BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah di lakukan, dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Dengan menggunakan tools OWASP ZAP dan Security Headers peneliti dapat menemukan beberapa kerentanan yang ada pada website YAS-ID setelah dilakukan penetration testing pada website tersebut.
2. Proses Pengujian keamanan web server pada website YAS-ID dilakukan dengan mengumpulkan data kerentanan dari hasil scanning menggunakan tools OWASP ZAP dan Security Headers, dari hasil pengujian yang telah dilakukan bahwa terdapat beberapa kerentanan, seperti Content Security Policy, Cross Domain Misconfiguration, Missing Anti Clickjacking Header, Cross Domain Java Script Source File Inclusion, Strict Transport Security Header, X Content Type Options Header, Information Disclosure, Modern Web Application, Re exanime Cache Control, Retrived from Cache. Tetapi peneliti hanya berfokus pada 3 kerentanan yatu Content Security Policy, Cross Domain Misconfiguration, dan Missing Anti Clickjacking Header dan menurut klasifikasi OWASP TOP 10 2021 kerentanan tersebut termasuk dalam ***A05:2021 – Security Misconfiguration.***
3. Berdasarkan hasil pengujian terdapat kerentanan yang telah dinilai sebagai kerentanan yang berbahaya yaitu Content Security Policy, Cross Domain Misconfiguration, dan Missing Anti Clickjacking Header karena merupakan 3 teratas kerentanan yang ada setelah dilakukan proses scanning menggunakan OWASP ZAP, proses minimalisir kerentanan tersebut dilakukan degan menambahkan Script pada web server file .htaccess website YAS-ID, hasil pengujian kembali dilakukan dengan OWASP ZAP sebanyak 30 kali setelah dilakukan penambahan Script mendapatkan hasil bahwa kerentanan Cross Domain Misconfiguration dan Missing Anti Clickjacking Header tidak ditemukan sedangkan Content Security Policy mengalami penurunan nilai kerentanan.

5.2 Saran

Pada penelitian ini masih terdapat beberapa kelemahan yang dapat dikembangkan pada penelitian selanjutnya, antara lain:

1. Penelitian ini hanya berfokus pada pengujian dari kerentanan berdasarkan klasifikasi Top 10 OWASP dengan menggunakan tools OWASP ZAP dan Security Headers, sehingga untuk penelitian selanjutnya dapat melakukan pengujian menggunakan tools lainnya atau yang lebih baik agar mendapatkan data yang lebih akurat.
2. Dalam penelitian ini ditemukan beberapa kerentanan dengan tingkat risiko rendah hingga menengah. Oleh karena itu, disarankan agar perusahaan dan Developer selalu melakukan uji keamanan pada aplikasi sebelum diperkenalkan kepada pengguna secara publik.
3. Mengkonfigurasi sistem web untuk mengamankan data yang seharusnya tidak ditampilkan, bertujuan untuk mencegah potensi ancaman dari pihak yang tidak bertanggung jawab.