7. XSS (Reflected)

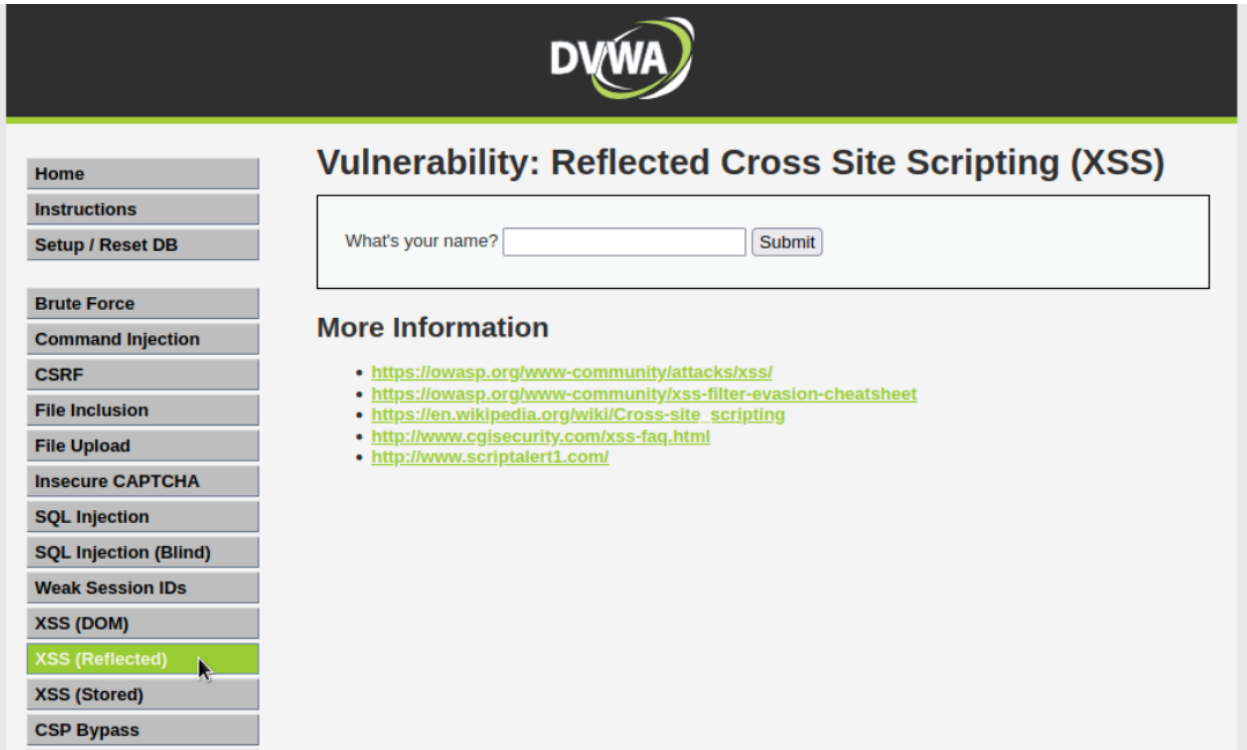
Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

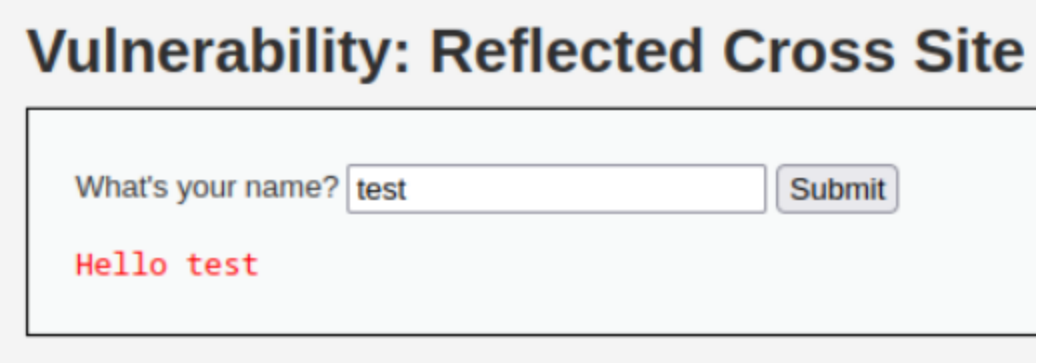
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ XSS/Cross-Site Scripting (Reflected)

Pada tampilan awal DVWA klik bagian XSS (Reflected)



Akan muncul field “What’s your name?”, coba isikan kata apa saja



Disini kata yang diinputkan akan diprint pada output dibawahnya

Dapat dilihat juga pada URL, akan ada kata yang diinputkan tadi

```
http://172.16.0.33:4280/vulnerabilities/xss_r/?name=test#
```

Pada level ini XSS menjalankan kode HTML tanpa filter, maka kode HTML yang dimasukkan dalam field nama akan dieksekusi juga oleh browser

Contoh saat field diisikan dengan perintah berikut

```
<h1 style="color:blue">Test</h1>
```

Akan menghasilkan output seperti berikut

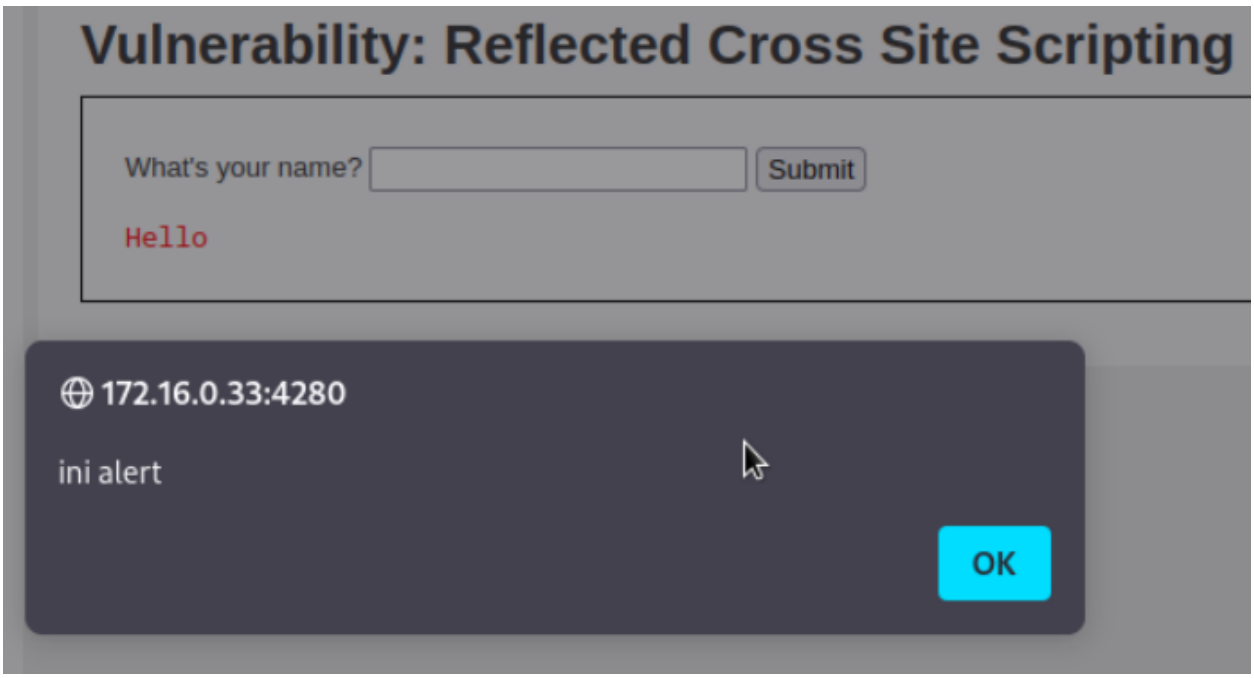
Tujuan dari XSS/Cross-Site Scripting biasanya untuk mendapatkan cookie dari browser korban. Session cookie yang didapat bisa digunakan penyerang untuk masuk ke akun

korban tanpa harus mengetahui user dan passwordnya, metode ini disebut Session Hijacking.

Untuk mendapatkan session cookie dari browser menggunakan XSS bisa dilakukan menggunakan fungsi `alert()` pada JavaScript. Untuk menjalankan JavaScript pada HTML gunakan element `<script>`. Perintah ini dapat disebut dengan payload

```
<script>alert('ini alert')</script>
```

Setelah submit browser akan menjalankan perintah JavaScript yang berisi alert dengan string “ini alert”

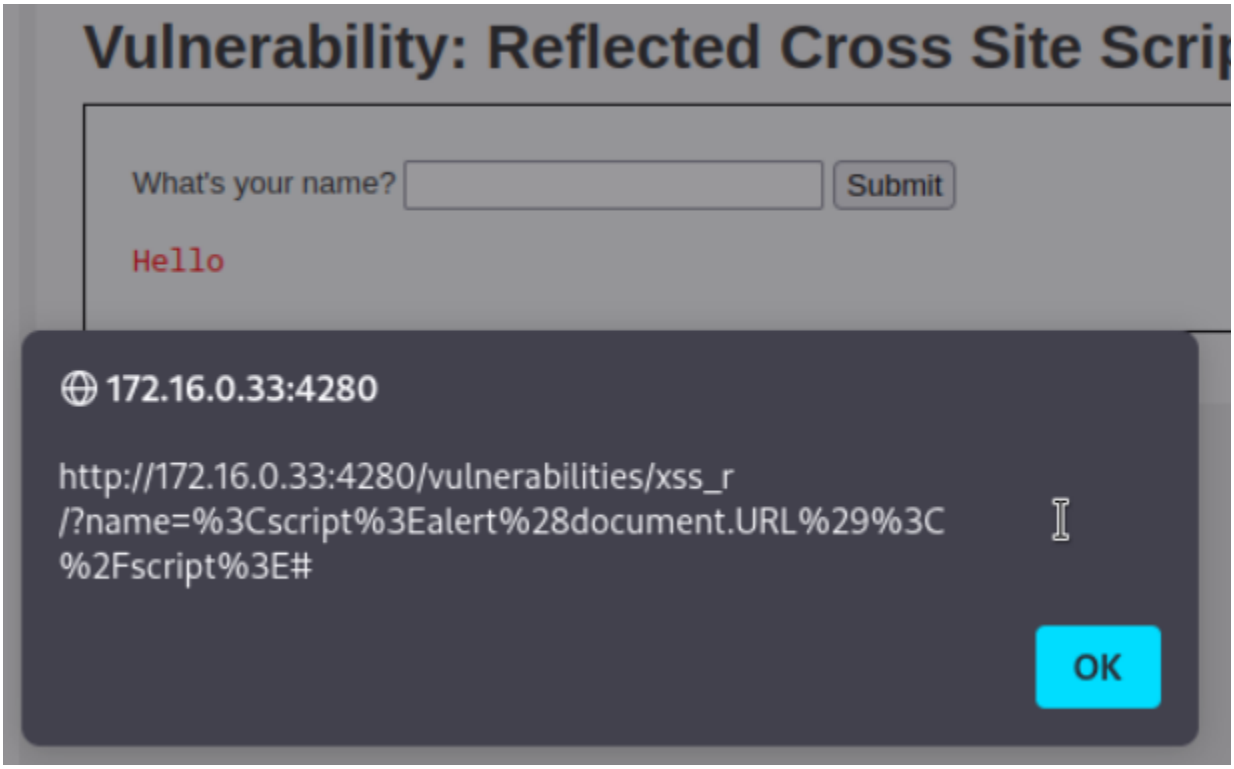


Tanda kurung pada fungsi `alert()` dapat dimasukkan string yang akan ditampilkan kembali ke browser, namun apakah ini juga berfungsi untuk menampilkan document object juga?

Coba lagi dengan memasukkan payload berikut

```
<script>alert(document.URL)</script>
```

Setelah klik submit, ternyata browser bisa mengembalikan URL dari halaman web



Ini berarti kemungkinan besar cookie dari website tersebut dapat diambil dengan metode yang sama

Gunakan payload berikut

```
<script>alert(document.cookie)</script>
```

Setelah klik submit, cookie dari browser tersebut dapat ditemukan

Note

- Metode ini hanya berfungsi pada website yang vulnerable
- Beberapa website memproteksi diri dari XSS dengan melakukan block pada berbagai payload XSS sehingga hasil payload tidak akan ditampilkan
- Payload pada artikel ini hanya payload dasar dan sudah pasti banyak diblock oleh website website
- Terkadang ada beberapa payload yang belum diblock oleh website sehingga masih ada celah untuk dilakukan XSS, banyak payload yang bisa dicoba untuk melakukan XSS seperti yang ada pada list ini
- XSS DOM dan Reflected hanya akan berjalan pada browser pelaku namun tidak pada browser pengguna lain, untuk membuat XSS yang dapat berjalan di browser pengguna lain gunakan script XSS yang tersimpan (stored)