BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap sistem SPADA UNTIRTA maka dapat disimpulkan beberapa hal sebagai berikut:

1. Berdasarkan hasil pemindaian dan analisis, ditemukan empat jenis kerentanan keamanan pada sistem SPADA UNTIRTA, terdiri atas tiga kerentanan dengan tingkat risiko Medium dan satu kerentanan dengan tingkat risiko Low. Kerentanan yang teridentifikasi meliputi *Content Security Policy (CSP) Header Not Set, Hidden File Found (composer.lock dan phpinfo.php),* TLS 1.0 dan TLS 1.1 masih aktif, serta *Timestamp Disclosure (Unix).* Temuan ini menunjukkan bahwa kelemahan sistem lebih banyak disebabkan oleh pengaturan konfigurasi keamanan web dan hardening server yang belum optimal, terutama pada pengelolaan header keamanan dan pembatasan akses file internal. Berdasarkan pemetaan ke OWASP *Top* 10 tahun 2021, temuan *CSP Header Not Set, Hidden File Found, dan Timestamp Disclosure (Unix)* termasuk dalam kategori *A05: Security Misconfiguration*, karena berkaitan dengan konfigurasi keamanan yang kurang ketat dan adanya informasi/komponen yang terekspos ke publik. Sementara itu, temuan TLS 1.0 dan TLS 1.1 masih aktif dipetakan ke *A02: Cryptographic Failures* karena terkait langsung dengan penggunaan protokol enkripsi yang sudah usang dan berpotensi melemahkan keamanan komunikasi. Dengan demikian, hasil penelitian menegaskan bahwa area prioritas perbaikan berada pada pengetatan konfigurasi keamanan (A05) dan penguatan enkripsi komunikasi (A02) untuk menurunkan risiko kebocoran informasi serta potensi penyalahgunaan celah pada layanan.
2. Berdasarkan tingkat risikonya, tidak ditemukan kerentanan dengan kategori *High Severity*. Dari total empat temuan, tiga kerentanan (75%) tergolong *Medium* dan satu kerentanan (25%) tergolong *Low*. Kerentanan dengan tingkat risiko *Medium* memiliki potensi berdampak langsung terhadap aspek

Confidentiality dan Integrity, karena dapat menyebabkan kebocoran informasi sensitif, penyadapan data, atau manipulasi konten web. Sementara itu, kerentanan dengan tingkat risiko *Low*, yaitu *Timestamp Disclosure*, memiliki dampak terbatas namun tetap berpotensi dimanfaatkan untuk mengumpulkan informasi teknis mengenai sistem. Tidak ditemukan celah yang secara langsung memengaruhi aspek *Availability*, sehingga layanan SPADA masih dapat berjalan, meskipun terdapat risiko terhadap keamanan data dan integritas informasi.

3. Langkah mitigasi yang direkomendasikan untuk mengatasi temuan tersebut meliputi penerapan *Content-Security-Policy (CSP)* dengan konfigurasi yang tepat untuk mencegah serangan *Cross-Site Scripting (XSS)*, penghapusan file sensitif dari direktori publik untuk mencegah kebocoran informasi server, serta penonaktifan protokol TLS 1.0 dan 1.1 guna memastikan komunikasi data terenkripsi dengan aman. Selain itu, disarankan untuk menghapus informasi *timestamp dari header HTTP*, melakukan audit keamanan secara berkala dan memperbarui sertifikat enkripsi secara rutin

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, penulis memberikan beberapa saran sebagai berikut:

1. Untuk pengelola sistem SPADA UNTIRTA:

   Pengelola web SPADA disarankan untuk segera memperbaiki pengaturan keamanan sistem. Langkah yang bisa dilakukan antara lain dengan menambahkan *Content-Security-Policy (CSP)* untuk mencegah penyisipan skrip berbahaya, menghapus file sensitif seperti *phpinfo.php* dan *composer.lock* dari folder publik agar tidak bisa diakses orang luar, serta menonaktifkan protokol lama TLS 1.0 dan 1.1 dan menggantinya dengan versi terbaru seperti TLS 1.2 atau 1.3 agar data pengguna lebih aman. Selain itu, perlu dilakukan pemeriksaan keamanan secara rutin menggunakan alat seperti OWASP ZAP dan Acunetix, serta memberikan pelatihan dasar keamanan web bagi pengelola dan pengembang sistem supaya kesadaran terhadap pentingnya keamanan data bisa meningkat.

2. Untuk penelitian selanjutnya:

   Dapat dilakukan pengujian lanjutan dengan metode berbeda, seperti NIST SP 800-115 dan Penelitian ini masih terbatas pada penggunaan dua alat pengujian, yaitu OWASP ZAP dan Acunetix. Peneliti selanjutnya disarankan untuk menggunakan lebih banyak alat uji, seperti Burp Suite atau Nessus, agar hasil pengujian lebih lengkap dan akurat. Selain itu, penelitian berikutnya dapat menambahkan uji coba serangan secara langsung (penetration testing) untuk melihat sejauh mana sistem mampu menahan serangan. Peneliti juga bisa meneliti aspek ketersediaan sistem (Availability) agar tidak hanya fokus pada kerahasiaan dan integritas data, tetapi juga pada kemampuan sistem dalam tetap berfungsi meskipun terjadi gangguan.