BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

Setelah dilakukannya pengujian menggunakan metode *penetration testing* terhadap *website gapura.umn.ac.id* dan *academic.umn.ac.id*, tingkat keamanan dari *website gapura.umn.ac.id* dan *academic.umn.ac.id* sudah tergolong cukup baik, dikarenakan dari tiga belas kerentanan yang ditemukan melalui *tools vulnerability scanner*, hanya dua kerentanan yang sifatnya valid. Hanya saja, kerentanan yang ditemukan ketika diukur menggunakan indikator CVSS v4.0, keduanya mendapatkan *score* 9,2 atau mencapai *level critical* yang menandakan kerentanan yang ditemukan cukup parah. Kedua kerentanan tersebut adalah *Vulnerabilities found for server-side software* dan *Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*. Kedua kerentanan yang ditemukan sama - sama membocorkan bahasa pemrograman dan juga *framework* yang dipakainya. Hal ini dapat berdampak buruk dikarenakan bahasa pemrograman dan *framework* yang dipakai memiliki *vulnerability* yang dapat diakses secara umum di internet, dan memudahkan orang jahat untuk mengeksploitasi hal tersebut. Solusi dari kerentanan *Vulnerabilities found for server-side software* adalah dengan melakukan pembaharuan versi untuk bahasa pemrograman dan *framework* yang dipakai, sementara itu untuk kerentanan *Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)* dapat diatasi dengan men-*disable* atau me-*remove header X-Powered-By*.

5.2 Saran

Berdasarkan kesimpulan dan hasil dari penelitian yang telah dilakukan, berikut ini merupakan saran yang dapat diberikan untuk penelitian selanjutnya.

1. Menggunakan *tools - tools* yang memiliki fitur lebih banyak dan tidak bersifat *open source*, dikarenakan pada penelitian ini hanya menggunakan *tools* yang bersifat *open source* dan gratis, sehingga mungkin saja jika menggunakan *tools* yang berbayar, akan ditemukan kerentanan lainnya.

2. Menggunakan *tools* untuk mengotomisasi tahap eksploitasi atau menggunakan metode - metode penetrasi yang lebih *advanced*, hal ini bertujuan untuk menemukan lebih banyak peluang penetrasi dalam mengeksploitasi *website*.
3. Mengggunakan *deep reinforcement learning* untuk membuat sebuah *tools intelligent penetration testing* yang dapat mengotomisasi kegiatan *penetration testing* sehingga dapat dilakukan secara rutin, karena celah keamanan yang bersifat dinamis dan bisa bertambah atau berkurang dalam periode waktu tertentu, sehingga harus rutin dijalankan *penetration testing*.