DVWA SQL Injection (Blind)(low)

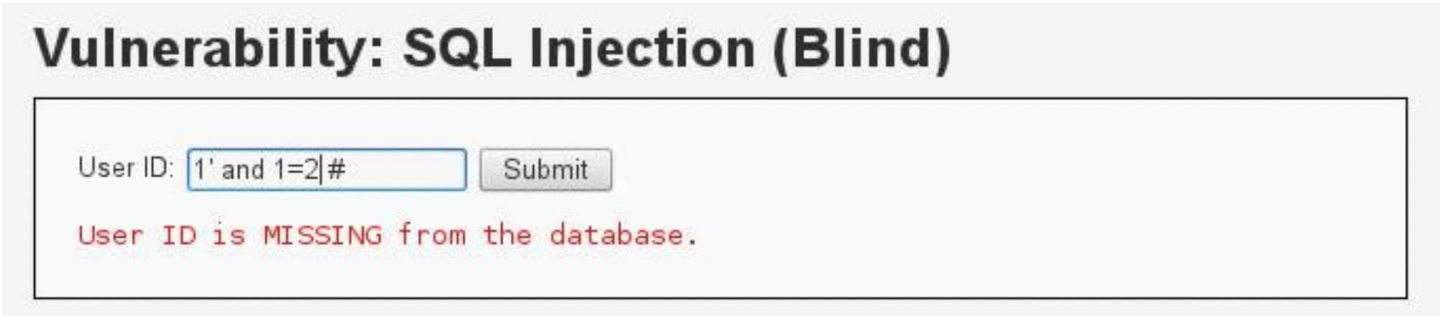
La pagina richiede di inserire un un numero id (in questo caso io ho inserito 1)

01 - Output Ok

Dopo di che per riprodurre un errore è stato inserito un classico apice:

02 - Output con Errore

A questo punto sono stati ottenuti tutti è due i tipi di risposte, ora è possibile attaccare lo script per fare dei raffronti.
Iniettando una query mysql la quale da sempre un risultato falso, si otterrà un risultato identico all'immagine precedente [img 02]
La condizione "AND 1=2#" restituirà sempre un errore perché 1≠2



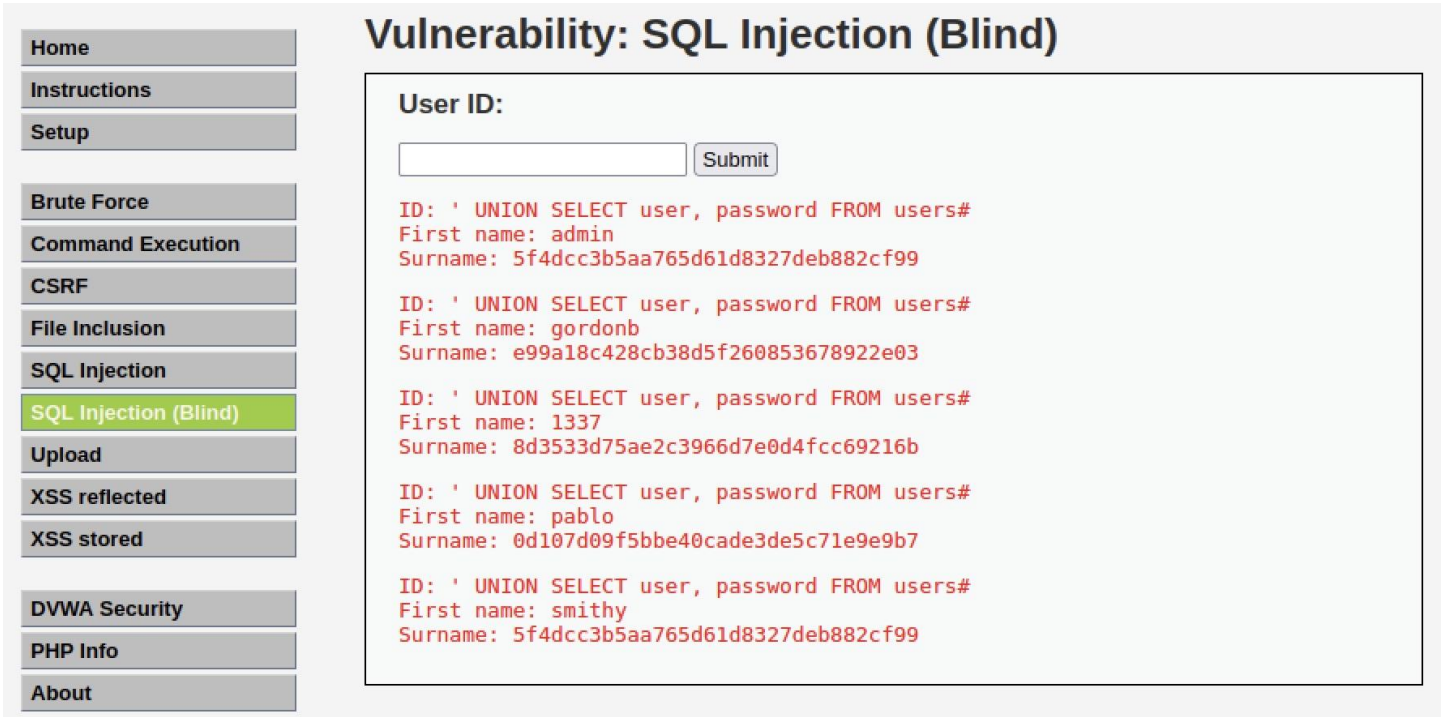
03 - Injection Low Level con Errore

Per avere conferma del payload giusto, vado ad iniettare una query che darà un risultato positivo: AND 1=1# il quale appunto è sempre vero.

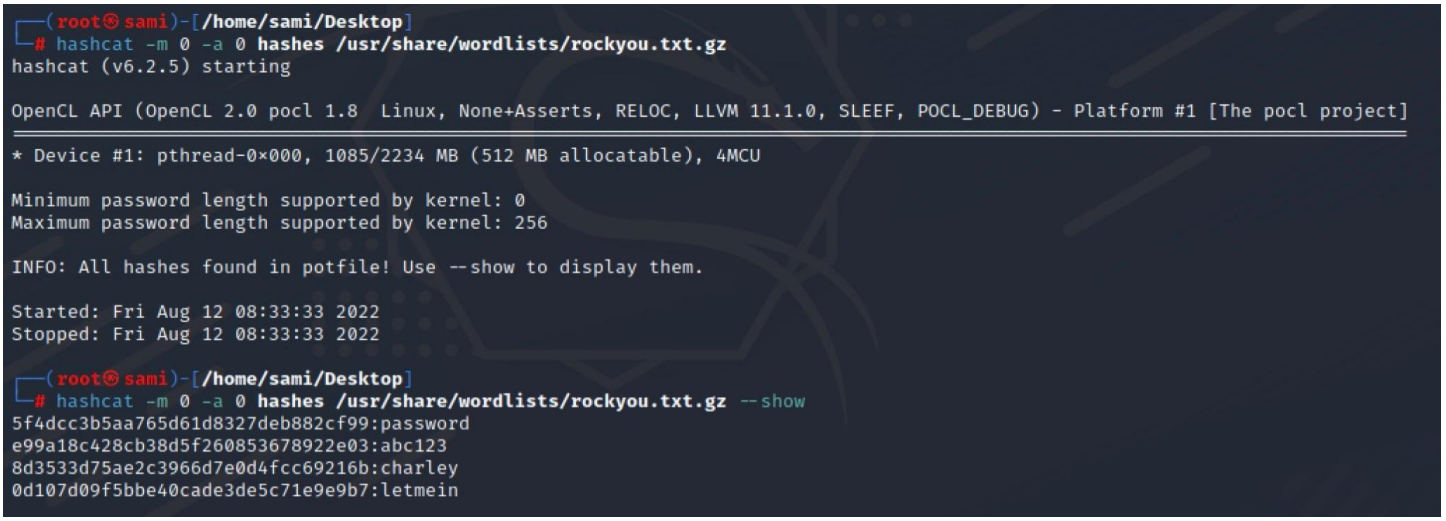
04 - Injection Low Level senza Errore

Confrontando img01 e img04 si può notare che restituiscono lo stesso risultato

Con il comando `'UNION SELECT user, password FROM users#` possiamo trovare tutti i username e le password



per decriptare questi hash è stato usato hashcat[v6.2.5]



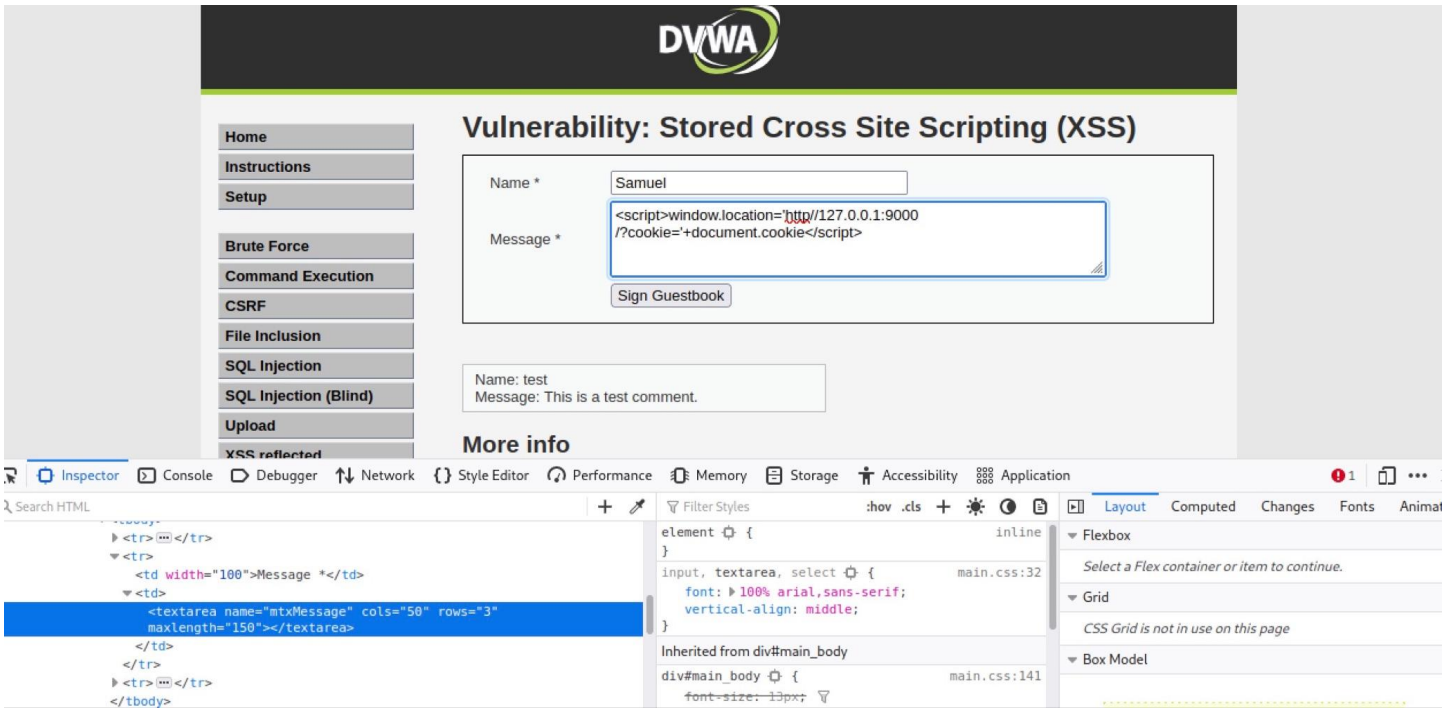
XSS stored

Per rubare i cookie andremo a sfruttare questa vulnerabilità
una volta creato il server si è usato python, il server ci servirà per indirizzare i cookie verso di noi, aperta la sessione torniamo sulle vulnerabilità XSS stored

```
┌──(sami㉿sami)-[~]
└─$ sudo apt install python3
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libpython3-dev libpython3-stdlib libpython3.10 libpython3.10-dev libpython3.10-minimal
  libpython3.10-stdlib libssl3 python3-dev python3-minimal python3.10 python3.10-dev
  python3.10-minimal
Suggested packages:
  python3-doc python3-venv python3.10-venv python3.10-doc binfmt-support
The following NEW packages will be installed:
  libssl3
The following packages will be upgraded:
  libpython3-dev libpython3-stdlib libpython3.10 libpython3.10-dev libpython3.10-minimal
  libpython3.10-stdlib python3 python3-dev python3-minimal python3.10 python3.10-dev
  python3.10-minimal
12 upgraded, 1 newly installed, 0 to remove and 1049 not upgraded.
Need to get 13.0 MB of archives.
After this operation, 6,660 kB of additional disk space will be used.
```

```
┌──(sami㉿sami)-[~]
└─$ python -m http.server --bind 127.0.0.1 9000
Serving HTTP on 127.0.0.1 port 9000 (http://127.0.0.1:9000/) ...
127.0.0.1 - - [12/Aug/2022 07:40:01] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 07:40:01] code 404, message File not found
127.0.0.1 - - [12/Aug/2022 07:40:01] "GET /favicon.ico HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.
```

Dopo aver cambiato la lunghezza massima consentita per lo script (da 50 a 150) inseriamo la nostra stringa nella sezione messagge



Una volta avviato lo script, ci porta alla pagina del nostro server, mostrandoci così cookie della nostra sessione [vedi img sotto]