BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pengujian keamanan pada website Sistem Akademik (SIAMIK) UPN "Veteran" Jawa Timur menggunakan teknik *penetration testing* dengan OWASP TOP 10 maka dapat disimpulkan beberapa kesimpulan sebagai berikut :

1. Pengujian celah keamanan website SIAMIK menggunakan teknik *Penetration Testing* berdasarkan OWASP TOP 10 merujuk pada proses uji penetrasi yang dilakukan terhadap sistem atau aplikasi web SIAMIK dengan tujuan untuk mengidentifikasi dan mengevaluasi celah keamanan yang mungkin ada. Teknik ini menggunakan kerangka kerja yang dikenal sebagai OWASP TOP 10, yang menyajikan sepuluh kerentanan keamanan paling umum pada aplikasi web yang sering dieksploitasi oleh para penyerang.
2. Hasil pemindaian terhadap website SIAMIK menunjukkan adanya 23 celah keamanan, dari jumlah tersebut ditemukan 20 celah yang masuk kedalam kategori OWASP TOP 10 yaitu Broken Access Control, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, dan Software and Data Integrity Failures. Teridentifikasi 5 celah dengan risiko tinggi, 4 celah dengan risiko sedang, 9 celah dengan risiko rendah, dan 5 celah tergolong dalam kategori informasi. Pengujian dilakukan secara spesifik terhadap celah keamanan dengan tingkat risiko tinggi yaitu Cross Site Scripting Reflected, Hash Disclosure, SQL Injection - Oracle - Time Based, SQL Injection – SQLite, dan Path Traversal. Pengujian juga dilakukan terhadap celah dengan tingkat risiko sedang, seperti Content Security Policy Header Not Set, Missing Anti-clickjacking Header, Vulnerable JS Library, dan Absence of Anti-CSRF Tokens. Hal ini memberikan gambaran yang lebih rinci terkait kerentanan keamanan yang ditemukan pada website SIAMIK.
3. Celah keamanan yang telah teridentifikasi pada website SIAMIK dapat dihindari melalui penyediaan laporan hasil dan rekomendasi perbaikan yang sesuai dengan analisis yang telah disampaikan sebelumnya. Hal ini akan

memungkinkan tim pengembang untuk memahami dengan jelas temuan keamanan yang ditemukan serta menerapkan langkah-langkah perbaikan yang diperlukan guna mengatasi kerentanan tersebut.

5.2 Saran

Dalam konteks pengembangan lebih lanjut, disarankan agar penelitian selanjutnya fokus pada pengujian celah keamanan yang lebih mendalam terhadap website SIAMIK. Hal ini penting untuk mengidentifikasi dan mengeksplorasi kemungkinan kelemahan yang mungkin tidak terdeteksi. Adapun saran yang sangat diinginkan untuk penelitian berikutnya adalah menggunakan OWASP Testing Framework, penggunaan kerangka kerja ini diharapkan dapat memberikan struktur yang lebih terorganisir dan komprehensif dalam menemukan berbagai celah keamanan yang lebih rinci dan terperinci pada sistem yang diuji. OWASP Testing Framework terkenal karena pendekatannya yang komprehensif dan dapat memberikan informasi yang lebih rinci terkait kerentanan keamanan yang mungkin ada dalam suatu sistem. Oleh karena itu, penggunaan kerangka kerja ini diharapkan dapat memberikan kontribusi yang signifikan dalam mengidentifikasi serta memperbaiki kelemahan keamanan yang ada pada website SIAMIK maupun sistem serupa di masa mendatang.