BAB V

PENUTUP

Dari hasil analisis dan uji kerentanan pada website posketanmu.mojokertokab.go.id, ditemukan berbagai kelemahan keamanan pada website. Proses pengujian melibatkan metode *Google Penetration Testing* dan standar OWASP Top 10. Langkah-langkah perbaikan meliputi penerapan kebijakan keamanan yang lebih ketat dan pembaruan konfigurasi server. Tujuan penelitian ini untuk mengetahui, menganalisis, dan memberikan rekomendasi perbaikan keamanan pada website Posketanmu berhasil tercapai. Dari analisis yang telah dilakukan, didapatkan kesimpulan dan saran dari penelitian ini yaitu :

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, hasil pengujian keamanan dari website posketanmu.mojokertokab.go.id menggunakan *metode Google Penetration Testing* dan metode OWASP Top 10 2021 diperoleh kesimpulan :

1. Proses pengujian keamanan website posketanmu.mojokertokab.go.id dilakukan dengan *google penetration testing* atau *google dorking* dengan menggunakan operator pencarian khusus serta kueri untuk mencari informasi yang rentan atau sensitif yang ada pada website posketanmu. Selanjutnya, digunakan metode OWASP Top 10 2021 yang digunakan sebagai kerangka kerja untuk evaluasi serta rekomendasi perbaikan. Penelitian ini melibatkan serangkaian teknik exploitasi untuk uji kerentanan dengan berbagai alat yang dirancang untuk mengekspos dan mengevaluasi kerentanan website. Proses ini *mencakup information gathering, vulnerability scanning, vulnerability assessment, exploitation dan reporting*.
2. Hasil pengujian menunjukkan adanya 19 kerentanan pada website posketanmu.mojokertokab.go.id. dengan 11 kerentanan yang diuji coba dan 4 kerentanan yang berhasil ditemukan. Pertama, kerentanan CSP *header Not Set,* yang menunjukkan bahwa website tidak menerapkan *header content-security policy* sehingga website mungkin rentan terhadap serangan XSS. Kedua, kerentanan *open redirect*, dimana pengguna website dapat diarahkan ke situs web yang berbahaya tanpa sepengetahuan pengguna.

Ketiga, kerentanan XSS stored, dimana website posketanmu dapat disisipkan skrip yang berbahaya ke dalam halaman website yang dapat dilihat oleh pengguna lain. Keempat, kerentanan *Strict-transport security Header not set* , dimana website rentan terhadap serangan *Man-in the-Middle* dan serangan serupa.

3. Untuk mengatasi dan mencegah kerentanan keamanan ini, ada beberapa langkah yang dapat diambil. Pertama, mengatur *header* CSP sehingga website memiliki proteksi lebih dalam hal perlindungan dari serangan XSS dan injeksi data. Kedua, melakukan validasi dan sanitasi URL secara ketat untuk mencegah open redirect. Ketiga, validasi input yang cermat pada sisi klien dan server merupakan langkah tepat untuk mencegah XSS Stored. Keempat, menggunakan pengaturan *header* HSTS atau *Strict-Transport-Security*.

5.2 Saran

Setelah melakukan pengujian keamanan website posketanmu.mojokertokab.go.id, beberapa saran yang dapat diimplementasikan adalah:

1. Setelah menyelesaikan tahap penetration testing yang melibatkan *exploitation*, dapat mempertimbangkan untuk mengembangkan skenario serangan lanjutan yang lebih kompleks. Misalnya, dari hasil penelitian ini, menemukan bahwa website POSKETANMU rentan terhadap serangan XSS. Dengan memanfaatkan informasi yang terkumpul selama fase *exploitation*, dapat mengembangkan skenario serangan yang lebih canggih, seperti serangan bertingkat yang mencakup *eksploitasi* XSS untuk mendapatkan akses ke sistem atau informasi yang lebih sensitif.
2. Segera melakukan perbaikan pada kerentanan yang berhasil teridentifikasi di website posketanmu.mojokertokab.go.id. Dengan melakukan langkah – langkah perbaikan mampu mengurangi risiko serangan dan website memiliki perlindungan yang lebih baik terhadap berbagai serangan.
3. Setelah pelaporan hasil penelitian, tim pengembang akan menerapkan dan melakukan mitigasi untuk mengatasi kerentanan yang ditemukan. Lalu, melakukan pengujian lanjutan setelah penerapan mitigasi untuk memastikan

bahwa langkah-langkah tersebut efektif dan tidak menyebabkan kerentanan baru. Misalnya, setelah penerapan mengatasi kerentanan XSS, dapat melakukan pengujian ulang untuk memverifikasi bahwa serangan XSS tidak lagi dapat direplikasi.

4. Melakukan pengujian lanjutan selain menggunakan metode google *penetration testing* dan metode OWASP top 2021.

Dengan saran yang telah diuraikan, diharapkan keamanan website posketanmu.mojokertokab.go.id dapat ditingkatkan secara signifikan, sehingga mengurangi kemungkinan serangan dan peningkatan perlindungan terhadap data pengguna dengan lebih efisien.