ABSTRAK

PENUTUPAN CELAH KEAMANAN MENGGUNAKAN METODE HARDENING

(STUDI KASUS: *CLOUDFRI*)

Oleh:

MUHAMMAD FARIZQI SETIAWAN

1202170314

Security Hardening merupakan metode yang ditujukan untuk meningkatkan keamanan suatu sistem agar suatu sistem tidak mudah dieksploitasi atau diserang oleh pihak yang tidak bertanggung jawab. Penelitian ini bertujuan untuk melakukan identifikasi kerentanan yang ada pada aplikasi berbasis *website* tap2go.cloudfri sekaligus menganalisis dan melakukan prosedur *hardening* pada *website.* Penelitian ini menggunakan metode *Security Hardening* sebagai panduan penelitian. Saat menggunakan metode *security hardening* dilakukan juga pengujian *vulnerability scanning* dan *penetration testing.* Hasil penelitian ini berupa analisis *vulnerability scanning* dan *penetration testing*. Kerentanan yang ditemukan yaitu kerentanan terhadap serangan DDoS, komunikasi yang tidak terenkripsi, tidak terpasangnya *Anti-ClickJacking* dan penggunaan SSl/TLS yang telah usang. *Penetration testing* yang dilakukan yaitu simulasi penyerangan DDos, Drupalgeddon, *Interception* dan SQL *Ijection.* Hasil *penetration testing* didapati sistem tersebut telah aman dari serangan SQL *injection* karena sudah terdapatnya *firewall* untuk menahan serangan tersebut sebaliknya untuk jenis serangan lainnya sistem tersebut belum aman dan perlu dilakukan konfigurasi ulang pada *web server* untuk meminialisir celah keamanan yang terdapat pada aplikasi berbasis *website* tap2go.cloudfri.

Kata Kunci: ***Security Hardening***, ***Vulnerability***, ***Penetration Testing***.