BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan pengujian keamanan menggunakan metode *National Institute of Standards and Technology* (NIST) SP 800-115 pada Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta, ditemukan beberapa kerentanan yang dapat menjadi acuan evaluasi tingkat keamanan sistem tersebut.

Pengujian dengan *Nikto Scanner* mengungkap beberapa kelemahan seperti kebocoran informasi melalui *ETags header*, *file robots.txt*, serta *cookies* PHPSESSID tanpa *secure* dan *httponly flags*. *Helium Security* menemukan lima kerentanan risiko sedang, empat risiko rendah, dan enam kerentanan informatif. Masalah utama termasuk ketidakhadiran token Anti-CSRF, kebijakan *Content-Security-Policy* (CSP) yang tidak memadai, dan *Sub Resource Integrity* (SRI) yang tidak diterapkan. Beberapa konfigurasi *cookie* tidak aman. ZAP (Zed Attack Proxy) mengidentifikasi SQL *Injection* pada *endpoint /proseslogin.php*, serta masalah CSP dan *library JavaScript* yang rentan.

Secara keseluruhan, dari 10 kategori OWASP Top 10, ditemukan kerentanan pada enam kategori dengan presentase 60%, yaitu A01:2021 – *Broken Access Control* (16.67%), A02:2021 – *Cryptographic Failures* (4.17%), A03:2021 – *Injection* (4.17%), A05:2021 – *Security Misconfiguration* (66.67%), dan A06:2021 – *Vulnerable and Outdated Components* (4.17%). Kategori A04, A07, A08, A09, dan A10 tidak ditemukan kerentanannya. Penelitian ini juga menunjukkan bahwa SICAMA memerlukan langkah-langkah mitigasi seperti penerapan token Anti-CSRF, pembaruan library yang rentan, penambahan *header* keamanan seperti *X-Frame-Options*, dan memperketat kebijakan CSP. Implementasi rekomendasi ini diharapkan dapat meningkatkan keamanan SICAMA Universitas Jenderal Achmad Yani Yogyakarta, memastikan

perlindungan yang lebih baik terhadap ancaman keamanan siber, dan meningkatkan keandalan layanan informasi kepada penggunanya.

5.2 SARAN

Berdasarkan hasil penelitian dan rekomendasi OWASP Top 10, berikut adalah saran untuk meningkatkan keamanan situs web SICAMA Universitas Jenderal Achmad Yani Yogyakarta:

1. Tambahkan *header X-Frame-Options* dengan nilai *DENY* atau *SAMEORIGIN* untuk mencegah *clickjacking* dan perketat *Content-Security-Policy* (CSP) dengan menghindari penggunaan *'unsafe-inline'* serta menggunakan *hash* untuk *script inline* guna mencegah XSS. Pastikan semua *cookies*, terutama PHPSESSID, memiliki *secure* dan *httponly flags* serta implementasikan atribut *SameSite* pada *cookies* untuk melindungi dari *sniffing,* XSS, dan CSRF.
2. Hindari atau konfigurasi ulang *ETags* agar tidak membocorkan informasi *inode* dan file *robots.txt* untuk memastikan tidak ada informasi yang terekspos. Gunakan sertifikat *wildcard *.unjaya.ac.id* hanya pada subdomain tepercaya dan dikelola dengan aman. Rutin memperbarui semua *library* dan *framework* yang digunakan untuk menghindari kerentanan yang diketahui.
3. Implementasikan token Anti-CSRF pada semua formulir penting dan terapkan validasi input ketat untuk semua parameter pengguna yang dimasukkan ke dalam *query* SQL guna mencegah CSRF dan injeksi SQL.

Dengan menerapkan saran-saran di atas berdasarkan rekomendasi OWASP Top 10, diharapkan situs web SICAMA Universitas Jenderal Achmad Yani Yogyakarta dapat meningkatkan keamanan dan melindungi data serta privasi pengguna dengan lebih baik. Langkah-langkah ini akan membantu dalam mencegah berbagai jenis serangan siber dan memastikan keandalan serta integritas sistem informasi yang digunakan.