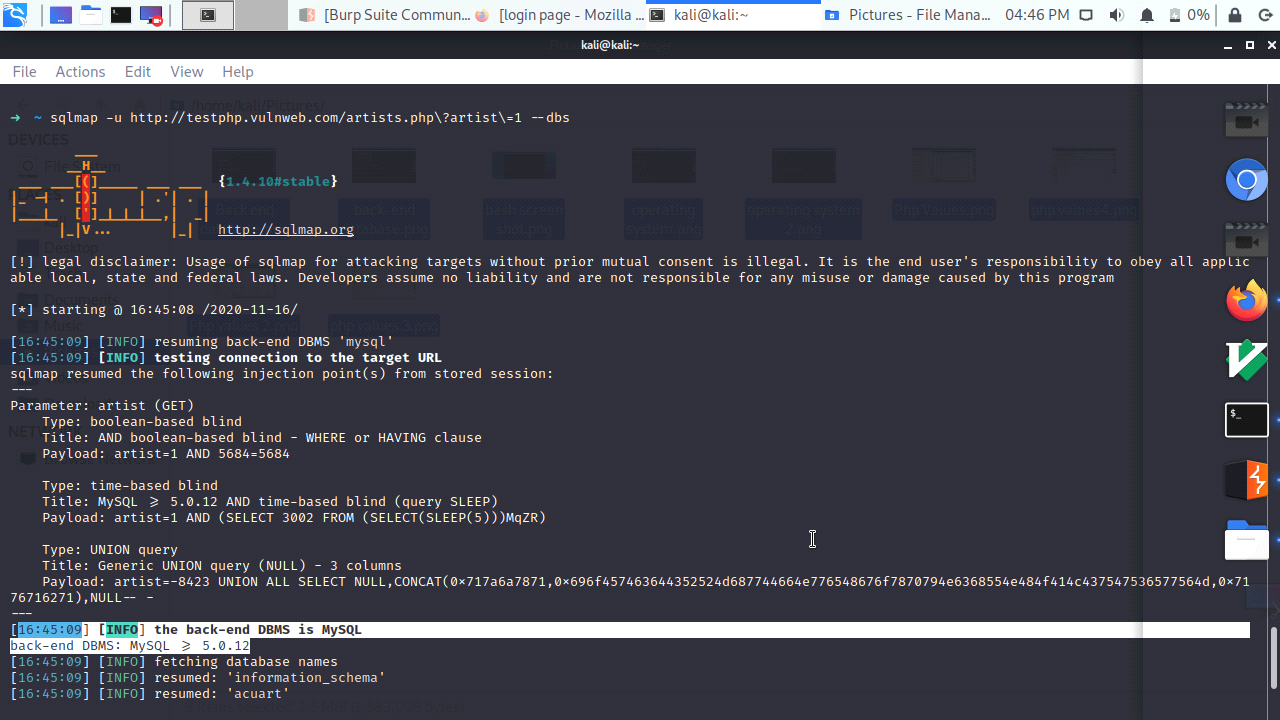
SQL INJECTION ON <http://testphp.vulnweb.com/login.php>

1. Back End Database

Backend database is MYSQL 5.0.12. To get this i used sqlmap.

Command used.

sqlmap -u <http://testphp.vulnweb.com/login.php\?artist=1> –dbs



2. The operating system

The OS used in this not clearly defined but they using some VMware on many flavors.

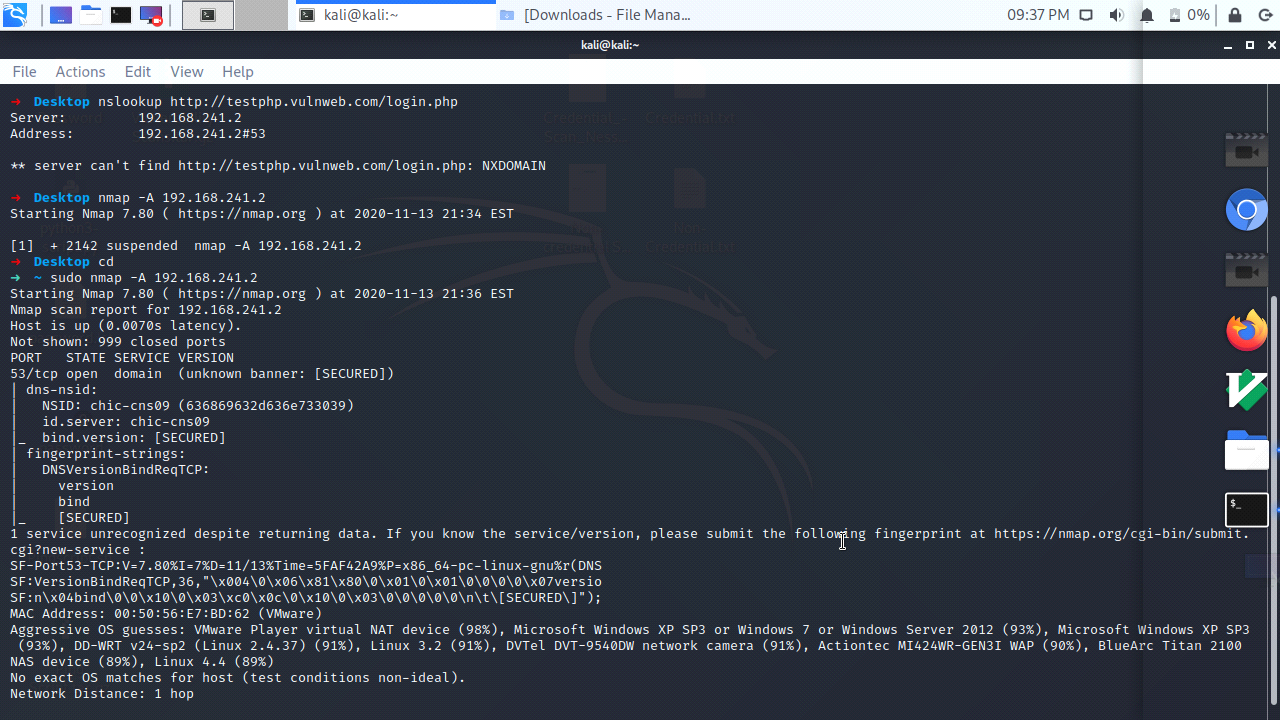
Commands.

1. Used nslookup to get IP.

nslookup <http://testphp.vulnweb.com/login.php>

2. Than used "NMAP -A option to get the details of operating system.

nmap -A 192.168.241.2



3. Php values of the site using "Burpsuite"

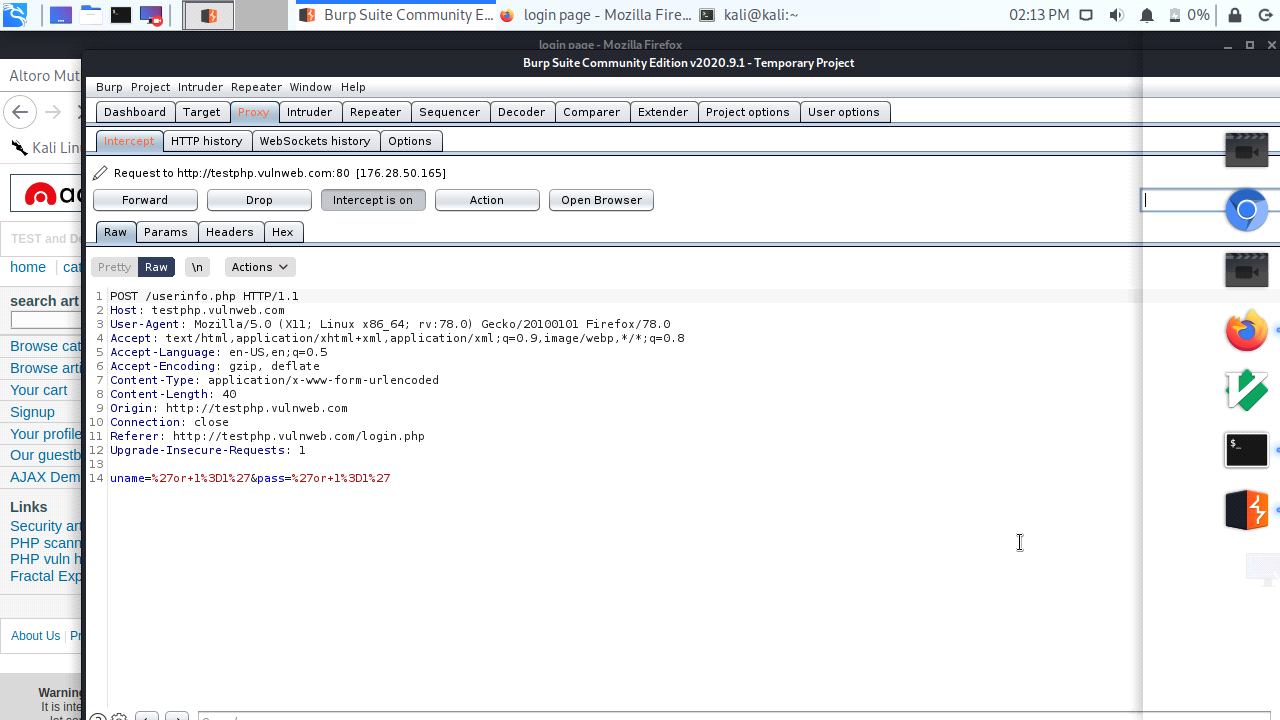
To check if the site is vulnerable to sql injection we must provide some random php values.

I used "WFUZZ" github random values which includes 125 sql injectable values.

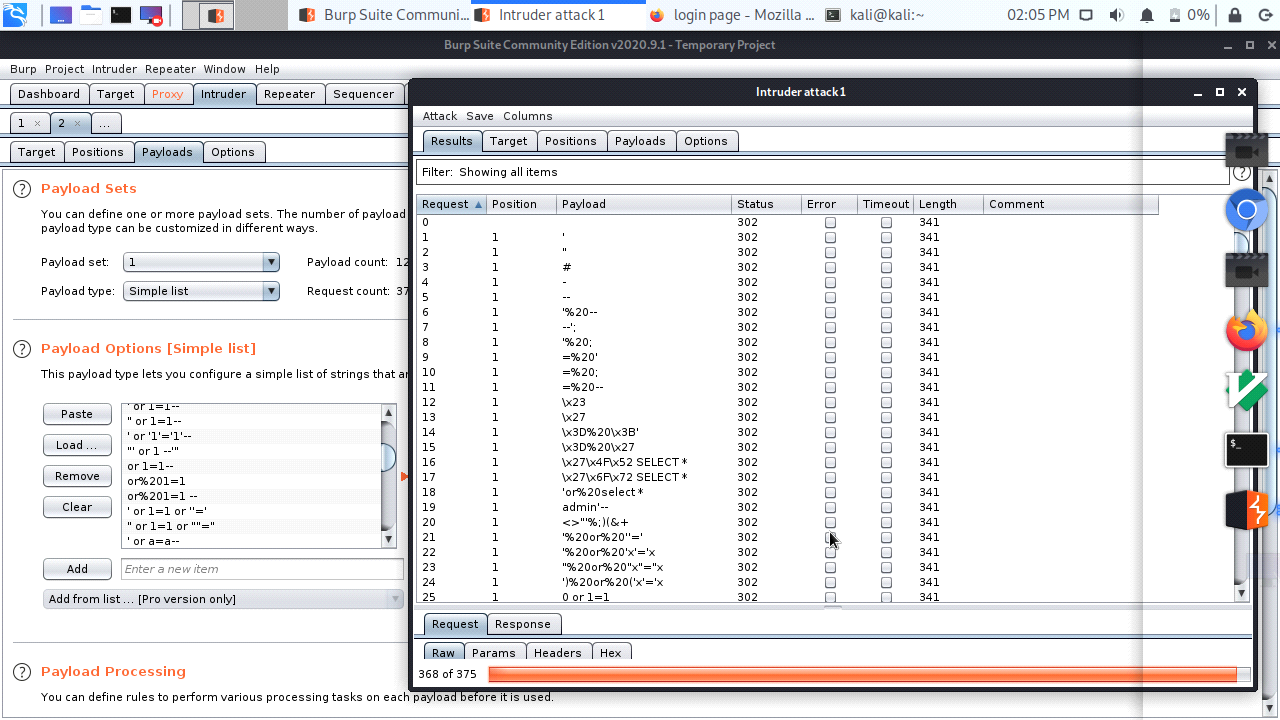
SOURCE : <https://github.com/xmendez/wfuzz/blob/master/wordlist/Injections/SQL.txt>

STEPS.

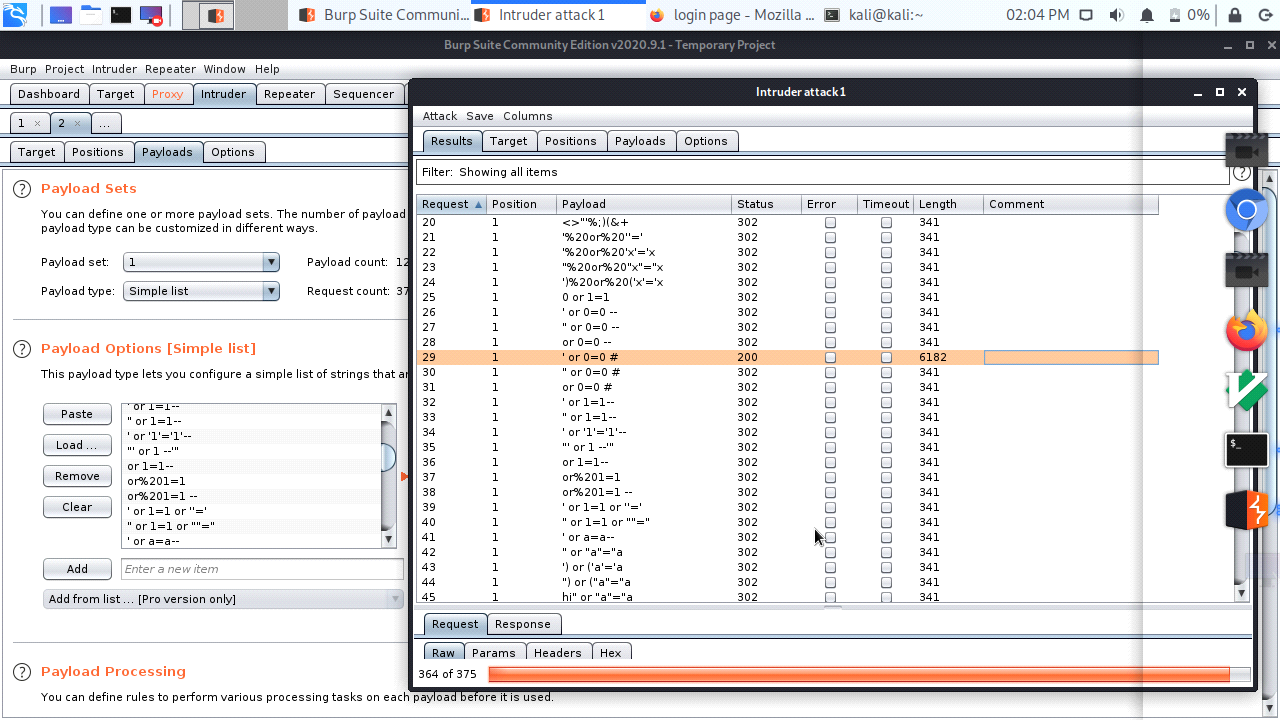
1. Firstly, I Changed the proxy setting on Firefox so burp can intersect the traffic between the site and work its way in to the request that are being made.

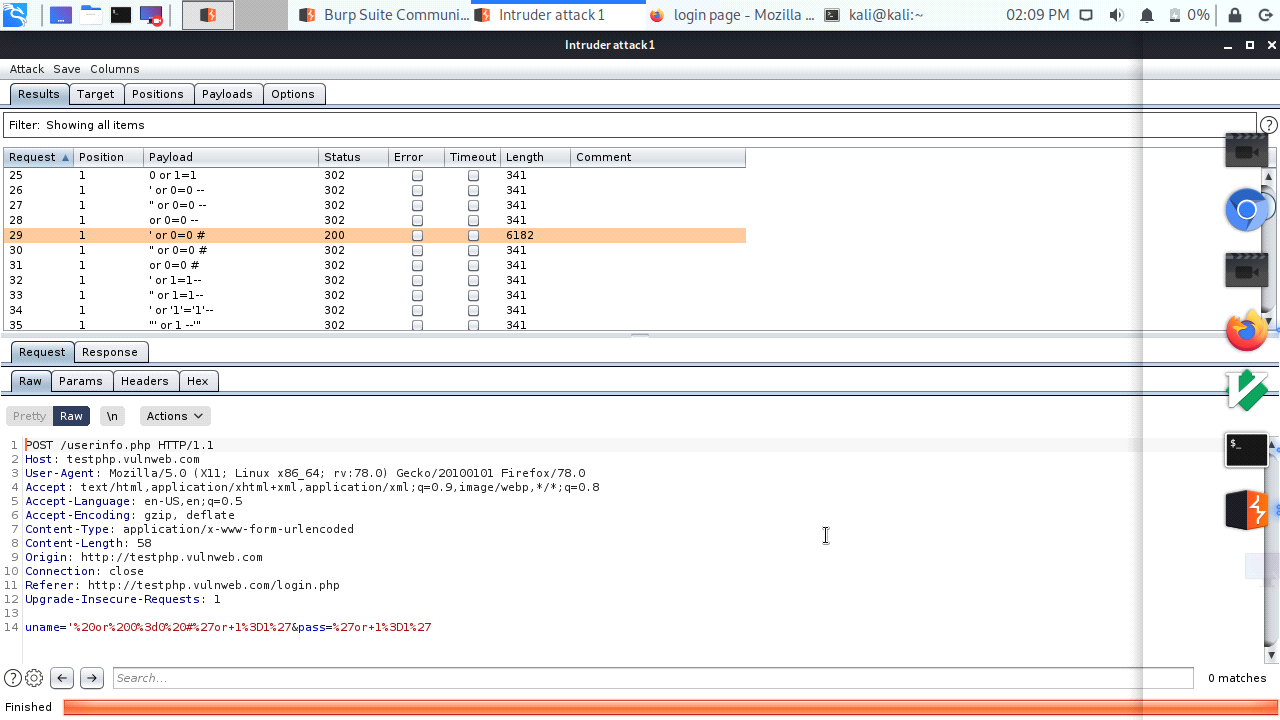


2. Than i used "Intruder" with the PAYLOAD options which includes the random SQL INJECTION wordlist from GitHub. The intruder target on the Username and password which is selected by me on intruder options.



3. As applying the payloads to burp on target site, we can see which values effect more to the SQL INJECTION by checking the STATUS field.





The request number 29 shows the most Sql injection can be made on our Host site which is

' or 0=0 #

200 Code informs about successful processing of the request which tells sql injection can be made by using the required values.