BAB 5

PENUTUP

5.1 Kesimpulan

1. Penulis megetahui kondisi serta tingkat keamanan sistem aplikasi web DVWA dengan cara melakukan kegiatan *penetration testing* terhadap aplikasi web tersebut dengan menggnakan metode *Zero Entry Hacking* (ZEH).
2. Celah keamanan yang dilakukan eksploit oleh penulis antara lain adalah *cross-site scripting* (XSS), *command injection, file inclusion, file upload, brute force attack,* dan *SQL injection*.
3. *Cross-Site Scripting* memiliki solusi mematikan HTTP TRACE pada web server, *command Injection* memiliki solusi untuk memvalidasi *whitelist*, *File injection* dapat dicegah dengan menghindari meneruskan input yang dikirimkan pengguna ke API filesystem/framework apa pun, pencegahan *File Upload* dapat dilakukan dengan jangan pernah menerima nama file dan ekstensinya secara langsung tanpa memiliki filter daftar yang diizinkan, *Brute Force Attack* dapat dicegah dengan memindai web agar dapat mengetahui apakah ada kerentanan, dan *SQL Injection* memiliki solusi kerentanan dengan melakukan validasi pada input.

5.2 Saran

Saran untuk penelitian yang akan datang yaitu perlu digunakannya lebih banyak *tools* lainnya dalam setiap prosesnya, melakukan lebih banyak jenis eksploitasi terhadap kerentanan yang ditemukan, dan melakukan pengaturan keamanan yang lebih tinggi terhadap aplikasi web *Damn Vulnerable Web Application* (DVWA),