

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan dan Saran

5.1.1 Kesimpulan

Setelah melakukan penelitian *penetration testing* terhadap celah keamanan *database website* menggunakan serangan *SQL Injection* menggunakan *tools sqlmap* diperoleh kesimpulan yaitu:

1. *Vulnerability detection* menggunakan *tools nmap* dan *nikto* mempunyai durasi kecepatan yang berbeda pada ketiga target. Perbedaan tersebut diperoleh dari hasil durasi *scanning vulnerability detection* pada target pertama selisih sekitar 7 menit, sedangkan pada target kedua selisih sekitar 8 menit dan pada target ketiga selisih sekitar 88 menit. Hal ini menunjukkan *tools nmap* lebih cepat mendeteksi kerentanan daripada *nikto*, namun *nikto* memberikan hasil deteksi yang lebih detail daripada *nmap*.
2. *Penetration testing* terhadap 3 target yaitu target pertama yang mempunyai keamanan *SSL*, target kedua dan ketiga yang tidak mempunyai keamanan *SSL* dengan serangan *SQL Injection*. Pada tahapan *vulnerability detection* menggunakan *tools nmap* dan *nikto* ditemukan kerentanan pada ketiga target. Target pertama mempunyai kerentanan terhadap serangan *SQL Injection*, *Clickjacking*, dan *XSS*. Selain itu pada target kedua mempunyai kerentanan yang sama dengan target pertama. Dan target ketiga tidak mempunyai kerentanan *SQL Injection* tetapi rentan terhadap serangan *Clickjacking* dan *XSS*.
3. Pada saat melakukan *penetration testing* menggunakan *tools sqlmap* ditemukan *database* pada target pertama yang meskipun mempunyai keamanan *SSL* namun tidak mempunyai *web application firewall*, maka target pertama dapat dengan mudah di eksploitasi dengan serangan *SQL Injection*. Namun pada target kedua dan ketiga saat melakukan serangan *SQL Injection* menggunakan *tools sqlmap* hasilnya tidak menemukan *database* yang

meskipun tidak mempunyai keamanan *SSL* tetapi mempunyai *web application firewall* sehingga target kedua dan ketiga terlindungi dari serangan *SQL Injection*.

4. Hasil dari durasi *penetration testing* menggunakan *tools sqlmap* dengan *stopwatch* menggunakan serangan *SQL Injection* terhadap kerentanan yang terdapat pada target pertama, kedua, dan ketiga mempunyai perbedaan durasi. Hasil durasi tersebut menjadi perbandingan terhadap ketiga target yang berhasil dan tidak berhasil saat *penetration testing* sedang berjalan hingga selesai. Dari hasil durasi pada target pertama menghasilkan durasi 37 menit yang cukup lama, disebabkan karena *tools sqlmap* berhasil mengeksploitasi kerentanan *SQL Injection*. Sedangkan pada target kedua dan ketiga menghasilkan durasi yang cepat hanya selisih 2 menit, hal ini disebabkan karena kegagalan dalam mengeksploitasi kerentanan *SQL Injection* dengan *tools sqlmap*.

5.1.2 Saran

Berdasarkan analisis dan kesimpulan yang telah diperoleh, maka saran yang dapat diberikan yaitu:

1. Perlunya melakukan *vulnerability detection* menggunakan *tools* selain *nmap* dan *nikto* untuk menemukan *tools* yang dapat dengan cepat mendeteksi kerentanan dan memberikan hasil yang lebih detail.
2. Perlunya memasang dan meningkatkan keamanan *website* dalam perlindungan data pada *database website*. Selain menggunakan *SSL* yang belum tentu aman dari serangan *SQL Injection* tetapi dibutuhkan juga dibutuhkan teknologi keamanan website lain seperti *WAF* yang mampu mencegah dan memblokir serangan *SQL Injection*.
3. Perlunya menggunakan *tools* selain *sqlmap* seperti *havij* dalam melakukan *penetration testing* untuk mengetahui kecepatan durasinya dalam mengeksploitasi kerentanan yang terdapat pada website target.