BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini berhasil melaksanakan uji penetrasi menggunakan kerangka kerja ISSAF pada website dummy sebagai acuan untuk pengujian sistem keamanan website lain. Pengujian dilakukan dengan metode black box testing, yang memungkinkan identifikasi celah-celah keamanan umum pada website. Hasil analisis menunjukkan adanya beberapa kerentanan yang signifikan, seperti *SQL Injection, Cross-Site Scripting (XSS) Attack, dan Cross-Site Request Forgery (CSRF) Injection*, yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeksploitasi sistem.

Selain itu, temuan lain meliputi potensi serangan Clickjacking, Brute-force attack pada halaman login, serta pengaturan konfigurasi keamanan yang belum optimal, seperti HSTS yang hilang, CSP yang tidak diterapkan, dan SameSite cookie attributes yang tidak ada. Hasil penelitian ini menggarisbawahi pentingnya penerapan langkah-langkah mitigasi untuk mengurangi risiko terhadap ancaman siber yang lebih serius.

5.2 Saran

Berdasarkan temuan-temuan tersebut, beberapa langkah mitigasi dapat diterapkan untuk meningkatkan keamanan website dan melindunginya dari potensi serangan. Beberapa saran yang dapat diberikan antara lain:

1. Penerapan Validasi Input yang Ketat
   Menggunakan filter yang ketat pada input pengguna, terutama untuk mencegah serangan *SQL Injection dan XSS*. Validasi input baik di sisi klien maupun server sangat penting untuk memastikan bahwa data yang masuk ke sistem tidak dapat dieksploitasi.
2. Penggunaan Kebijakan Keamanan Konten (CSP)
   Menerapkan kebijakan CSP untuk mengurangi risiko serangan XSS dengan membatasi sumber daya eksternal yang dapat dimuat oleh browser.

3. Pengaturan Keamanan Cookie yang Lebih Ketat Menggunakan atribut SameSite untuk cookie dan memastikan bahwa cookie tidak mudah disalahgunakan dalam serangan CSRF.
4. Penerapan HSTS dan Pengaturan HTTPS
   Menggunakan HSTS untuk memastikan bahwa komunikasi dengan website selalu dilakukan melalui protokol HTTPS, sehingga menghindari potensi serangan man-in-the-middle.
5. Mengamankan Halaman Login Menerapkan pembatasan percakapan login dan menggunakan metode otentikasi yang lebih kuat, seperti CAPTCHA atau otentikasi dua faktor (2FA), untuk melindungi dari serangan Brute-force.
6. Menghapus Informasi Sensitif pada Header HTTP
   Menyembunyikan informasi sensitif pada header HTTP seperti X-Powered-By untuk mengurangi eksposur terhadap potensi eksploitasi oleh pihak luar.

Dengan menerapkan langkah-langkah mitigasi tersebut, keamanan website dapat meningkat secara signifikan, mengurangi potensi kerentanannya, dan memastikan perlindungan yang lebih baik terhadap data dan sistem.