BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dalam *penetration testing*, dapat dikesimpulkan sebagai berikut.

1. Kegiatan *penetration testing* yang telah dilakukan dalam mencari celah kerentanan sistem *website* menggunakan metode *Open Web Application Security Project* (OWASP) Top 10 2021 dengan tahapan Pengumpulan Informasi (*Information Gathering*), Pemindaian (*Scanning and Vulnerability Assessment*), Eksploitasi (*Exploitation*), dan Pelaporan (*Reporting*) pada *domain* target yaitu mhs.amikom.ac.id telah berhasil dalam menghasilkan daftar kerentanan sehingga dapat dilakukan proses evaluasi untuk memperbaiki celah keamanan yang telah ditemukan.
2. Setelah dilakukan pengujian kerentanan dan analisis dari hasil *penetration testing*, *domain* target memiliki 11 kerentanan yang dapat dieksploitasi. Dari 11 kerentanan tersebut ada 1 kerentanan masuk kategori tingkat risiko sedang (*medium*), 7 kerentanan masuk kategori tingkat risiko rendah (*low*), dan 3 kerentanan masuk kategori tingkat risiko informasi (*informational*). Adapun kerenanan tersebut ialah *Directory listings*, *Clickjacking: X-Frame-Options header*, *Cookie without SameSite Attribute*, *Cookie with missing, insconsistent or contradictory properties*, *Session cookie scoped to parent domain*, *Content Security Policy* (CSP) *not implemented*, *Cookie without Secure flag set*, HTTP *Strict Transport Security* (HSTS) *not implemented*, TSL/SSL *certificate about to expire*, *Cross-Domain JavaScript Source File Inclusion*, dan *Loosely Scoped Cookie*.

5.2 Saran

Berdasarkan kesimpulan dan analisis yang telah dilakukan, terdapat saran yang diberikan sebagai berikut.

1. Melakukan kegiatan *penetration testing* dengan menggunakan metode dan alat (*tools*) yang berbeda sebagai acuan kerentanan sistem yang lebih akurat.

2. Menyesuaikan dan menerapkan rekomendasi perbaikan yang telah diberikan pada penelitian ini untuk menutup kerentanan sistem *website*.