BAB I
PENDAHULUAN

1.1 Latar Belakang

TriUpasedanan merupakan sebuah web aplikasi pembelajaran yang dikembangkan untuk memberikan pengalaman simulasi dalam mengelola sistem reservasi kamar, pengelolaan profil pengguna, serta interaksi melalui komentar. Aplikasi ini digunakan sebagai media edukasi dalam memahami penerapan dan tantangan keamanan aplikasi web, khususnya untuk menguji potensi serangan Cross-Site Scripting (XSS).

Seiring dengan perkembangan fitur dan kebutuhan evaluasi keamanan sistem, pihak pengembang TriUpasedanan meminta bantuan kepada PT. Sekuriti Siber Indonesia (Nemo Security) untuk melakukan pengujian keamanan terhadap aplikasinya. Permintaan ini ditindaklanjuti dengan melibatkan penulis sebagai peserta magang untuk mengidentifikasi dan menguji potensi kerentanan, khususnya serangan Cross-Site Scripting (XSS). PT. Sekuriti Siber Indonesia merupakan perusahaan IT Konsultan yang bergerak di bidang keamanan informasi. Perusahaan ini menyediakan berbagai layanan profesional seperti penetration testing, audit keamanan, serta pemantauan insiden melalui Security Operation Center (SOC). Ruang kerja yang disediakan tidak hanya berfokus pada pemantauan keamanan secara real-time, tetapi juga sebagai pusat pengujian, perencanaan strategi mitigasi, dan pengembangan edukasi keamanan siber. Selama magang, penulis berkesempatan untuk terlibat langsung dalam kegiatan penetration testing terhadap aplikasi TriUpasedanan, dengan pendampingan dari mentor profesional.

Pengujian dilakukan melalui pendekatan berbasis standar OWASP ASVS, yang bertujuan tidak hanya untuk menemukan celah keamanan, tetapi juga memahami dampak nyata dari serangan XSS serta proses mitigasinya. Serangan Cross-Site Scripting (XSS) sendiri termasuk dalam Top 10 OWASP, yaitu jenis serangan di mana penyerang menyisipkan skrip berbahaya ke dalam masukkan

pengguna. Skrip tersebut kemudian dijalankan secara otomatis oleh browser, yang dapat menyebabkan pencurian informasi penting seperti cookie session, manipulasi tampilan, hingga pengambilalihan akun. Dalam kasus TriUpasedanan, penyerang menyisipkan payload seperti `<script>alert('XSS')</script>` atau `<img src=x onerror=alert('XSS')>` pada form komentar atau edit profil. Ketika admin membuka halaman yang berisi masukkan tersebut, kode langsung aktif dan dapat mengirimkan cookie admin ke endpoint eksternal seperti xss.report.

Dengan demikian, latar belakang tugas akhir ini berfokus pada pengujian keamanan terhadap aplikasi TriUpasedanan melalui simulasi serangan XSS sebagai bagian dari proyek pembelajaran. Proyek ini juga menekankan pentingnya kolaborasi antara dunia pendidikan dan industri keamanan dalam membangun kesadaran serta keahlian praktis dalam menangani ancaman siber nyata.

1.2 Deskripsi Pekerjaan

Selama menjalani program magang di PT. Sekuriti Siber Indonesia, penulis berfokus pada berbagai tugas yang berkaitan langsung dengan praktik keamanan siber, khususnya pada aktivitas monitoring, pelaporan, dan pengujian kerentanan aplikasi web. Kegiatan ini dilakukan dalam lingkungan Security Operation Center (SOC) dengan arahan dari tim keamanan. Adapun lingkup pekerjaan yang penulis lakukan adalah sebagai berikut:

1. Monitoring Aktivitas Log di SIEM Wazuh

   Melakukan pemantauan aktivitas log sistem client secara berkala menggunakan platform Security Information and Event Management (SIEM), yaitu Wazuh. Aktivitas ini bertujuan untuk mendeteksi anomali, indikasi serangan, atau aktivitas mencurigakan lainnya yang dapat menjadi tanda dari adanya kerentanan atau upaya serangan. Dalam praktiknya, dilakukan analisis pola akses, validasi alert, dan pencatatan aktivitas yang dianggap tidak normal.
2. Pembuatan Laporan Log Mencurigakan

3.

Jika ditemukan alert mencurigakan dalam sistem log Wazuh, penulis bertanggung jawab untuk menyusun laporan yang mencakup analisis sumber alert, dampak potensial, serta rekomendasi mitigasi. Laporan ini kemudian digunakan oleh tim keamanan untuk mengambil keputusan cepat terhadap potensi insiden siber dan mencegah ancaman yang lebih besar.

4. Pembelajaran dan Praktik Penetration Testing

   Sebagai bagian dari peningkatan kapasitas teknis, penulis mengikuti kegiatan pembelajaran yang berfokus pada teknik penetration testing terhadap aplikasi web. Materi yang dipelajari meliputi pengenalan OWASP Top 10, pemindaian port menggunakan Nmap, serta eksploitasi masukkan yang tidak tervalidasi sehingga berpotensi serangan Cross-Site Scripting (XSS) dan SQL Injection.

5. Pengujian Keamanan Aplikasi Web TriUpasedanan

   Dalam kegiatan praktik, penulis turut serta dalam proyek pengujian keamanan aplikasi TriUpasedanan, yaitu aplikasi simulasi yang digunakan sebagai media pembelajaran internal. Fokus pengujian difokuskan pada kerentanan XSS, di mana dilakukan injeksi payload ke masukkan pengguna (seperti komentar dan edit profil), disertai simulasi pencurian cookie session menggunakan platform pihak ketiga (xss.report). Setelah ditemukan celah, dilakukan perbaikan dan pengujian ulang untuk memastikan keamanan aplikasi meningkat sesuai standar OWASP ASVS.

Dalam lingkup magang ini menampilkan kompleksitas yang menuntut ketelitian, kemampuan analisis, dan pemahaman mendalam tentang keamanan siber. Setiap tugas dilakukan secara kolaboratif dengan tim untuk memastikan bahwa sistem yang dikelola aman dan sesuai dengan standar keamanan yang berlaku.

1.3 Tujuan

Tujuan dari pengujian keamanan yang dilakukan adalah untuk menemukan, memeriksa, dan memperbaiki kemungkinan kerentanan Cross-Site Scripting (XSS) pada fitur-fitur utama situs web aplikasi TriUpasedanan. Kerentanan ini terutama terjadi pada form komentar dan edit profil. Langkah ini bertujuan untuk memastikan bahwa setiap masukkan yang dikirimkan oleh pengguna tidak bisa langsung dieksekusi dalam bentuk skrip berbahaya, sehingga menjaga integritas tampilan dan fungsi aplikasi.

1.4 Manfaat

Pengujian keamanan untuk mengatasi kerentanan Cross-Site Scripting (XSS) pada aplikasi web TriUpasedanan meningkatkan perlindungan data pengguna dan menjaga integritas sistem secara keseluruhan. Proses pengamanan menjadi lebih fokus dan tepat sasaran untuk mencegah penyalahgunaan masukkan yang dapat digunakan penyerang untuk mencuri sesi atau mengambil alih akun admin dengan mengidentifikasi dan menghilangkan kerentanan secara langsung pada fitur penting seperti edit profil dan komentar. Selain itu, proses pengujian ini membantu pengembang memahami efek nyata dari XSS dan pentingnya melakukan validasi dan sanitasi masukkan sebelum ditampilkan ke dalam antarmuka pengguna.