BAB V
PENUTUP

Dalam bab ini akan dijelaskan kesimpulan dari penelitian yang telah dilakukan pada bab sebelumnya.

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pengujian keamanan pada Website SIPATCA menggunakan metode ISSAF dengan pendekatan black box serta acuan OWASP Web Security Testing Guide (WSTG) v4.2, diperoleh kesimpulan sebagai berikut:

1. Berdasarkan hasil pengujian, ditemukan beberapa kerentanan keamanan pada Website SIPATCA yang berkaitan dengan konfigurasi keamanan server, penerapan security header, dan keamanan sisi klien. Kerentanan yang berhasil divalidasi meliputi missing security headers, password field autocomplete enabled, browser cache weakness, server version disclosure, serta redirect/information disclosure. Namun, tidak ditemukan kerentanan kritis seperti SQL Injection, Cross Site Scripting (XSS), Remote Code Execution, maupun authentication bypass.
2. Hasil analisis menggunakan metode ISSAF dengan pendekatan black box menunjukkan bahwa Website SIPATCA secara umum telah memiliki mekanisme keamanan yang cukup baik pada proses autentikasi dan manajemen sesi. Session ID berhasil berubah setelah login sehingga terhindar dari session fixation, cookie session telah menggunakan atribut HttpOnly, komunikasi login menggunakan protokol HTTPS, serta pengelolaan CSRF token berjalan dengan baik. Selain itu, beberapa hasil scanning dikategorikan sebagai informational atau false positive sehingga tidak termasuk kerentanan valid.

Rekomendasi teknis yang dapat diberikan untuk meningkatkan keamanan website meliputi penerapan security headers seperti Content Security Policy (CSP), X-Frame-Options, X-Content-Type-Options, dan HTTP Strict Transport Security (HSTS), penonaktifan autocomplete pada form login, pengamanan cache browser, penyembunyian informasi versi server, serta evaluasi konfigurasi keamanan server

secara berkala. Berdasarkan keseluruhan hasil pengujian, Website SIPATCA berada pada tingkat risiko rendah hingga sedang.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk pengembangan dan peningkatan keamanan Website SIPATCA di masa mendatang, yaitu sebagai berikut:

1. Pengelola Website SIPATCA disarankan untuk melakukan evaluasi dan pemeliharaan sistem secara rutin agar keamanan website tetap terjaga dari perkembangan ancaman siber yang terus meningkat. Selain itu, penerapan standar keamanan website sesuai pedoman OWASP perlu terus diperhatikan guna meminimalisir potensi celah keamanan pada sistem.
2. Pengembang website disarankan untuk melakukan monitoring serta audit keamanan secara berkala, terutama setelah adanya pembaruan sistem maupun penambahan fitur baru. Pengujian keamanan secara rutin dapat membantu dalam mengidentifikasi potensi risiko sejak dini sehingga mitigasi dapat dilakukan sebelum kerentanan dimanfaatkan oleh pihak yang tidak bertanggung jawab.
3. Penelitian selanjutnya disarankan untuk menggunakan metode pengujian keamanan lainnya atau memperluas cakupan pengujian pada sistem yang berbeda agar diperoleh hasil analisis yang lebih mendalam dan komprehensif. Selain itu, penelitian berikutnya juga dapat mengombinasikan pengujian manual dan automated tools yang lebih beragam, serta melakukan analisis pada aspek lain seperti keamanan jaringan, keamanan API, maupun konfigurasi server sehingga hasil penelitian menjadi lebih luas dan terstruktur.

Halaman ini sengaja dikosongkan