BAB V
PENUTUP

5.1 Simpulan

1. Identifikasi kerentanan pada *website* Pemerintah ABC dilakukan berdasarkan metode *OWASP Top 10* dan hasil *scanning* yang dilakukan pada tahap *discovery*. Dimana kerentanan berdasarkan *OWASP Top 10* memiliki 10 kategori dan kerentanan yang ditemukan dari hasil *scanning OWASP ZAP* terdapat satu kerentanan yaitu *clickjacking*.
2. Hasil pengujian penetrasi terhadap *website* pemerintah ABC menunjukkan bahwa terdapat 3 kerentanan yang ditemukan dari *website* tersebut 2 diantaranya merupakan kategori *OWASP Top* 10 yaitu *broken access control*, *security misconfiguration*, dan satu kerentanan dieksploitasi berdasarkan hasil *scanning* menggunakan *OWASP ZAP* yaitu *clickjacking*.
3. Jenis kerentanan yang ditemukan pada *website* target:
   a. *Broken Access Control*

      Saat melakukan scanning dengan *tools Dirb* ditemukan *file server-status* yang berisi informasi sensitif mengenai server, sistem operasi, dan lain-lain. File tersebut dapat diakses tanpa harus melakukan validasi identitas terlebih dahulu, oleh karena itu dapat dijadikan celah oleh penyerang untuk mengenal *environment website* target.

   b. *Security Misconfiguration*

      Kerentanan pada kategori ini ditemukan dengan melakukan proses *scannin*g pada *port* yang terbuka dan konfigurasinya. Hasil menunjukkan SSLV3 bersifat *enabled.* SSLV3 tidak digunakan lagi karena rusak dan seharusnya bersifat *disabled* untuk keamanan *port* SSL.

   c. *Clickjacking*

      Celah keamanan *Clickjacking* tidak termasuk dalam daftar kategori *OWASP TOP* 10, namun kerentanan ini ditemukan saat melakukan scanning terhadap *website* target menggunakan OWAPS ZAP. Setelah dilakukan percobaan untuk membuktikan celah keamanan ini,

ditemukan hasil bahwa *website* target memiliki celah keamanan untuk melakukan *clickjacking*.

4. Versi *CKAN* yang digunakan yaitu versi 2.7.4 dimana versi ini sudah mengalami perbaikan, saat ini sudah hadir versi *CKAN* 2.9.5 dengan berbagai perubahan minor dan major, juga *bugfixes*.

5.2 Saran

Berdasarkan hasil pengujian yang dilakukan pada *website* target terdapat beberapa saran yang dapat digunakan untuk penelitian selanjutnya maupun sistem target:

1. Pemilik *website* melakukan update versi *CKAN* ke yang terbaru karena telah banyak perbaikan yang dilakukan mulai dari perubahan bersifat minor dan major, hingga *bugfixes* berdasarkan dokumentasi *CKAN*.
2. Hasil pengujian menunujukkan adanya beberapa celah keamanan yang terdapat pada target, hal ini menandakan perlu dilakukan pengujian celah keamanan secara berkala dan lebih mendalam terhadap *website* target demi mencari kelemahan yang mungkin tidak disadari.