

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah melakukan penelitian pengujian keamanan sistem website dengan Teknik penetration testing dengan metode Open Web Application Security Project (OWASP) pada studi kasus sub domain upnjatim.ac.id, didapatkan sebuah hasil eksploitasi dan celah keamanan yang memungkinkan dapat dimanfaatkan pihak yang tidak bertanggung jawab. Penelitian yang bertujuan untuk mengetahui dan menguji kelemahan keamanan yang dimiliki oleh website pada studi kasus. Diperoleh beberapa kesimpulan yang uraikan sebagai berikut.

1. Kelemahan keamanan pada kelima website studi kasus dapat dicari menggunakan tools yang bernama Nessus, OWASP ZAP, dan Script NMAP Vulscan. Didapatkan hasil *vulnerability* seperti pada tahapan *Vulnerability Testing*.
2. Website pada studi kasus memiliki celah keamanan terkait pada daftar OWASP TOP 10. Yang mana ditemukan melalui tahapan *vulnerability testing*.
3. Pengujian *Penetration Testing* terhadap kelemahan keamanan website berdasarkan CIA TRIAD yang telah ditemukan dapat dilakukan dengan mengacu pada tahapan *vulnerability testing* menggunakan alat BurpSuite. Namun, hasil *penetrasi testing* tidak mendapatkan hal yang bersifat mengganggu CIA TRIAD website.
4. Kelemahan website yang ditemukan dapat dicegah dengan memberikan hasil *reporting* dan rekomendasi sesuai dengan yang telah dijelaskan.

5.2. Saran

Terdapat beberapa saran terkait penelitian selanjutnya, yang akan diuraikan sebagai berikut.

1. Penelitian dengan teknik Penetration Testing akan lebih mudah dijalani, jika mengerti struktur pemrograman dengan Bahasa PHP, HTML, JavaScript, dan paham SQL.
2. Penelitian dengan topik ini alangkah baik nya ditambahkan alur untuk eksploitasi yang jelas.