BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan teknologi yang semakin cepat, penggunaan aplikasi web dalam mendukung kegiatan operasional perusahaan semakin meningkat. Salah satu contoh penerapan teknologi tersebut adalah sistem manajemen persediaan (*Inventory Management*) yang berfungsi untuk mencatat, mengatur, dan memantau persediaan barang dan pergerakannya secara *real-time.* Namun, terlalu mudahnya akses dan ketepatan yang ditawarkan oleh aplikasi web juga membawa risiko keamanan yang nyata dan semakin rumit, khususnya terhadap lalu lintas atau serangan siber.

PT. Sekuriti Siber Indonesia merupakan sebuah perusahaan yang bergerak dibidang konsultan keamanan siber, termasuk layanan *penetration testing, Security Operation System* (SOC), serta kepatuhan terhadap standar keamanan informasi. Dalam mendukung praktik keamanan siber, perusahaan mendorong penanganan keamanan siber yang diimplementasikan dalam sistem web *inventory management* yang digunakan untuk mencatat seluruh aktivitas logistik barang. Karena sistem ini menyimpan informasi strategis dan sensitif, maka keamanan aplikasi tersebut harus diuji secara berkala dan intensif untuk mendeteksi potensi celah keamanan sebelum dieksploitasi pihak yang tidak bertanggung jawab.

Fitur upload gambar, jika tidak diimplementasikan dengan baik, dapat menjadi celah bagi serangan seperti *upload* file berbahaya, *content spoofing*, *extension bypass*, bahkan *remote code execution* (RCE) jika server tidak dikonfigurasi dengan benar. Oleh karena itu, perlu dilakukan eksplorasi secara teknis dan praktis terhadap potensi kerentanan dalam fitur upload gambar.

Penelitian ini dilakukan untuk menguji secara langsung sistem *Inventory Management* menggunakan pendekatan *Penetration Testing.* Melalui metode ini, penulis bertujuan untuk mengidentifikasi celah keamanan, mengevaluasi potensi

dampaknya. Diharapkan penelitian ini dapat memberikan kontribusi nyata dalam memperkuat ketahanan sistem sistem informasi perusahaan, serta menjadi referensi bagi pengembang dan praktisi keamanan dalam mengelola risiko siber di aplikasi web.

1.2 Deskripsi Pekerjaan

Selama menjalani program magang, penulis berfokus pada berbagai tugas yang berkaitan dengan keamanan siber, pelaporan, serta pengujian kerentanan pada aplikasi web. Lingkup pekerjaan yang saya lakukan adalah sebagai berikut:

1. Pengenalan *OWASP ASVS* dan Cakupan Uji

ASVS adalah standar terbuka untuk verifikasi keamanan aplikasi, digunakan dalam audit, pengujian penetrasi (*pentest*), atau pembangunan sistem. *OWASP ASVS* dibagi menjadi 3 level verifikasi keamanan:

a. *ASVS* Level 1 (L1) - *Opportunistic*
    1. Uji untuk aplikasi umum.
    2. Fokus pada serangan seperti XSS, *SQL Injection*, dan CSRF.
    3. Cocok untuk mendeteksi eksploitasi dasar terhadap fitur upload gambar yang tidak aman.

b. *ASVS* Level 2 (L2) - *Standard*
    1. Diterapkan untuk aplikasi yang menangani data pengguna.
    2. Uji validasi input, kontrol akses file, dan otorisasi.
    3. Relevan dalam menguji apakah sistem *upload* gambar bisa dimanipulasi oleh pengguna yang tidak sah.

c. *ASVS* Level 3 (L3) - *Advanced/High Assurance*
    1. Uji untuk aplikasi dengan tingkat keamanan tinggi.
    2. Fokus pada eksploitasi lanjutan, misalnya *bypass filter* MIME-*type* atau penyisipan file berbahaya.

2. Pembelajaran dan Praktik *Penetration Testing*

Mendalami teori dan teknik *penetration testing* untuk mengidentifikasi kerentanan keamanan pada aplikasi web. Penulis secara langsung mempraktikkan teknik-teknik pengujian untuk mengidentifikasi kerentanan pada fitur *upload* gambar. Proses meliputi:

1. Pengujian Eksploitasi:
   a. Melakukan *upload* file berbahaya seperti shell/backdoor .php.
   b. Menggunakan *Burp Suite* untuk:
      i. Memodifikasi *request* HTTP.
      ii. *Bypass* validasi *client-side.*
      iii. Menyisipkan ekstensi ganda.
      iv. Memanipulasi MIME-*type* dan parameter file.
2. Verifikasi Eksekusi File:
   a. Mengakses file yang telah di*upload* untuk melihat apakah file dapat dijalankan di server.
   b. Jika berhasil, mengakses *command shell* yang menjadi bukti keberhasilan eksploitasi
3. Dokumentasi Hasil

   Setiap aktivitas pengujian terdokumentasi secara sistematis, termasuk:
   a. Deskripsi Celah
   b. Langkah Eksploitasi
   c. Bukti Teknis

Dalam lingkup magang ini mencerminkan keseriusan dan kompleksitas yang menuntut ketelitian, kemampuan analisis, serta pemahaman yang mendalam terkait dengan keamanan siber.

1.3 Tujuan

Tujuan dari implementasi yang dihasilkan bisa mendukung sistem manajemen persediaan yang lebih terstruktur, sinkron, serta aman bagi perusahaan. Namun, tujuan utama dari penelitian ini yaitu pada eksplorasi teknik *penetration testing* pada aplikasi yang dikembangkan oleh para *Internship* milik

PT. Sekuriti Siber Indonesia dengan mengeksplorasi fitur *upload* gambar pada aplikasi web berbasis PHP. Penelitian ini bertujuan untuk mengidentifikasi potensi yang rentan dalam aplikasi, serta menguji tingkat kerentanannya melalui simulasi serangan secara teknis hingga menganalisis dampak yang dapat ditimbulkan jika celah tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain itu, penelitian ini juga ditujukan untuk menyusun dan langkah mitigasi serta perbaikan yang dapat diterapkan guna meningkatkan keamanan aplikasi dan mencegah serangan serupa di masa mendatang.

1.4 Manfaat

Pengimplementasian dan pengujian keamanan berstandar *OWASP ASVS* pada sistem manajemen persediaan (*Inventory Management*) yang memberikan manfaat dalam rangka mendukung keberhasilan operasional web aplikasi sekaligus melindungi kepentingan pengguna dan bisnis.