BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah dilakukannya pengujian penetrasi pada server Universitas PQR, dapat disimpulkan beberapa hal berikut.

1. Pengujian penetrasi terhadap keamanan data pribadi mahasiswa pada server Universitas PQR dilakukan dengan melalui 4 fase pengujian, yaitu fase *planning*, fase *discovery*, fase *attack*, dan fase *reporting*.
2. Kerentanan yang ditemukan sebagai hasil dari pengujian penetrasi adalah ditemukannya 13 kerentanan yang dapat dieksploitasi dengan rincian 2 kerentanan termasuk kategori *critical yaitu Default Credentials* dan *PHP Unsupported Version Detection*, 3 kerentanan termasuk kategori *high yaitu SSL Version 2 and 3 Protocol Detection, PHP < 7.3.24 Multiple Vulnerabilities, SSL Medium Strength Cipher Suites Supported (SWEET32),* 8 kerentanan termasuk kategori *medium* yaitu *SSL Certificate Cannot Be Trusted, SSL Self-Signed Certificate, TLS Version 1.0 Protocol Detection, PHPinfo() Information Disclosure, Unencrypted Password Form, HTTP TRACE / TRACK Methods Allowed, SSL Certificate Expiry, SSL RC4 Cipher Suites Supported (Bar Mitzvah),* dan 1 kerentanan adalah *false positive yaitu PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability*.
3. Kerentanan-kerentanan yang ditemukan dapat dimitigasi dengan cara yang berbeda-beda untuk setiap kerentanan. Rekomendasi untuk kerentanan *Default Credential* yaitu *username* dan *password* yang ada seharusnya diubah menjadi rumit seperti melakukan kombinasi dari huruf kapital, huruf biasa, angka, dan *symbol* serta mengatur banyaknya *character* yang lebih dari 8. Rekomendasi untuk kerentanan *PHP Unsupported Version Detection* dan *PHP <*

7.3.24 Multiple Vulnerabilities yaitu melakukan pembaharuan pada PHP menjadi versi PHP terbaru yang didukung. Rekomendasi untuk kerentanan *SSL Version 2 and 3 Protocol Detection* yaitu menonaktifkan protokol SSL. Rekomendasi untuk kerentanan *SSL Medium Strength Cipher Suites Supported (SWEET32)* yaitu melakukan konfigurasi ulang terhadap aplikasi yang terpengaruh serta menghindari penggunaan cipher berkekuatan sedang. Rekomendasi untuk kerentanan *SSL Certificate Cannot Be Trusted*, *SSL Self-Signed Certificate*, serta *SSL Certificate Expiry* yaitu melakukan pembaharuan terhadap sertifikat SSL. Rekomendasi untuk kerentanan *TLS Version 1.0 Protocol Detection* yaitu menonaktifkan protokol TLS versi 1.0 dan versi 1.1 dan mengaktifkan protokol TLS versi 1.2 dan versi 1.3. Rekomendasi untuk kerentanan *PHPinfo() Information Disclosure* yaitu menghapus file info.php pada sistem. Rekomendasi untuk kerentanan *Unencrypted Password Form* yaitu enggunakan protokol enkripsi yang terbaru dan paling aman, yaitu TLS versi 1.2 dan versi 1.3 Protokol versi lama seperti SSL versi 1, SSL versi 2, TLS versi 1.0, TLS versi 1.1, dan sandi lemah (< 128 bit) juga harus dinonaktifkan Rekomendasi untuk kerentanan *HTTP TRACE / TRACK Methods Allowed* yaitu menonaktifkan metode Trace pada HTTP. Rekomendasi untuk kerentanan *SSL RC4 Cipher Suites Supported (Bar Mitzvah)* yaitu melakukan konfigurasi ulang terhadap aplikasi yang terpengaruh serta menghindari penggunaan cipher RC4. Peneliti hanya memberikan rekomendasi yang dapat dilakukan untuk memitigasi kerentanan yang ditemukan. Penerapan dari rekomendasi akan diserahkan sepenuhnya kepada pihak terkait, yaitu Universitas PQR.

5.2 Saran

Berdasarkan pada pembahasan dan kesimpulan yang telah dijelaskan, maka Penulis memberikan beberapa saran yaitu sebagai berikut.

1. Pengujian selanjutnya dapat dilakukan dengan menambahkan metode *threat hunting* pada pengujan supaya dapat menemukan kerentanan secara lebih mendalam.
2. Pengujian ulang pada sistem sebaiknya dilakukan kembali jika sistem telah berhasil diremediasi oleh Universitas PQR.