BAB V
PENUTUP

Pada bab penutup ini berisi ringkasan dari seluruh proses pengujian keamanan yang telah dilakukan pada website RPH Surabaya. Berdasarkan hasil vulnerability scanning dengan OWASP ZAP, validasi menggunakan Burp Suite, Firefox Developer Tools, dan SQLMap, serta analisis terhadap temuan kerentanan, ditemukan beberapa celah keamanan yang tervalidasi beserta rekomendasi perbaikan. Selanjutnya, akan dijelaskan kesimpulan serta saran yang diharapkan dapat menjadi panduan bagi pengelola website dalam meningkatkan tingkat keamanan sistem, melindungi data sensitif, dan mencegah potensi serangan siber yang mungkin terjadi di masa yang akan datang.

5.1. Kesimpulan

Berdasarkan hasil pengujian keamanan web RPH Surabaya menggunakan NIST SP 800-115 sebagai acuan metodologi dan OWASP Top 10 2021 acuan kerentanan, diperoleh beberapa kesimpulan sebagai berikut:

1. Proses pengujian teknis dilakukan melalui tahap *discovery* yang terdapat 2 tahap didalamnya, yang pertama adalah *information gathering* menggunakan tools seperti Nslookup, Whois, Nmap, Dirsearch, Wappalyzer, dan Google Dorking, yang kedua adalah *vulnerability scanning* dengan OWASP ZAP, serta setelah *discovery* yaitu tahap *attack* dengan validasi menggunakan Burp Suite, Firefox Developer Tools, dan SQLMap yang dijalankan pada OS Kali Linux, dan *reporting* sebagai pelaporan. Pendekatan OWASP Top 10 2021 digunakan sebagai kerangka utama untuk kategorisasi kerentanan serta referensi rekomendasi perbaikan dan NIST SP 800-115 sebagai acuan utama metodologi pengujian.
2. Hasil scanning OWASP ZAP berdasarkan OWASP Top 10 2021 mendeteksi 13 kerentanan potensial. Dari jumlah tersebut, setelah validasi pada tahap *attack*, terdapat 10 kerentanan yang terkonfirmasi valid, yaitu *Absence of Anti-CSRF Tokens, Directory Browsing, Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, Vulnerable JS Library (jQuery outdated), Cookie No HttpOnly Flag (pada cookie poling), Cookie without SameSite Attribute (pada ci_session), Strict-Transport-Security Header Not Set, X-Content-Type-Options Header Missing*, serta *User Controllable HTML*

Element Attribute (Potential XSS). Kerentanan ini sebagian besar termasuk dalam kategori A05: *Security Misconfiguration* dan A03: *Injection* pada OWASP Top 10 2021, dengan beberapa *false positive* atau beberapa kerentanan tidak tervalidasi seperti SQL Injection dengan 2 alert dan Application Error Disclosure.

3. Untuk mengatasi kerentanan yang tervalidasi, pertama direkomendasikan penerapan konfigurasi header keamanan seperti CSP, X-Frame-Options, X-Content-Type-Options, dan Strict-Transport-Security. Kedua melakukan update library jQuery ke versi terbaru dengan SRI. Ketiga penonaktifan directory listing. Keempat melakukan penambahan flag HttpOnly dan SameSite pada cookie. Langkah-langkah ini diharapkan dapat meningkatkan tingkat keamanan situs, mengurangi risiko serangan seperti XSS, clickjacking, dan *misconfiguration*, serta mendukung praktik pengelolaan keamanan berkelanjutan bagi pengembang dan administrator website.

5.2. Saran

Berdasarkan hasil pengujian keamanan web RPH Surabaya, berikut beberapa saran yang dapat diimplementasikan untuk meningkatkan keamanan website serta pengembangan penelitian selanjutnya:

1. Segera menerapkan rekomendasi perbaikan terhadap 10 kerentanan yang telah tervalidasi, seperti penambahan header keamanan (CSP, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security), melakukan update jQuery ke versi terbaru dengan SRI, penonaktifan directory listing, serta konfigurasi flag HttpOnly dan SameSite pada cookie. Langkah ini akan mengurangi risiko serangan XSS, clickjacking, CSRF, dan misconfiguration, sehingga situs memiliki perlindungan yang lebih kuat terhadap ancaman.
2. Lakukan maintenance rutin terhadap website, termasuk monitoring log akses server untuk deteksi kerentanan, update dependensi (library dan framework CodeIgniter) secara berkala, serta pengujian ulang untuk memverifikasi bahwa kerentanan tidak lagi dapat dieksploitasi dan tidak muncul celah baru.
3. Administrator website disarankan untuk monitoring lalu lintas web, misalnya dengan atau log analyzer, untuk mendeteksi upaya serangan dan meminimalisir dampak serangan skala yang lebih besar, serta dapat memastikan keamanan website.

Halaman ini sengaja dikosongkan