

8. XSS (DOM)

Disusun oleh :

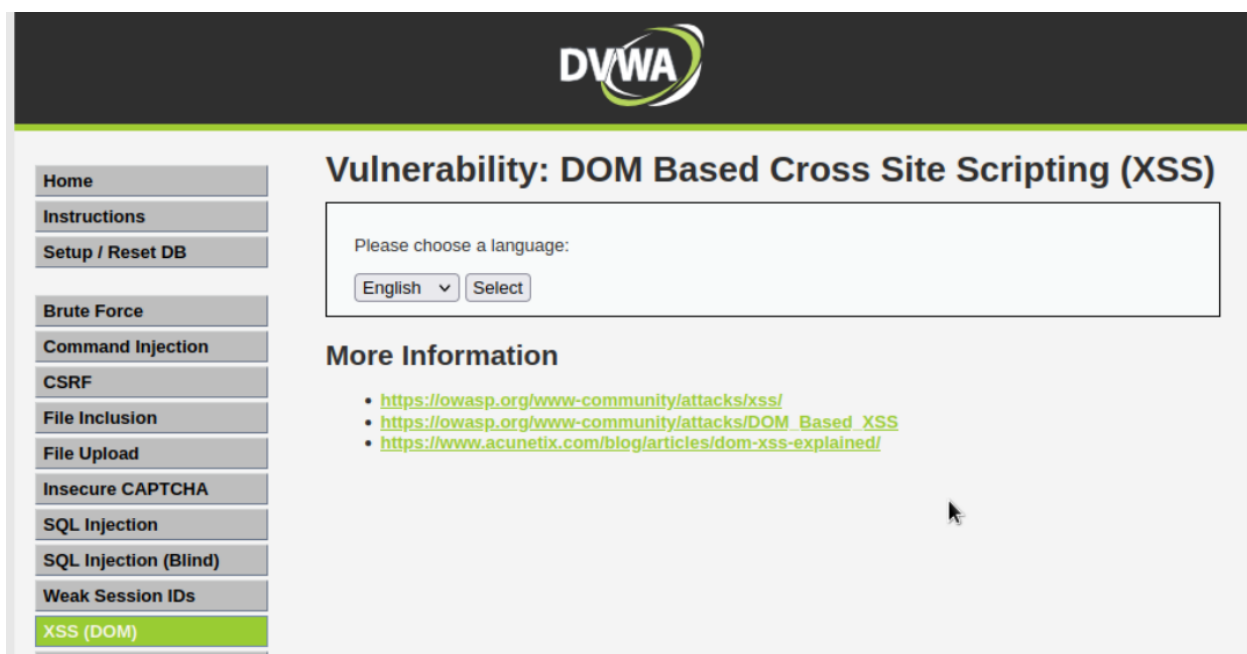
Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafidh 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”

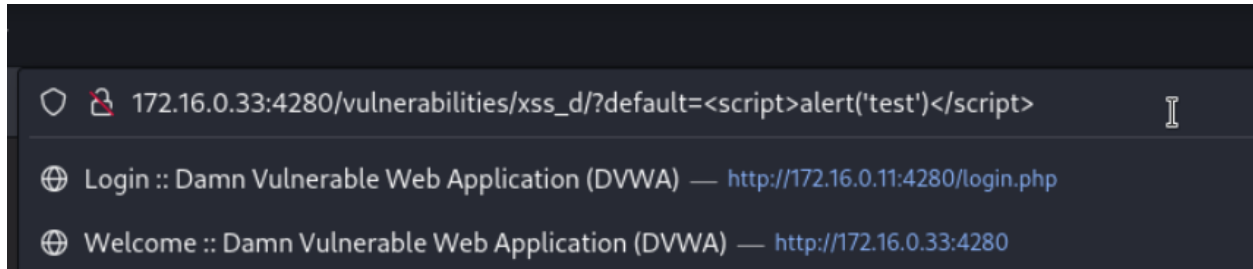
Tidak ada perubahan yang terjadi pada halaman web, namun jika dilihat pada URL akan menampilkan bahasa yang baru saja dipilih

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

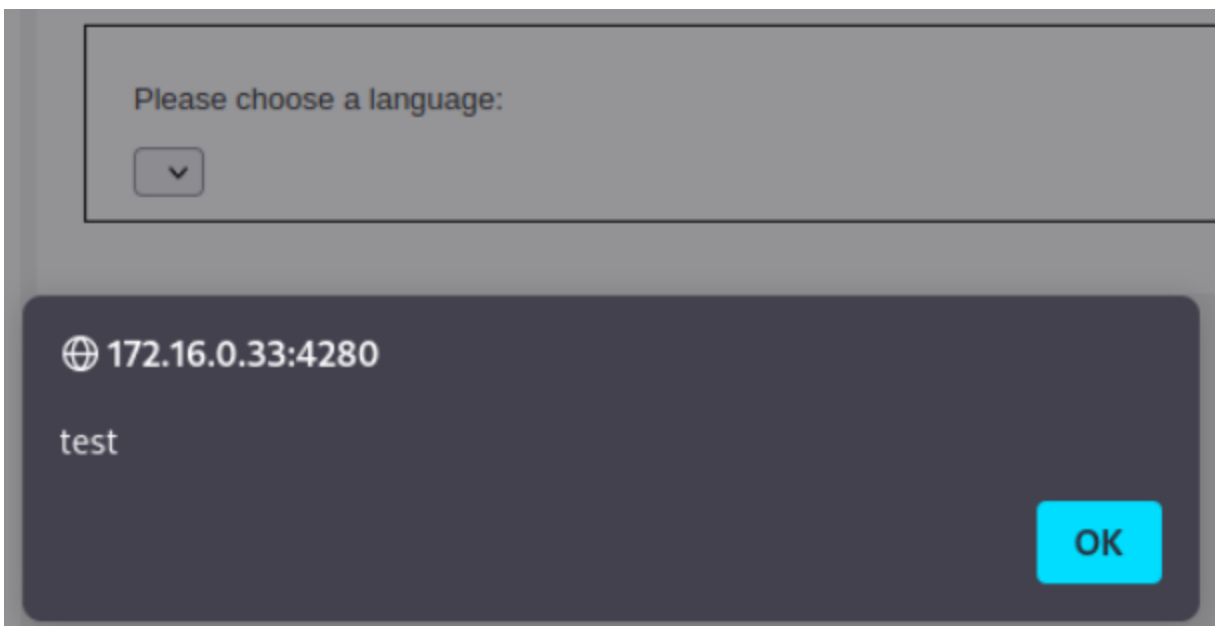
Karena tidak ada kolom input pada halaman web, maka payload XSS akan dimasukkan dalam URL

Gantikan value pada bahasa dengan payload XSS

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

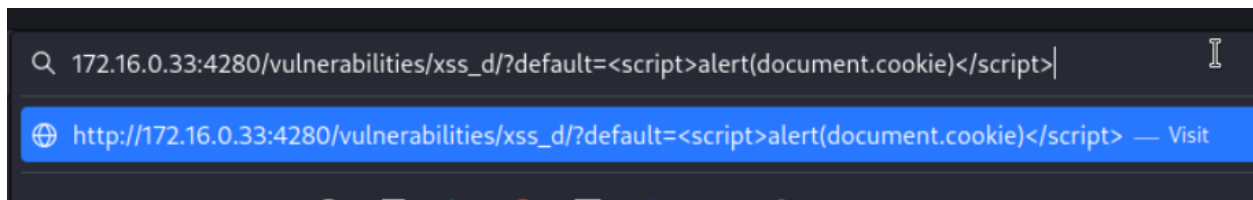


XSS dapat dijalankan

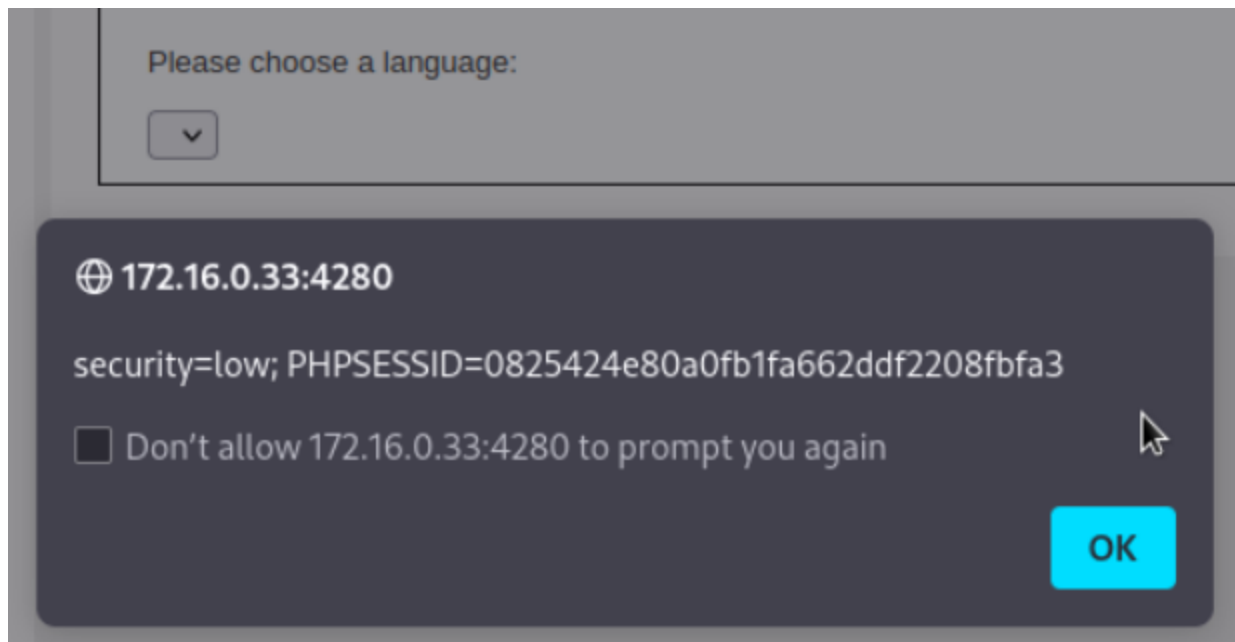


Coba untuk masukkan payload untuk mendapatkan cookie

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



Cookie berhasil didapatkan



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)