

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa:

1. Penelitian berhasil melakukan analisis keamanan pada website skripsifasilkom.id dengan metode *penetration testing* berbasis OWASP Top 10, berfokus pada pengujian kerentanan *SQL Injection* menggunakan *tools* BurpSuite dan SQLMap. Hasil pengujian menunjukkan bahwa tidak ditemukan celah *SQL Injection* pada *form login*, yang mengindikasikan adanya penerapan mekanisme keamanan input yang memadai.
2. Meskipun tidak ditemukan kerentanan *SQL Injection*, pengujian lanjutan menggunakan OWASP ZAP mengidentifikasi beberapa potensi kerentanan lain dengan tingkat risiko rendah hingga sedang, seperti tidak adanya *header* keamanan (*Content Security Policy*, *Anti-Clickjacking*), penggunaan *JavaScript library* yang rentan, serta konfigurasi *cookie* yang kurang aman.
3. Berdasarkan hasil identifikasi dan penilaian risiko terhadap seluruh temuan, dapat disimpulkan bahwa website skripsifasilkom.id tergolong cukup aman terhadap eksploitasi *SQL Injection*, namun tetap disarankan untuk melakukan perbaikan terhadap kerentanan minor guna meningkatkan keamanan sistem secara menyeluruh dan mencegah potensi penyalahgunaan di masa depan.
4. Penilaian risiko terhadap seluruh temuan menggunakan CVSS v3.1 menghasilkan skor berkisar antara 3.1 (*low*) hingga 6.5 (*medium*). Skor ini menunjukkan bahwa meskipun kerentanan yang ditemukan bersifat minor dan tidak berdampak langsung terhadap integritas atau ketersediaan sistem

secara kritis, perbaikan tetap diperlukan untuk meningkatkan ketahanan dan keamanan sistem secara menyeluruh.

5.2 Saran

Berdasarkan hasil penelitian ini, penulis memberikan beberapa rekomendasi sebagai langkah perbaikan, yaitu:

1. Menerapkan header keamanan seperti *Content Security Policy (CSP)*, *X-Frame-Options*, *Strict-Transport-Security*, dan *X-Content-Type-Options* untuk mengurangi risiko serangan seperti *clickjacking* dan *cross-site scripting*.
2. Memperbarui dan rutin memeriksa *library* JavaScript yang digunakan pada *website* agar terhindar dari kerentanan yang terdapat pada versi lama.
3. Mengimplementasikan mekanisme token *anti-CSRF* pada *form-form* penting, khususnya yang terkait proses autentikasi, untuk mencegah serangan *Cross-Site Request Forgery*.
4. Melakukan pengujian keamanan secara berkala (*penetration testing*), termasuk pada fitur lain di luar *form login*, guna mendeteksi potensi kerentanan yang mungkin muncul akibat pembaruan sistem atau perubahan konfigurasi.
5. Meningkatkan *monitoring* dan *logging* sistem untuk mendeteksi aktivitas mencurigakan secara lebih dini, serta memanfaatkan *Web Application Firewall (WAF)* sebagai lapisan keamanan tambahan.

Untuk penelitian selanjutnya, disarankan memperluas pengujian ke kerentanan lain seperti *Cross-Site Scripting (XSS)*, *Broken Access Control*, atau uji terhadap konfigurasi keamanan server guna memperoleh gambaran keamanan *website* yang lebih komprehensif. Dengan demikian, dapat disimpulkan bahwa situs

skripsifasilkom.id , pada cakupan pengujian yang dilakukan, cukup aman terhadap serangan *SQL Injection*. Namun, penguatan aspek keamanan lainnya masih perlu diterapkan agar situs *web* lebih tangguh dalam menghadapi potensi serangan siber di masa depan.

