BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Sistem *zero knowledge proof* ini telah berhasil diimplementasikan sebagai proses autentikasi dengan metode Guillou-Quisquater. *Zero Knowledge Proof* merupakan suatu metode autentikasi. Dengan metode ini, *server* dapat mengautentikasi *user* tanpa mengetahui *password* milik *user*. Sistem dibuat dengan bahasa pemrograman PHP dan *database* MySQL. Dari segi teknis, terdapat dua metode yang dapat digunakan untuk melakukan autentikasi, yaitu sertifikat beserta *key* dan *local storage*. Dengan metode sertifikat beserta *key*, *user* dapat *login* di perangkat yang berbeda-beda dengan cara mengunggah *file* sertifikat dan kunci privat miliknya, sedangkan metode *local storage* lebih cocok digunakan jika perangkat yang digunakan untuk *login* selalu sama, karena sertifikat dan kunci privat akan diambil dari *local storage browser* yang digunakan. Hal tersebut membuat metode *local storage* menjadi lebih praktis dibandingkan metode *key*. Berdasarkan uji coba yang telah dilakukan, kedua metode tersebut dapat mengautentikasi *user* dengan benar.

Dari segi keamanan, peneliti telah melakukan uji coba menggunakan skenario autentikasi OWASP. Percobaan-percobaan untuk *login* sebagai *unauthorized user* ataupun mengambil sertifikat dan kunci privat milik *user* seperti *sniffing* data *login*, *bypass* sistem autentikasi, memanfaatkan celah

keamanan pada fungsi *logout*, dan XSS untuk mengambil data *local storage* gagal dilakukan. Hasil *penetration testing* oleh pakar menunjukkan terdapat tiga *vulnerability* yang dianggap dapat menjadi ancaman bagi sistem ini. Ketiga *vulnerability* tersebut adalah *default error message*, *credentials send in clear text*, dan *sensitive data exposure*. Berdasarkan hasil estimasi risiko, masing-masing *vulnerability* berada pada risiko *medium*. *Vulnerability* yang menjadi prioritas untuk diperbaiki adalah *sensitive data exposure* karena penyerang bisa mendapatkan pengetahuan *username* yang terdaftar. Walaupun demikian, peretas masih harus memiliki sertifikat, kunci privat, dan *password* milik *user* agar bisa masuk ke dalam sistem.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, berikut adalah saran yang dapat digunakan untuk penelitian berikutnya.

1. Melakukan pengujian sistem autentikasi Guillou-Quisquater dari segi keamanan dan kecepatan dengan menggunakan dua bilangan prima untuk RSA *cryptosystem* yang lebih besar dari 9 bit.
2. Melakukan pengujian sistem autentikasi dari segi keamanan dengan menerapkan metode lainnya seperti Feige-Fiat-Shamir dan Schnorr.
3. Membuat aplikasi *mobile* iOS dan Android agar *user* dapat mengunduh sertifikat dan *key* saat melakukan registrasi dan mengubah *password* menggunakan *mobile device*.