BAB V
PENUTUP

5.1 Kesimpulan

Setelah melakukan pengujian serangan *Watering Hole* pada website KOPPERATI, maka dapat disimpulkan dengan hasil sebagai berikut:

1. Simulasi serangan *Watering Hole* pada website KOPPERATI menggunakan *cross site scripting* dilakukan dengan cara menginputkan script hook.js kedalam sistem dari website KOPPERATI, kemudian menjalankan *tool BeEF* untuk menjalankan *command exploitation* pada browser korban. Dari proses simulasi tersebut mendapatkan hasil bahwa website dengan karakteristik input data (halaman Ganti Pin website KOPPERATI) cenderung lebih rentan terhadap serangan *Watering Hole* dengan teknik *cross site scripting* yang menyebabkan data pengguna bocor dan disalah gunakan oleh penyerang.
2. Serangan *Watering Hole* dapat dianalisis dengan melakukan simulasi pengujian teknik serangan yang ada dalam *Watering Hole* berupa *cross site scripting* pada website KOPPERATI. Hasil yang didapatkan dari pengujian serangan *Watering Hole* pada website KOPPERATI dengan teknik *XSS* berupa, pelaku akan menginputkan script (hook.js) kedalam celah dari *sanitize input* yang ada pada halaman Ganti Pin dari website, ketika korban mengakses halaman tersebut, maka secara otomatis script akan mengirimkan respon pada tools yang digunakan oleh pelaku (*BeEF*) untuk menjalankan *kit exploitasi* pada browser dari korban dengan tujuan mendapatkan data penting atau sensitif seperti akun google

5.2 Saran

Adapun saran yang penulis dapat sampaikan untuk penelitian lebih lanjut tentang pengujian serangan *Watering Hole* pada website KOPPERATI berupa :

1. Mengembangkan lebih lanjut tentang *script* dan *syntax* yang digunakan untuk melakukan pengujian serangan *Watering Hole*.
2. Melakukan penelitian lebih mendalam tentang data yang didapatkan dari proses pengujian serangan *Watering Hole*.
3. Mengembangkan lebih lanjut tentang pengujian serangan *watering hole* dengan teknik lainnya.