BAB 5 PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis, didapatkan informasi bahwa *Cross Site Scripting* (XSS) yang ditemukan pada *website* sebagai berikut :

- Bahaya *Cross Site Scripting* (XSS) yang ditemukan biasanya terjadi dikarenakan tidak adanya atau kurang lengkapnya *filter* yang diterapkan dalam *input user* sehingga seorang *attacker* atau *hacker* bisa menggunakan payload untuk memunculkan bug XSS pada kolom *search* ataupun pada inputan lainya yang terhubung dengan database. Jika berhasil menginjeksi *payload* maka hacker tersebut bisa mengambil *session* dan *cookie* dari user yang *login* ataupun yang mengklik link yang mencurigakan, dimana nantinya dari link tersebut akan diarahkan kewebsite hacker ataupun website yang ingin dituju oleh target disaat itu juga *session* dan *cookie user* akan terambil dan tersave didalam *file hacker*. Dan jika *payload* ter*save* didalam database maka bug tersebut akan terus ada dan permanen selama *payload* tersebut tidak ditindak lanjuti dan tersimpan didatabase. Jika sudah terambil *cookie* dan session dari *user* maka *hacker* dapat melakukan *login* tanpa perlu autentikasi login kedalam website dengan cara mengganti *session* dan *cookie* miliknya menjadi punya korban dan dapat disalah gunakan lebih parah lagi dikarenakan informasi yang dipakai adalah informasi orang lain sehingga identitas *hacker* disini anonim.

- Lalu berdasarkan hasil pengujian dengan metacharacter dan *form validation* didapatkan bahwa dengan menggunakan metacharacter saja masih belum cukup dan perlu melakukan perulangan atau penginputan pola *payload* secara manual terus menerus dikarenakan setiap saat payload akan terbarui maka dengan begitu dapat ditambahkan *form validation* untuk menambah pengamanan dengan begitu inputan yang tidak terfilter oleh metacharacter akan masuk kedalam *filter form validation* untuk dicek kembali apakah format sudah benar atau belum dengan begitu pengamanan inputan akan maksimal dan berhasil mencegah *bug Cross Site Scripting* (XSS) yang tedapat pada website yang diracang sebelumnya.

5.2 Saran

Saran yang dapat diajukan untuk penelitian selanjutnya adalah diharapkan dapat menggunakan metode yang lain lagi seperti encoding. Kemudian menganalisis keefektifan tiap metode dalam mengatasi serangan ini. Lalu menguji metode ini menggunakan *framework* dan berbagai web browser yang berbeda - beda ataupun menggunakan database dalam membuat list pola yang nantinya digunakan didalam metacharacter.

Fuad Bawazir Alatas, 2021
PENINGKATAN KEAMANAN WEBSITE DARI SERANGAN CROSS SITE SCRIPTING (XSS) DENGAN METODE METACHARACTER DAN FORM VALIDATION
UPN Veteran Jakarta, Fakultas Ilmu Komputer, Informatika
[www.upnvj.ac.id - www.library.upnvj.ac.id - www.repository.upnvj.ac.id]