BAB V
PENUTUP

5.1 Kesimpulan

Dari hasil temuan dan pengujian yang dilakukan pada website SIAKAD Mahasiswa UPNVJ, didapatkan kesimpulan sebagai berikut:

1. Pengujian penetrasi terhadap Website SIAKAD Mahasiswa UPNVJ berhasil mengungkap tujuh kerentanan yang telah divalidasi melalui pengujian manual. Kerentanan tersebut meliputi stored XSS pada fitur Konsultasi Dikjar dan Dosen PA, Insecure Direct Object Reference (IDOR) pada fitur Foto Profil dan SPC Billing, tidak adanya mekanisme rate limiting pada fitur Konsultasi Dikjar dan Dosen PA, serta reflected XSS pada fitur Materi Ajar.
2. Berikut ini merupakan rincian risiko dari tujuh kerentanan yang berhasil diidentifikasi pada *website* SIAKAD Mahasiswa UPNVJ: Stored XSS pada fitur Konsultasi Dikjar (risiko: Medium, severity: 4.6), stored XSS pada fitur Dosen PA (risiko: Medium, severity: 4.6), Insecure Direct Object Reference (IDOR) pada fitur Foto Profil (risiko: Medium, severity: 4.3), IDOR pada fitur SPC Billing (risiko: Medium, severity: 4.3), tidak adanya mekanisme rate limit pada fitur Konsultasi Dikjar (risiko: Medium, severity: 4.3), tidak adanya rate limit pada fitur Dosen PA (risiko: Medium, severity: 4.3), serta reflected XSS pada fitur Materi Ajar (risiko: Low, severity: 3.5).
3. Setiap kerentanan dapat diperbaiki dengan langkah-langkah berikut:
    1. Stored XSS pada Konsultasi Dikjar dan Stored XSS pada Dosen PA: Lakukan validasi serta sanitasi input secara menyeluruh untuk mencegah eksekusi skrip berbahaya. Pastikan bahwa semua data yang ditampilkan di halaman web tidak dapat dieksekusi sebagai kode oleh browser.
    2. *Insecure Direct Object Reference* (IDOR) pada Foto Profil: Terapkan kontrol akses yang sesuai agar setiap pengguna hanya dapat melihat foto profilnya sendiri dan tidak memiliki akses ke foto profil mahasiswa lain.
    3. *Insecure Direct Object Reference* (IDOR) pada SPC Billing: Implementasikan validasi akses berbasis sesi atau token untuk memastikan bahwa hanya pemilik

akun yang dapat melihat informasi tagihan UKT mereka sendiri. Hindari penggunaan ID langsung dalam parameter yang dapat dimanipulasi.

4. No Rate Limit pada Konsultasi Dikjar dan Dosen PA: Terapkan mekanisme pembatasan jumlah permintaan (*rate limiting*) untuk mengontrol jumlah pesan yang dapat dikirim dalam periode tertentu. Tambahkan CAPTCHA atau sistem autentikasi tambahan untuk mencegah spam dari bot.
5. Reflected XSS pada Materi Ajar: Gunakan Content Security Policy (CSP) untuk membatasi sumber skrip yang dapat dijalankan. Selain itu, lakukan encoding dan escaping pada setiap input yang ditampilkan guna mencegah serangan XSS.

5.2 Saran

Saran yang dapat diberikan penulis antara lain:

1. Pada tahap *discovery*, gunakan tools *vulnerability assessment* yang lebih sesuai dengan karakteristik *website* SIAKAD UPNVJ agar dapat mengidentifikasi kerentanan dengan baik.
2. Untuk penelitian selanjutnya, disarankan menggunakan variasi tools yang lebih beragam agar dapat mengidentifikasi lebih banyak kerentanan dan memperoleh hasil analisis keamanan yang lebih komprehensif.