BAB V
PENUTUP

Pada bab ini, akan disajikan kesimpulan dari hasil penelitian yang telah dilakukan pada *website* Dinas Sosial Surabaya melalui pengujian *penetration testing*. Berdasarkan temuan-temuan yang diperoleh selama pengujian, serta analisis terhadap kerentanannya, beberapa rekomendasi perbaikan akan diberikan. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan *website*, dengan mengidentifikasi potensi kerentanan yang ada dan memberikan langkah-langkah mitigasi yang sesuai. Pada akhirnya, diharapkan hasil dari penelitian ini dapat memberikan panduan yang jelas bagi pengelola *website* untuk meningkatkan sistem keamanan yang ada dan melindungi data serta informasi penting dari ancaman yang mungkin terjadi.

5.1. Kesimpulan

Derdasarkan penelitian ini, hasil pengujian keamanan pada *website* Dinas Sosial Surabaya dengan menggunakan metode *penetration testing* dan pendekatan OWASP Top 10 dan MITRE ATT&CK diperoleh Kesimpulan :

1. Proses pengujian keamanan *website* Dinas Sosial Surabaya dilakukan dengan metode penetration testing yang terdiri dari 5 proses yaitu *information gathering, footprinting & scanning, vulnerability assessment, exploitation,* dan *analyze & report*. Selanjutnya, digunakan pendekatan OWASP Top 10 2021 yang digunakan sebagai kerangka kerja untuk evaluasi serta rekomendasi perbaikan serta pendekatan MITRE ATT&CK untuk melakukan pengujian exploitasi terhadap *website.*
2. Hasil pengujian menunjukan terdapat 17 indikasi kerentanan yang ada pada *website* Dinas Sosial Surabaya. Semua kerentanan tersebut diuji coba dan didapatkan 6 kerentanan yang berhasil ditemukan. Pertama, kerentanan *Browsable Web Directories*, dimana terdapat direktori terbuka yang berisi data mengenai *website* yang seharusnya tidak bisa diakses oleh pengguna umum. Kedua, *web.config File Information Disclosure* yang menunjukan *file web.config website* terbuka, sehingga pengguna bisa melihat konfigurasi penting pada *website*. Ketiga. *Content Security Policy (CSP) Header Not Set*, yang dimana *website* tidak menerapkan header

content security policy (CSP) sehingga *website* mungkin rentan terhadap serangan XSS. Keempat, *Strict-Transport-Security Header Not Set*, dimana *website* memungkinkan rentan terhadap serangan *Man-in the-Middle* (MITM). Kelima *Timestamp Disclosure – Unix*, dimana *website* menunjukan informasi waktu dalam format Unix Timestamp tanpa pengamanan. Keenam, kerentanan *X-Content-Type-Options Header Missing*, dimana *website* tidak mengatur *HTTP XContent-Type-Options* yang membuat konten diperlakukan sebagai jenis file yang tidak diinginkan.

3. Untuk mengatasi dan mencegah kerentanan tersebut, ada beberapa langkah yang dapat diambil yaitu meliputi penerapan *header Content-Security-Policy* (CSP) untuk mencegah serangan *Cross-Site Scripting* (XSS), penggunaan *header X-Content-Type-Options: nosniff* dan *Strict-Transport-Security* (HSTS) guna meningkatkan perlindungan terhadap serangan *MIME-sniffing* dan memastikan komunikasi terenkripsi. Selain itu, disarankan untuk menonaktifkan direktori yang dapat diakses publik untuk menghindari *Browsable Web Directories* dan menyembunyikan *file* konfigurasi yang sensitif untuk mencegah *File Information Disclosure*. Terakhir, pemantauan dan pembaruan secara berkala terhadap *timestamp Unix* pada *header response* untuk mengurangi *Timestamp Disclosure* akan semakin meningkatkan keamanan *website*. Penerapan langkah-langkah ini diharapkan dapat mengurangi risiko serangan dan menjaga keamanan *website* secara keseluruhan.

5.2. Saran

Setelah melakukan pengujian keamanan *website* Dinas Sosial Surabaya, terdapat beberapa saran yang dapat dilakukan sebagai berikut:

1. Segera melakukan perbaikan terhadap kerentanan yang berhasil di uji coba dan terindentifikasi pada *website* Dinas Sosial Surabaya. Dengan melakukan langkah-langkah perbaikan diharapkan mampu mengurangi resiko serangan dan *website* memiliki perlindungan yang lebih baik terhadap serangan yang bisa terjadi.
2. Melakukan *maintenance* terhadap *website* Dinas Sosial secara teratur dan Melakukan pengujian lanjutan dengan tingkatan yang lebih lanjut.

3. Administrator harus memonitor terhadap lalu lintas *website* agar meminimalisir serangan dengan skala yang lebih besar.
4. Disarankan untuk penelitian selanjutnya mengembangkan atau menggunakan kombinasi metode pengujian keamanan lainnya, seperti NIST Cybersecurity Framework atau ISO/IEC 27001, untuk mendapatkan perspektif keamanan yang lebih luas dan menyeluruh terhadap aplikasi web, khususnya di sektor pemerintahan.