sebaliknya, *penetration testing* dapat memperkuat keamanan web serta memastikan layanan sistem berjalan secara efektif.

1.2. Rumusan Masalah

1. Apa saja kerentanan keamanan yang terdapat pada website RPH Surabaya?
2. Bagaimana tingkat risiko dari kerentanan yang ditemukan berdasarkan standar OWASP Top 10 dan NIST SP 800-115?
3. Apa rekomendasi perbaikan untuk mengatasi kerentanan tersebut?

1.3. Tujuan Penelitian

1. Mengidentifikasi dan menganalisis kerentanan keamanan pada website RPH Surabaya.
2. Menilai tingkat risiko kerentanan menggunakan OWASP Top 10 dan NIST SP 800-115.
3. Memberikan rekomendasi perbaikan untuk meningkatkan keamanan website.

1.4. Manfaat Penelitian

1. Memberikan kontribusi dalam peningkatan keamanan siber di lingkungan RPH Surabaya.
2. Memberikan pemahaman implementasi standar OWASP Top 10 dan NIST SP 800-115 dalam analisis kerentanan keamanan website.
3. Memberikan rekomendasi referensi akademik bagi penelitian serupa di masa depan.

1.5. Batasan Penelitian

Untuk memastikan penelitian ini tetap fokus dan terarah, beberapa batasan berikut diterapkan:

1. Pengujian hanya dilakukan pada website RPH Surabaya dan tidak mencakup sistem RPH Surabaya lainnya.
2. Hasil penelitian memberikan rekomendasi perbaikan berdasarkan kerentanan, tanpa mencakup perbaikan langsung pada website RPH Surabaya.

Halaman ini sengaja dikosongkan