16. XSS (Reflected)

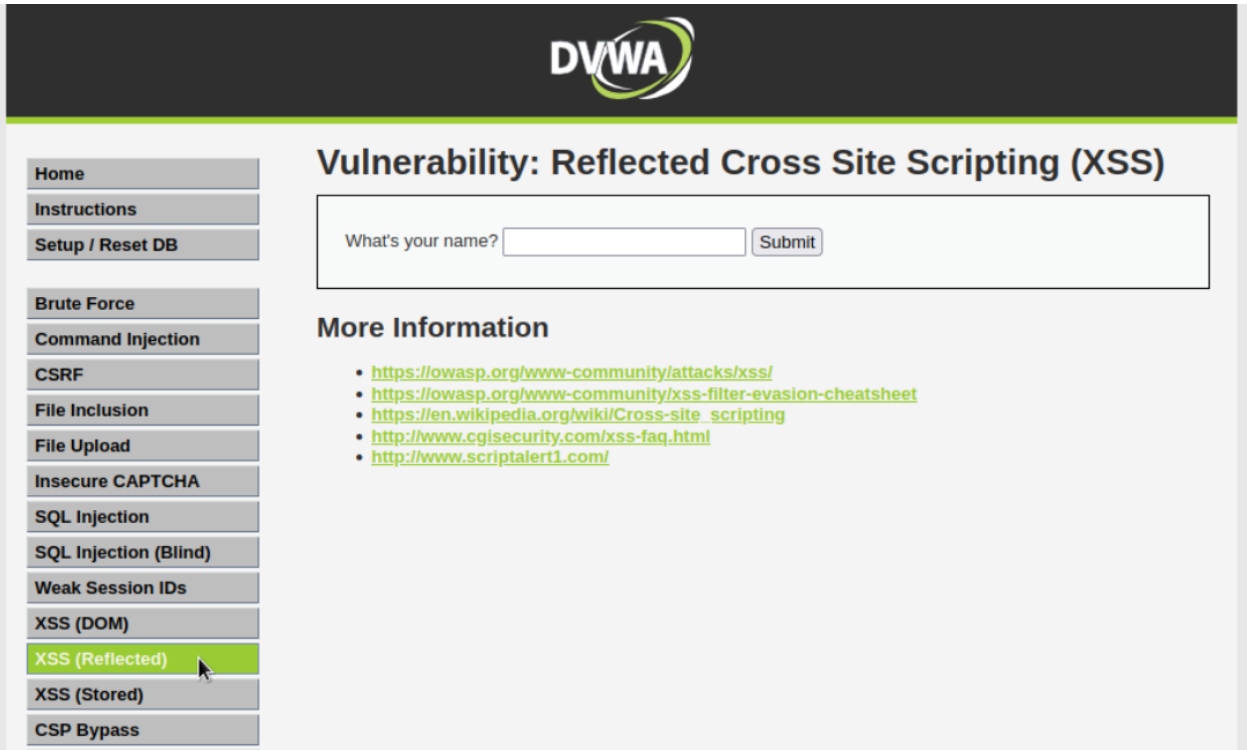
Disusun oleh :

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

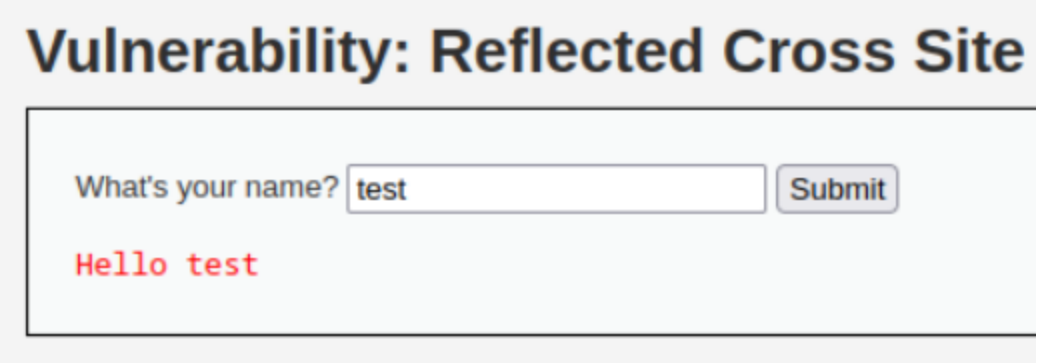
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ 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>
```

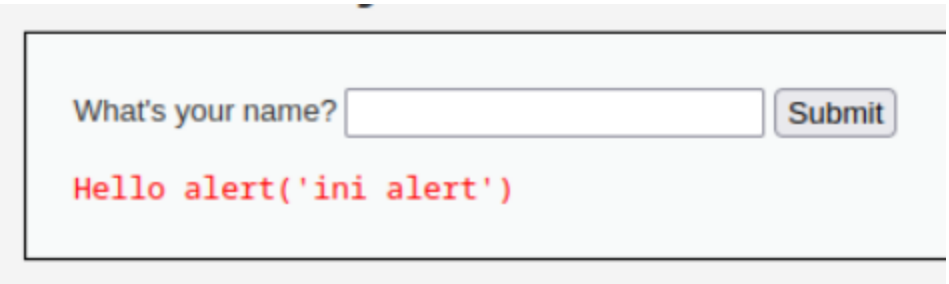
Akan menghasilkan output seperti berikut

Pada XSS reflected level low dijelaskan bahwa 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.

Coba untuk memunculkan alert yang berisi cookie dari browser korban dengan memasukkan script berikut ke input text lalu klik Submit

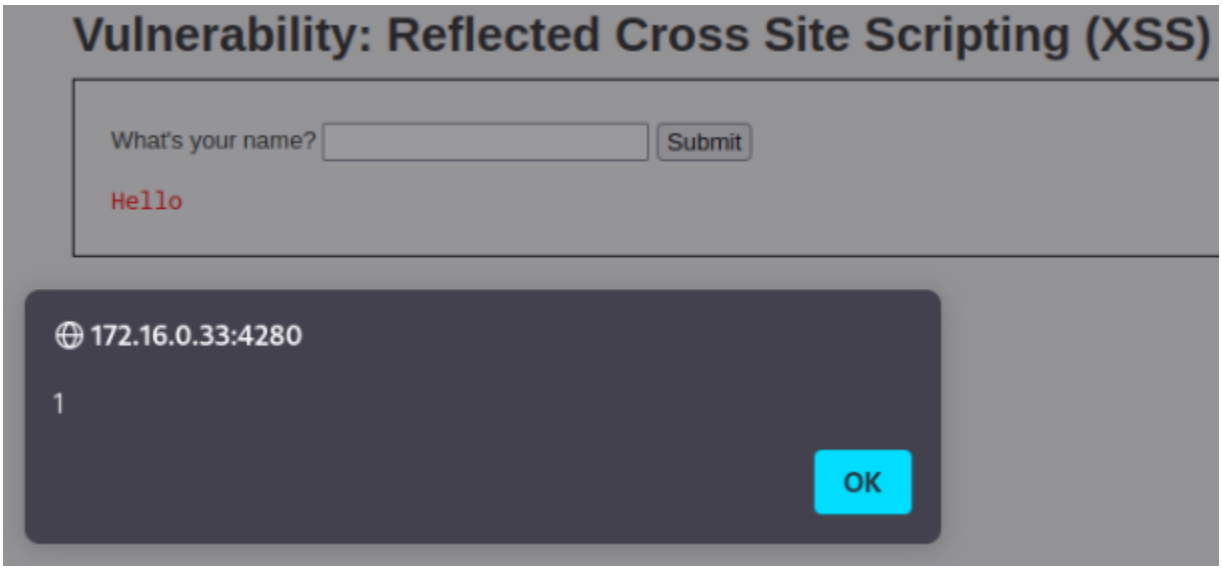
```
<script>alert('ini alert')</script>
```



Yang muncul adalah teks didalam tag `script` dan tidak memunculkan alert sama sekali pada browser. Ini dikarenakan pada level medium DVWA melakukan filtering pada tag tertentu, dan pada kasus ini tag `script` difilter oleh sistem, sehingga yang dicetak hanya pesan yang ada dalam tag `script`.

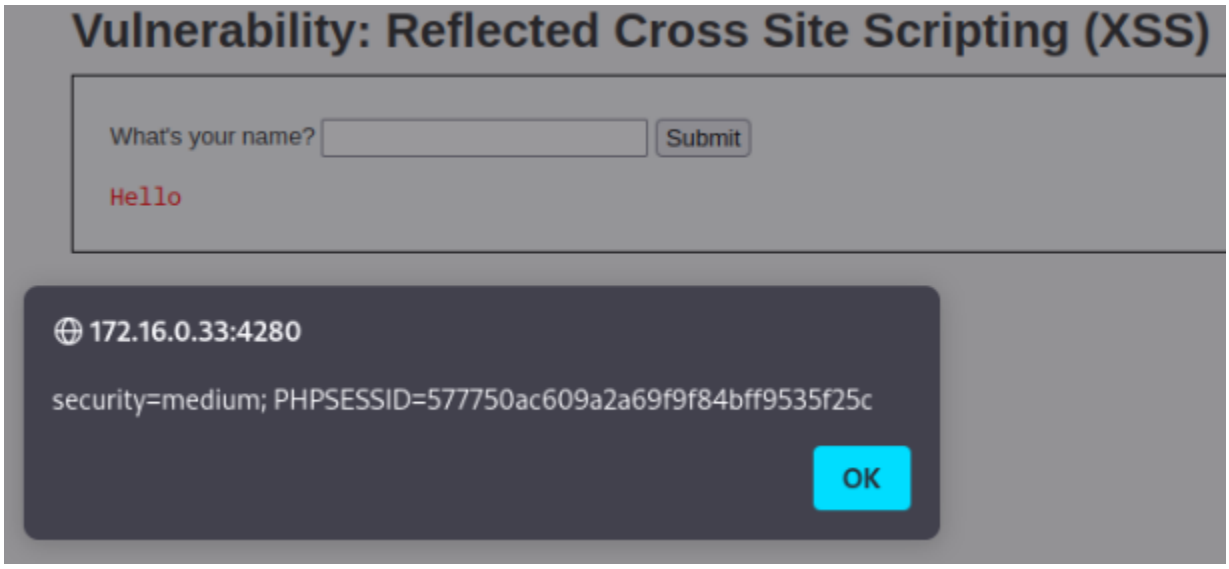
Untuk mengatasi hal ini dapat menggunakan tag lain yang kemungkinan tidak difilter oleh website, seperti contohnya tag `img`. Gunakan tag `img` untuk melakukan XSS attack, seperti contoh script berikut akan menampilkan alert menggunakan tag `img`.

```
<img src/onerror=alert(1)>
```



Akan muncul pop up alert dengan value 1 didalamnya, ini berarti tag `img` tidak difilter oleh sistem sehingga dapat dilakukan XSS melaluinya. Coba untuk memunculkan cookie yang tersimpan pada browser dengan mengganti value `1` pada alert menjadi `document.cookie`

```
<img src/onerror=alert(document.cookie)>
```



Setelah klik submit maka cookie akan ditampilkan dalam alert

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)