BAB V
PENUTUP

5.1 Simpulan

Penelitian ini menemukan, menguji, dan mengevaluasi masalah keamanan pada aplikasi web TriUpasedanan. Kerentanan yang difokuskan pada serangan Cross-Site Scripting (XSS) adalah yang paling berhasil. Melalui tahapan simulasi yang dilakukan mulai dari login sebagai user biasa, pengisian form seperti komentar dan edit profil, hingga simulasi sebagai attacker yang mengeksploitasi celah XSS, ditemukan bahwa masukkan dari pengguna ditampilkan langsung tanpa proses sanitasi atau validasi yang memadai.

Berikut hasil dari pengujian yang menunjukkan bahwa:

a. Fitur Edit Profil rentan terhadap XSS, terutama pada kolom masukkan nama. Payload XSS yang disisipkan langsung dijalankan tanpa validasi, menyebabkan pop-up alert muncul sebagai tanda berhasilnya injeksi skrip.
b. Fitur Komentar juga terbukti rentan terhadap XSS, di mana skrip yang disisipkan pada komentar langsung dieksekusi saat halaman dimuat.
c. Payload XSS digunakan untuk mencuri cookie admin melalui XSS Report. Ketika admin membuka halaman yang telah disisipi skrip, cookie admin dikirim secara otomatis ke endpoint pelaporan yang telah disiapkan.
d. Simulasi sebagai attacker berhasil dilakukan, di mana penyerang mengambil cookie admin dari XSS Report, memodifikasi cookie menggunakan ekstensi Cookie Editor, dan berhasil masuk ke halaman admin tanpa melakukan login.
e. Perbaikan dilakukan dengan menambahkan fungsi , yang mencegah eksekusi skrip dengan cara mengubah karakter spesial menjadi teks biasa. Setelah dilakukan perbaikan dan pengujian ulang, tidak ditemukan lagi eksekusi payload XSS, dan semua masukkan ditampilkan dengan aman sebagai teks.

5.2 Saran

Berdasarkan temuan dan analisis yang dilakukan selama penelitian, berikut

adalah beberapa rekomendasi untuk meningkatkan keamanan aplikasi TriUpasedanan :

a. Terapkan Validasi Input dan Sanitasi Output

   Setiap masukkan dari pengguna, terutama yang akan ditampilkan kembali di halaman web seperti nama profil atau komentar, harus divalidasi dan sanitasi. Gunakan fungsi atau sejenisnya agar skrip berbahaya tidak bisa dijalankan.

b. Gunakan Middleware Keamanan untuk Deteksi dan Pencegahan

   Tambahkan lapisan keamanan seperti Web Application Firewall (WAF) atau Content Security Policy (CSP) untuk mencegah eksekusi skrip berbahaya.

c. Perkuat Otentikasi dan Manajemen Session

   Gunakan autentikasi dua faktor (2FA) dan atur session timeout agar sesi login yang tidak aktif segera ditutup. Ini dapat mencegah penyalahgunaan cookie oleh pihak ketiga.

d. Latih Tim Developer Mengenai Secure Coding Practice

   Penting untuk memberikan pelatihan kepada pengembang aplikasi agar memahami praktik pengkodean yang aman (secure coding), terutama dalam menangani masukkan dan output pengguna.

Dengan menerapkan saran-saran di atas, keamanan aplikasi TriUpasedanan dapat ditingkatkan secara menyeluruh, serta memberikan perlindungan yang lebih baik terhadap data pengguna dan mencegah eksploitasi dari pihak yang tidak bertanggung jawab. Langkah-langkah tersebut juga berperan penting dalam membangun kepercayaan pengguna terhadap sistem.