BAB V
PENUTUP

5.1 Kesimpulan

Setelah dilakukan penelitian terhadap keamanan *website* sistem pembelajaran *online* dengan metode ISSAF sehingga dapat disimpulkan sebagai berikut.

1. Framework ISSAF merupakan metodologi penetration testing yang sangat terstruktur, dimulai dari *tahap Information Gathering, Network Mapping, Vulnerability Scanning, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Files, Maintaining Access, hingga Covering the Tracks*.
2. Berdasarkan sembilan tahapan tersebut diperoleh hasil bahwa *website* demoxxxxx.xxxxx.ac.id tidak aman dari serangan seperti *Brute-force Attack*, *Cross-Site Request Forgery* (CSRF) *Attack*, *Session Hijacking* melalui *Cookie*, maupun *IDOR (Insecure Direct Object Reference).*
3. Rekomendasi yang dapat diberikan adalah *limit login attempt* untuk mencegah *Brute-force Attack*, penerapan *CSRF token* pada *hidden field* untuk mencegah *CSRF Attack,* penerapan *hide parameter URL* atau *Indirect Reference Map* untuk mencegah celah pada *IDOR (Insecure Direct Object Reference)*, dan penerapan *Regenerate Cookie* pada setiap *request* untuk mencegah *Session Hijacking* melalui *Cookie*.
4. Kerentanan yang ditemukan merupakan kerentanan *critical-medium* maka dapat disimpulkan *website* demoxxxxx.xxxxx.ac.id tidak cukup aman.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, diperlukannya suatu pengujian dan pengembangan penelitian lebih lanjut. Saran untuk penelitian ini ialah sebagai berikut.

1. Pengujian *framework penetration testing* menggunakan metode lainnya agar dapat digunakan sebagai pelengkap hasil pengujian, misal *OSSTMM*

untuk keamanan dari sisi *hardware* dengan menghitung *score protection* pada sebuah *website*.

2. Dilakukan pengujian secara berkala, karena *website* tentunya akan terus berkembang dengan berbagai fitur baru, sehingga kemungkinan terdapat celah baru akan selalu ada. Pengujian *penetration testing* secara berkala juga harus diiringi dengan *tools* yang *up-to-date* juga.