BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilakukan mengenai analisis keamanan website almudaya.or.id menggunakan metode *penetration testing* berbasis *OWASP* Top 10, maka diperoleh beberapa kesimpulan penting sebagai berikut:

1. Metode *penetration testing* efektif untuk mengevaluasi keamanan website.

   Penelitian ini menunjukkan bahwa metode *penetration testing* dapat digunakan untuk mengidentifikasi kelemahan keamanan yang ada pada sebuah website secara sistematis. Tahapan yang dilakukan mulai dari information gathering, vulnerability scanning, analisis manual, hingga *Proof of Concept (PoC)* mampu memberikan gambaran nyata tentang kondisi keamanan website yang diuji.

2. Website almudaya.or.id masih memiliki beberapa celah keamanan yang perlu diperhatikan.

   Dari hasil pemindaian kerentanan menggunakan tools *Arachni*, ditemukan berbagai jenis kerentanan yang berpotensi dieksploitasi. Kerentanan tersebut mencakup Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), parameter tampering pada transaksi, bypass *CAPTCHA*, clickjacking, serta beberapa kelemahan konfigurasi keamanan lainnya. Hal ini menunjukkan bahwa sistem masih memiliki celah pada aspek validasi *input*, kontrol akses,

dan konfigurasi server.

3. *Proof of Concept (PoC)* membuktikan bahwa sebagian kerentanan benar-benar dapat dieksploitasi.

   Tahapan PoC dilakukan untuk memastikan bahwa temuan hasil scanning tidak hanya bersifat indikatif, tetapi benar-benar dapat dimanfaatkan dalam kondisi tertentu. Hasil penelitian membuktikan bahwa kerentanan seperti Reflected XSS pada halaman registrasi, CSRF pada proses transaksi checkout, manipulasi harga transaksi, bypass *CAPTCHA*, dan clickjacking dapat dilakukan secara nyata. Dengan demikian, temuan yang dihasilkan memiliki validitas yang kuat.

4. Kerentanan yang ditemukan memiliki keterkaitan langsung dengan kategori *OWASP* Top 10.

   Hasil analisis menunjukkan bahwa sebagian besar kerentanan yang ditemukan termasuk dalam kategori risiko *OWASP* Top 10, khususnya pada:

   a. A01 Broken Access Control, seperti CSRF dan parameter tampering
   b. A03 Injection, seperti XSS
   c. A05 Security Misconfiguration, seperti clickjacking dan direktori umum
   d. A07 Identification and Authentication Failures, seperti *CAPTCHA* bypass

   Dominasi kategori tersebut menunjukkan bahwa kelemahan utama website terletak pada kontrol akses transaksi dan konfigurasi keamanan aplikasi yang belum optimal.

5. Website sudah memiliki keamanan dasar, tetapi masih memerlukan penguatan lebih lanjut.

Website almudaya.or.id telah menggunakan HTTPS dengan sertifikat SSL yang valid, sehingga komunikasi data sudah terenkripsi. Namun, beberapa pengaturan keamanan aplikasi web masih perlu diperbaiki agar website dapat lebih tahan terhadap serangan siber, terutama pada fitur yang bersifat sensitif seperti autentikasi dan transaksi pembayaran.

6. Hasil penelitian ini dapat menjadi bahan evaluasi bagi pengelola website.

   Temuan dalam penelitian ini dapat digunakan sebagai dasar untuk meningkatkan keamanan website, mengurangi risiko eksploitasi di masa depan, serta menjaga kepercayaan pengguna terhadap sistem yang digunakan.

5.2 SARAN

Berdasarkan hasil penelitian serta kerentanan yang ditemukan, peneliti memberikan beberapa saran perbaikan sebagai berikut:

1. Pengelola website perlu segera menerapkan mitigasi sesuai rekomendasi *OWASP* Top 10.

   Perbaikan keamanan harus dilakukan secara menyeluruh dengan mengacu pada standar internasional seperti *OWASP*, agar sistem lebih terlindungi dari berbagai jenis serangan web modern.

2. Pencegahan XSS harus diperkuat melalui validasi *input* dan encoding output.

   Semua *input* pengguna yang ditampilkan kembali pada halaman web harus difilter dan diencoding dengan benar agar tidak dapat disisipkan kode berbahaya. Selain itu, penerapan Content Security Policy (CSP) juga

disarankan untuk membatasi eksekusi skrip berbahaya di browser.

3. Perlindungan CSRF dan keamanan transaksi checkout wajib ditingkatkan.

   Website perlu menerapkan token anti-CSRF pada semua form sensitif, khususnya transaksi pembayaran. Server juga harus memvalidasi permintaan yang masuk agar tidak dapat dipicu dari halaman eksternal tanpa izin pengguna.

4. Parameter sensitif seperti harga transaksi harus divalidasi di sisi server.

   Sistem tidak boleh mempercayai nilai yang dikirimkan oleh klien, karena dapat dimodifikasi dengan mudah. Harga dan nominal transaksi harus dihitung langsung oleh server berdasarkan database.

5. Sistem *CAPTCHA* harus dikonfigurasi ulang dan divalidasi secara server-side.

   CAPTCHA tidak boleh hanya ditampilkan di halaman, tetapi harus diverifikasi dengan API resmi agar tidak bisa dilewati oleh penyerang menggunakan request manual atau bot otomatis.

6. Penerapan security headers sangat penting untuk mencegah clickjacking.

   Website perlu menerapkan header X-Frame-Options atau Content-Security-Policy frame-ancestors untuk mencegah halaman dimuat dalam iframe eksternal.

7. Pengujian keamanan perlu dilakukan secara berkala.

   Karena ancaman siber terus berkembang, pengelola website disarankan melakukan vulnerability assessment dan *penetration testing* secara rutin untuk mendeteksi kerentanan baru serta menjaga keamanan sistem jangka

panjang.

8. Penelitian selanjutnya dapat dilakukan dengan cakupan yang lebih luas. Penelitian berikutnya dapat mengembangkan pengujian pada aspek lain seperti keamanan API, audit source code (white box testing), serta pengujian eksploitasi lebih lanjut untuk memperoleh hasil yang lebih komprehensif.

.