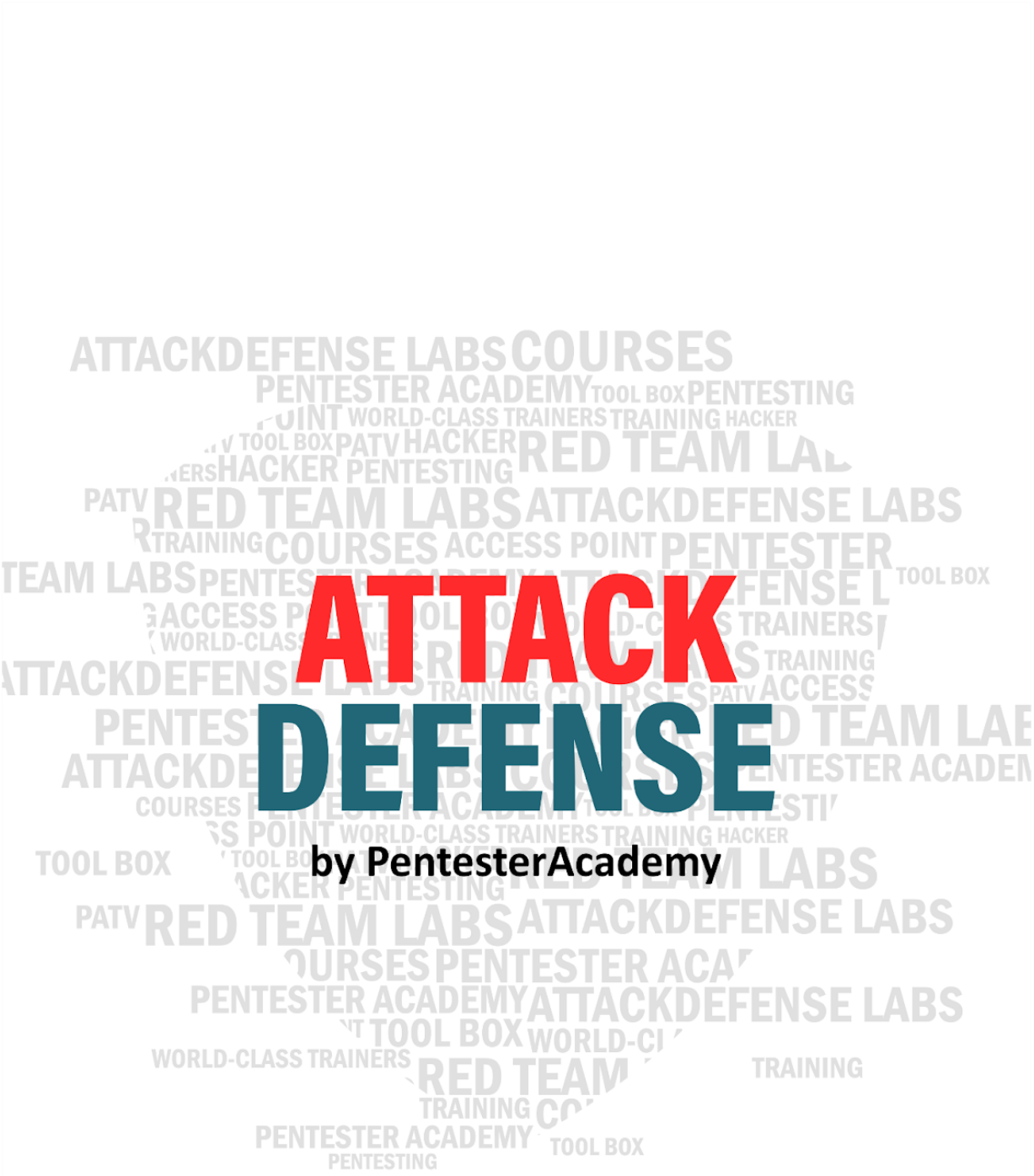

ATTACK
DEFENSE
by PentesterAcademy

Name	Attacking Basic Auth with Burp Suite
URL	https://attackdefense.com/challengedetails?cid=1896
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Determining the IP address of the target machine.

Command: ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.3  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:03  txqueuelen 0  (Ethernet)
        RX packets 626  bytes 87006 (84.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 556  bytes 1662537 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.253.50.2  netmask 255.255.255.0  broadcast 192.253.50.255
        ether 02:42:c0:fd:32:02  txqueuelen 0  (Ethernet)
        RX packets 18  bytes 1452 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1990  bytes 14480541 (13.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1990  bytes 14480541 (13.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.253.50.2

Therefore, the target machine has IP address 192.253.50.3

Step 2: Scan the target machine using nmap.

Command: nmap 192.253.50.3

```
root@attackdefense:~# nmap 192.253.50.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 18:29 IST
Nmap scan report for target-1 (192.253.50.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:FD:32:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@attackdefense:~#
```

We have discovered that HTTP and MYSQL services are running on the target machine.

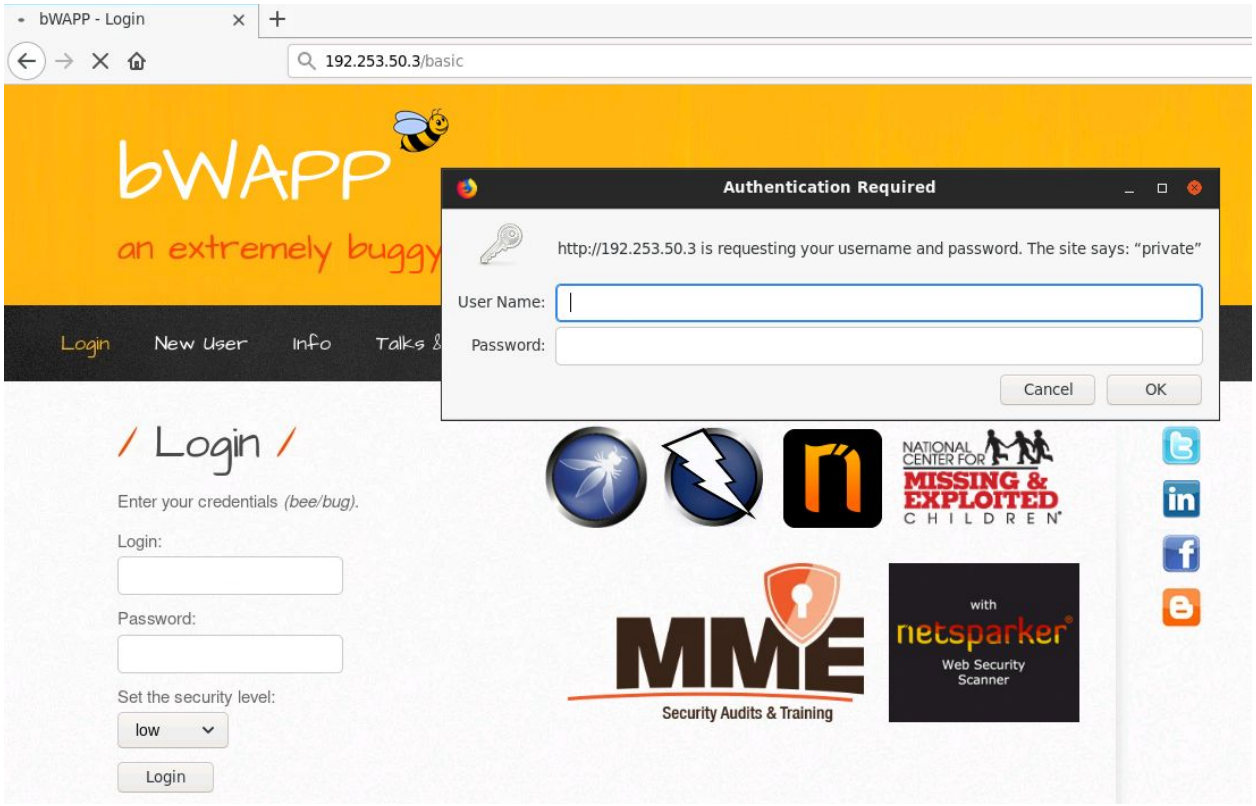
Step 3: Checking the application available on port 80 of the target machine.

URL: http://192.253.50.3

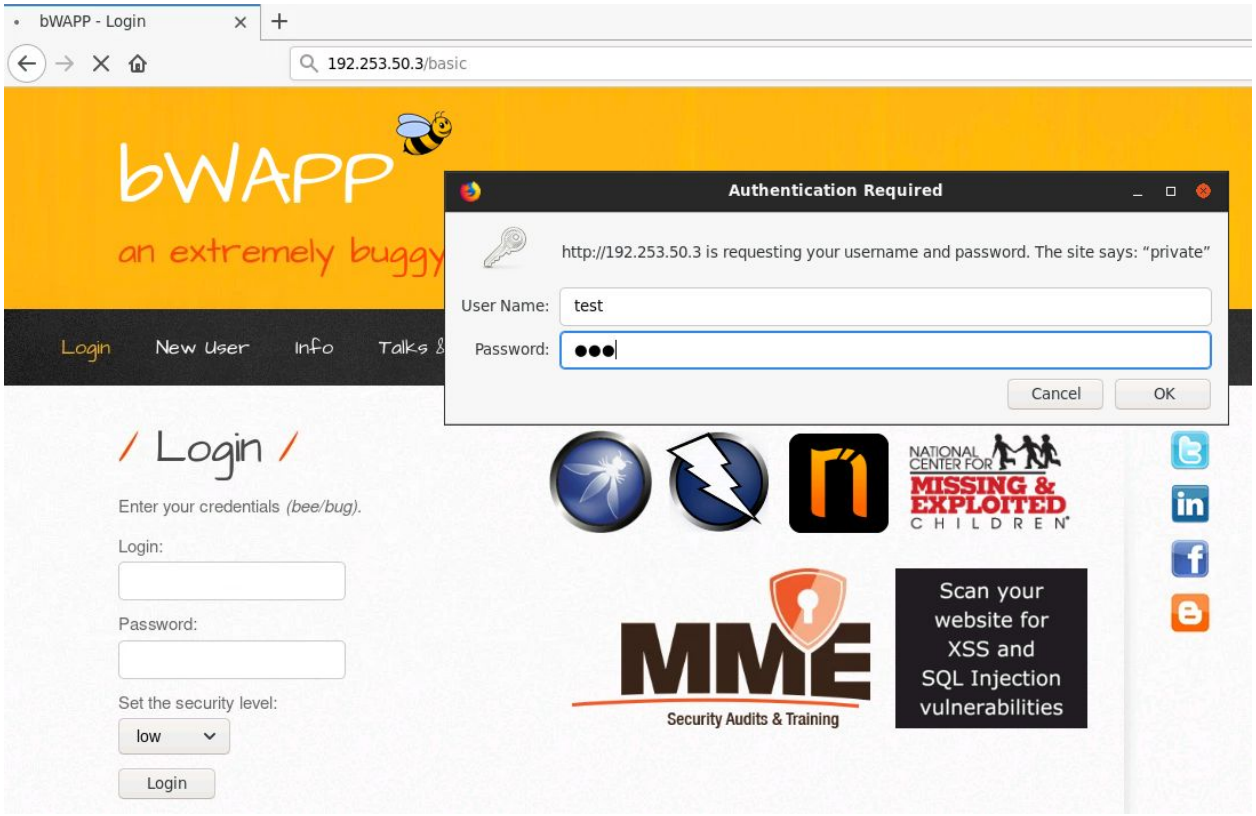
bWAPP application is hosted on the target machine.

Access the /basic directory:

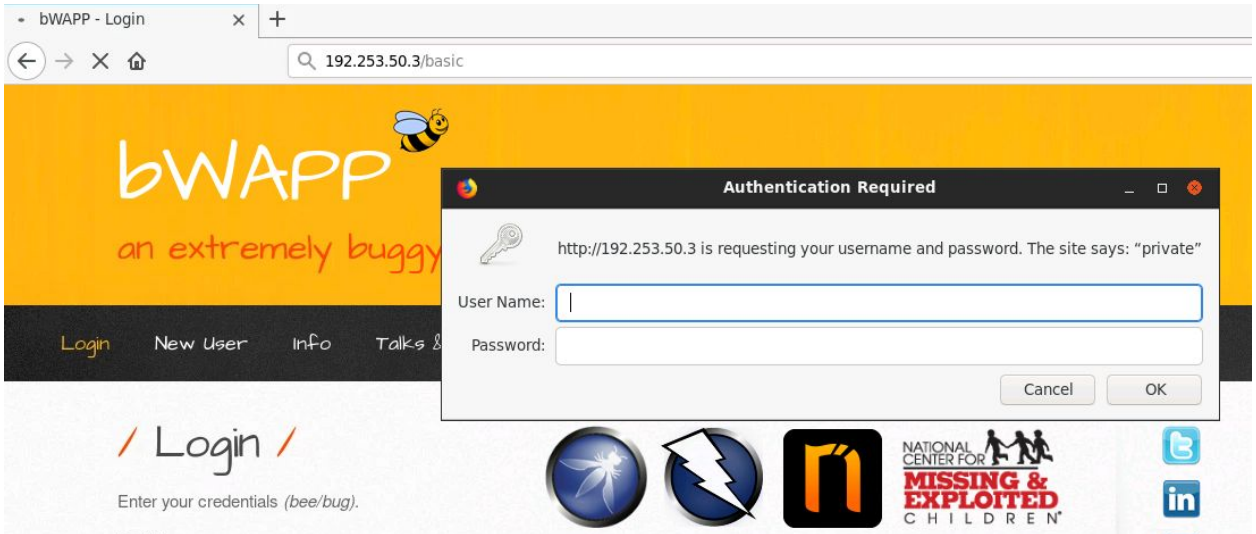
URL: http://192.253.50.3/basic



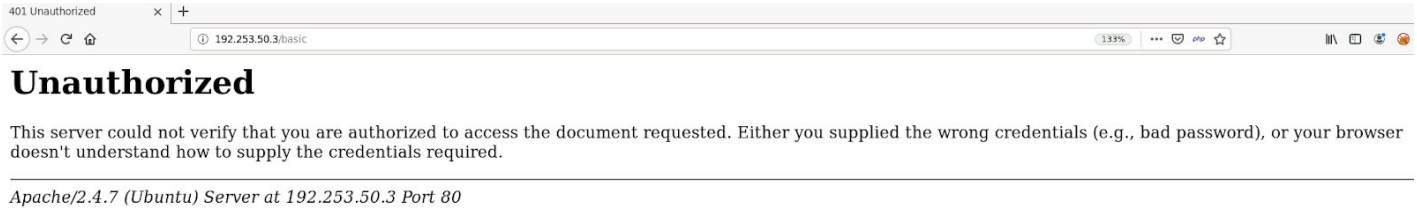
Enter some random username - password combination.



Since the credentials were incorrect, the same login prompt would appear again:



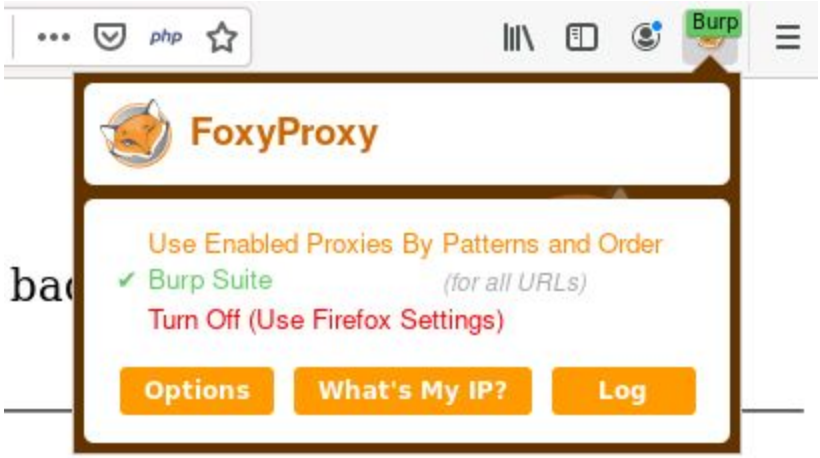
Click on the "Cancel" button:



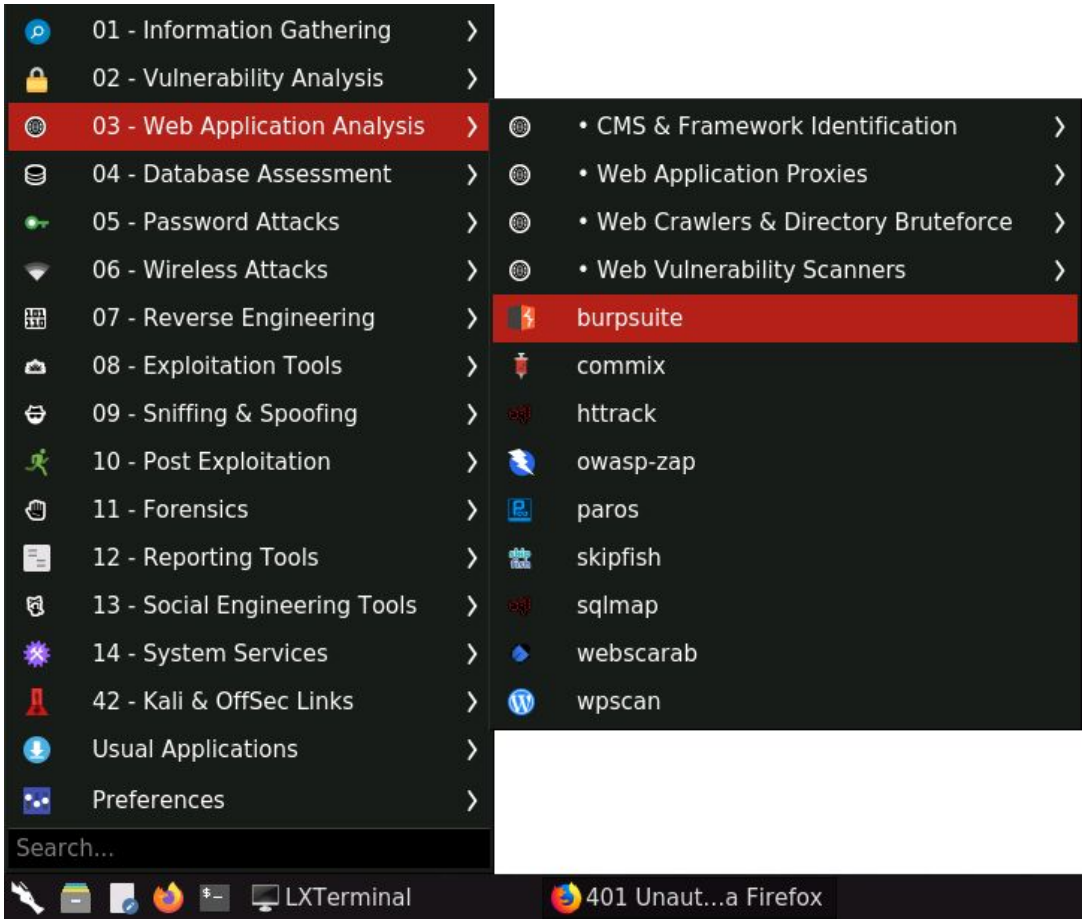
Step 3: Using Burp Suite to crack the Basic Auth:

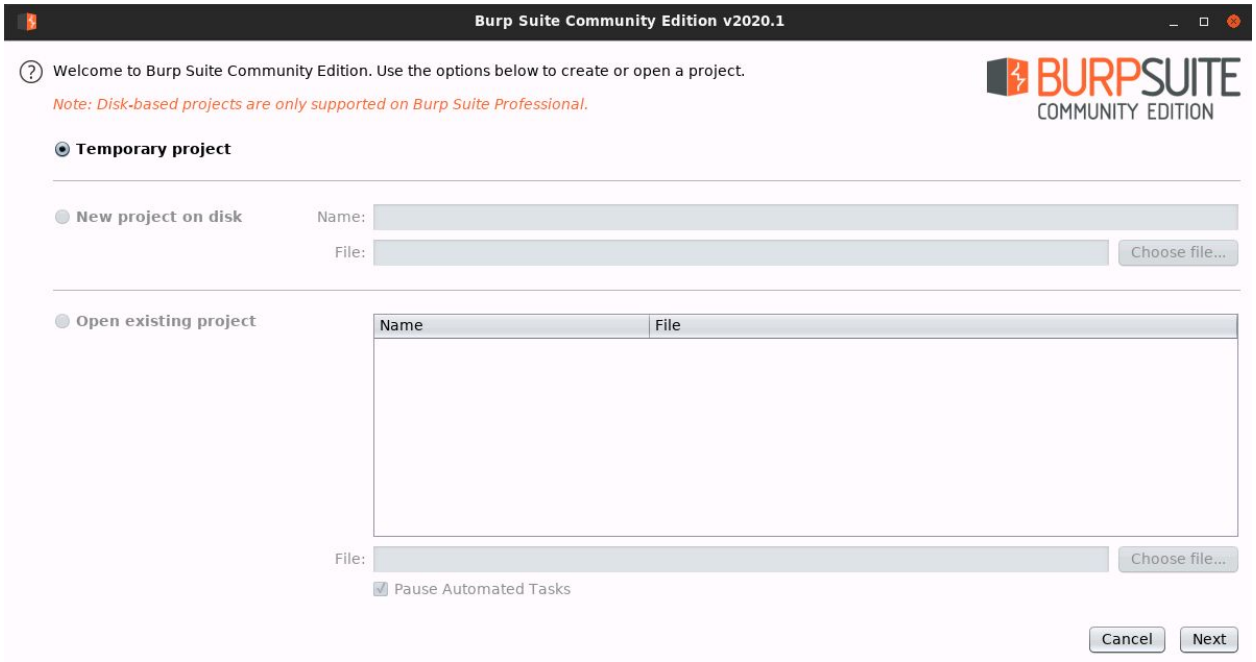
Click on the FoxyProxy plugin icon on the top-right of the browser.

Select Burp Suite option from the list:

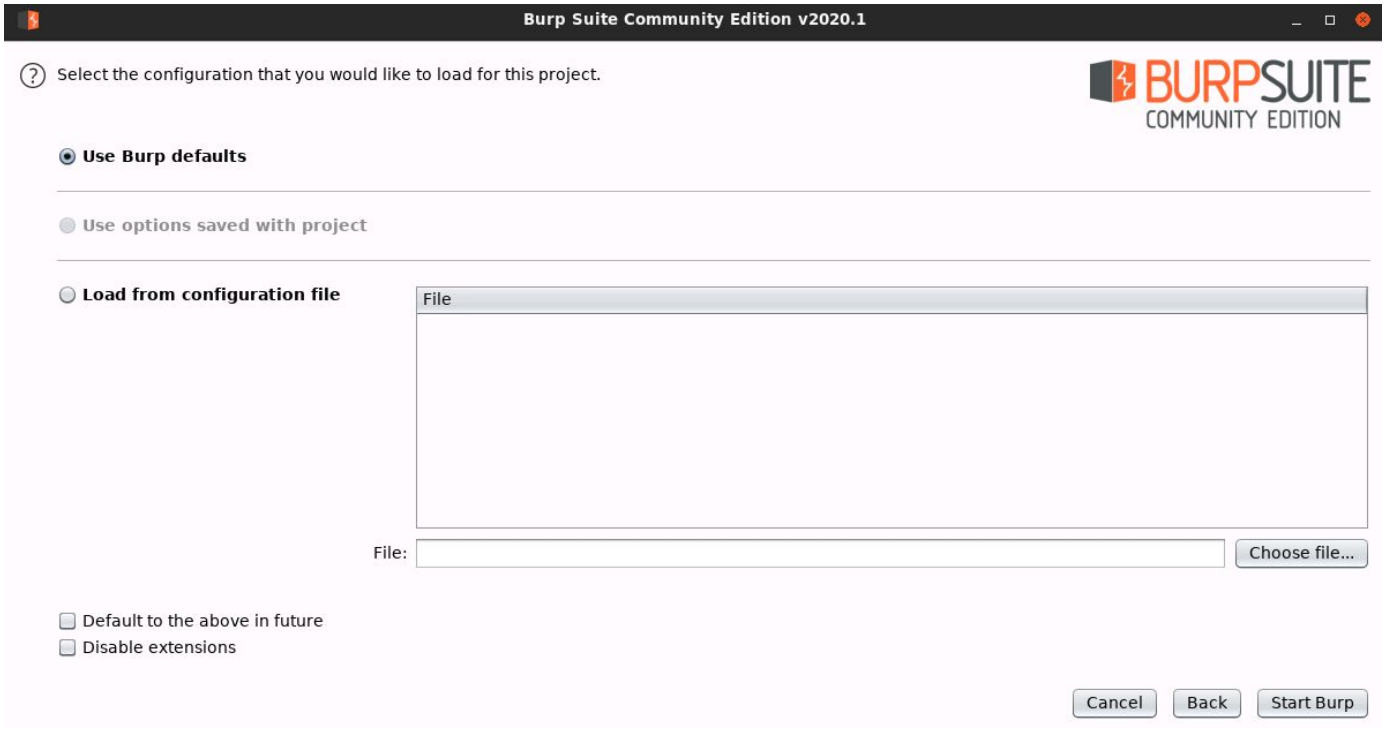


Start Burp Suite:

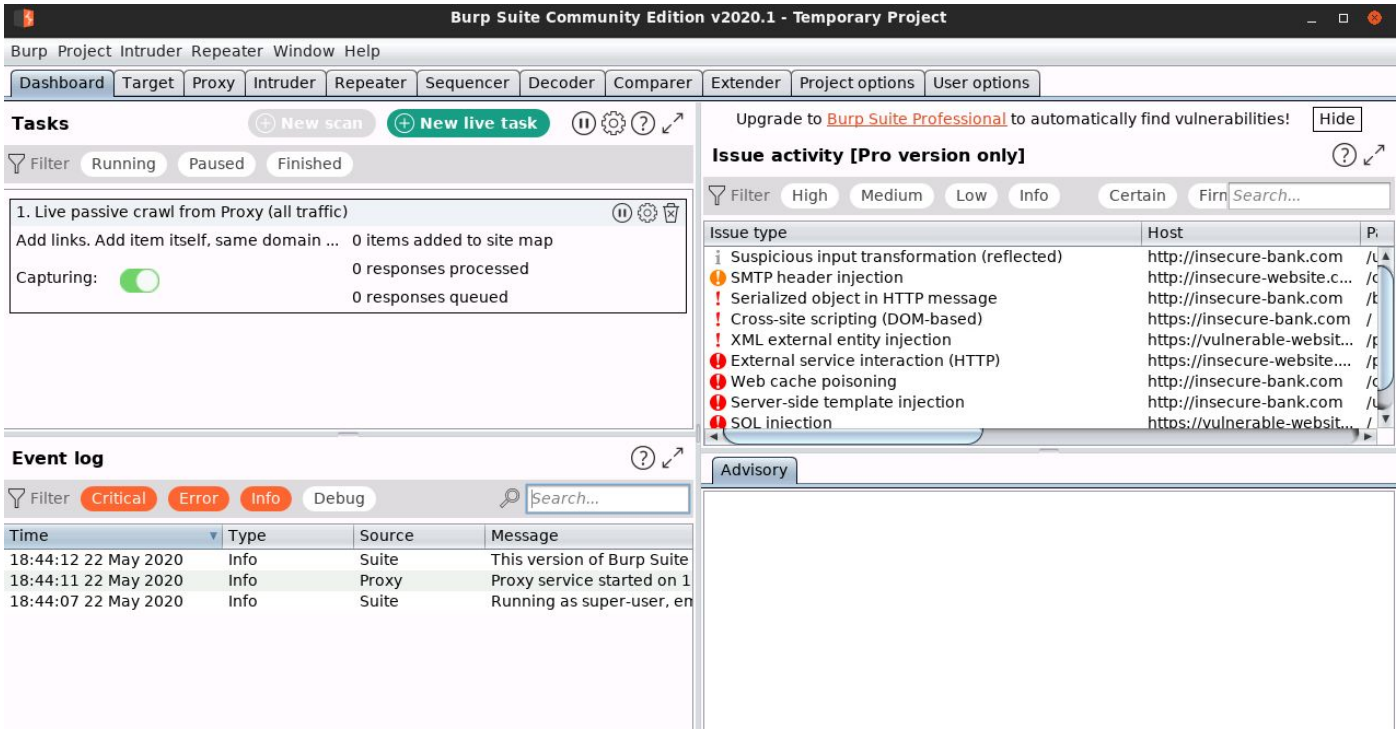



Burp Suite Community Edition v2020.1
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE
COMMUNITY EDITION
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
File:
Choose file...
Pause Automated Tasks
Cancel
Next

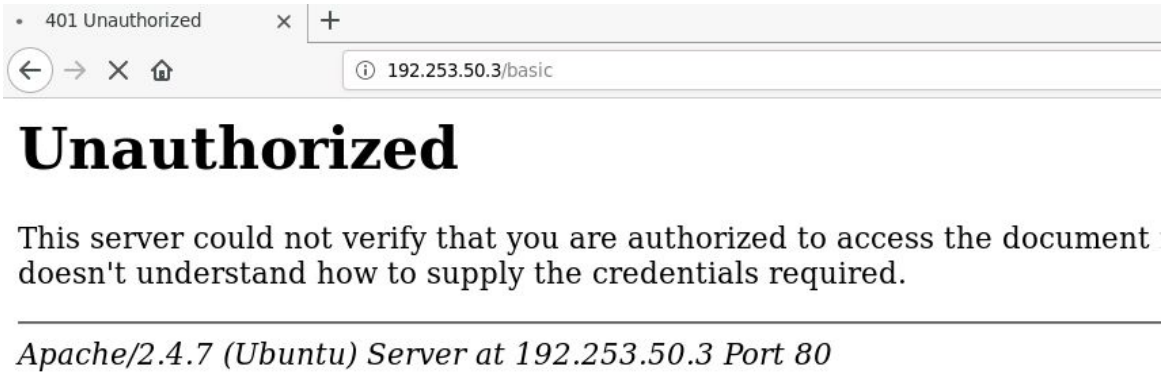
Click Next


Burp Suite Community Edition v2020.1
Select the configuration that you would like to load for this project.
BURPSUITE
COMMUNITY EDITION
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp

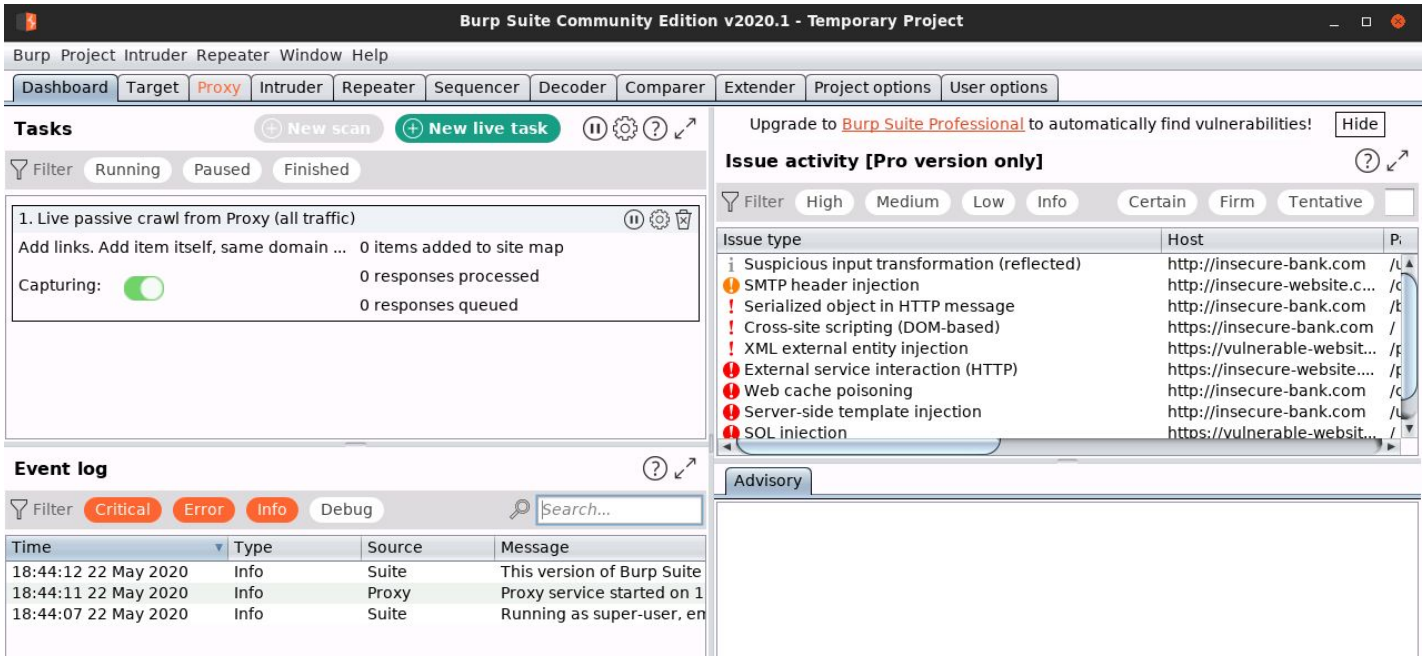
Click on Start Burp



Burp Suite is opened. Now, access the /basic directory again.



Notice that Burp window comes into focus as it has intercepted the request.

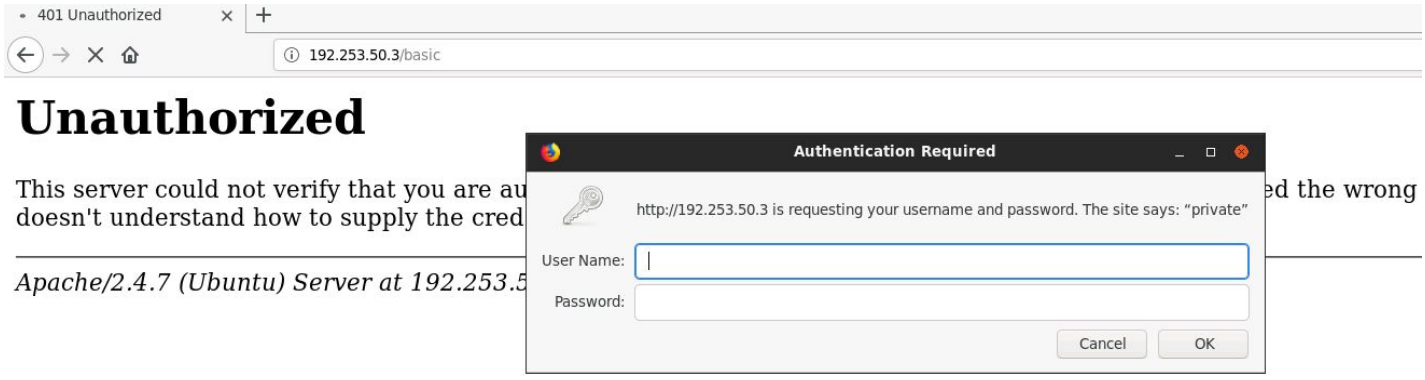


Notice that the Proxy button in Burp Suite lit up (orange).

Click on the Proxy button

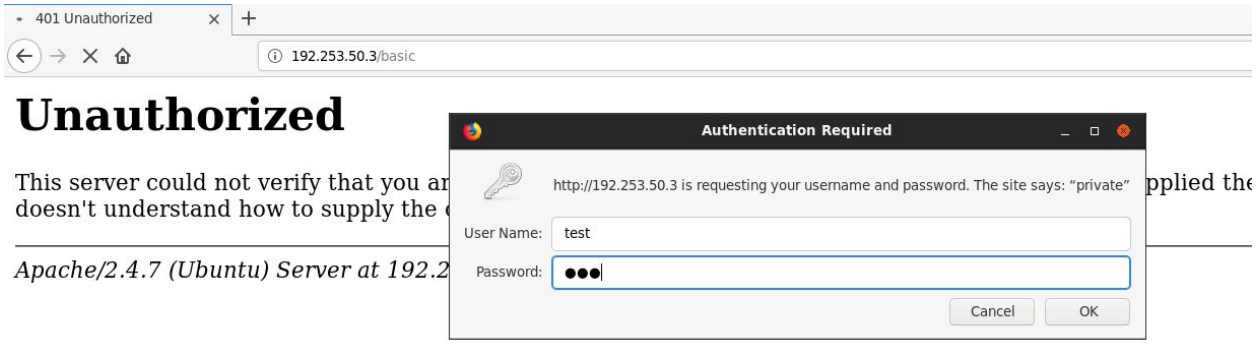
Notice the request being made by the browser.

Forward the above intercepted request and switch back to the browser window:

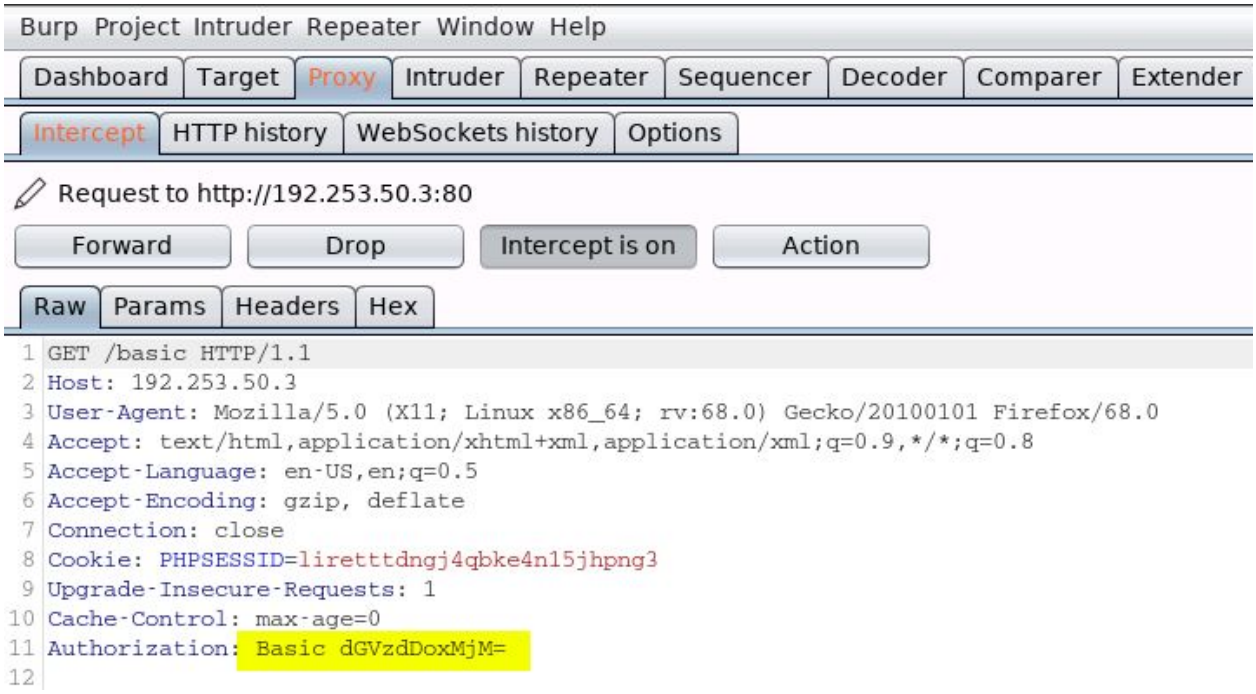


Notice that the application is prompting for credentials.

Enter some random credentials and press Ok.

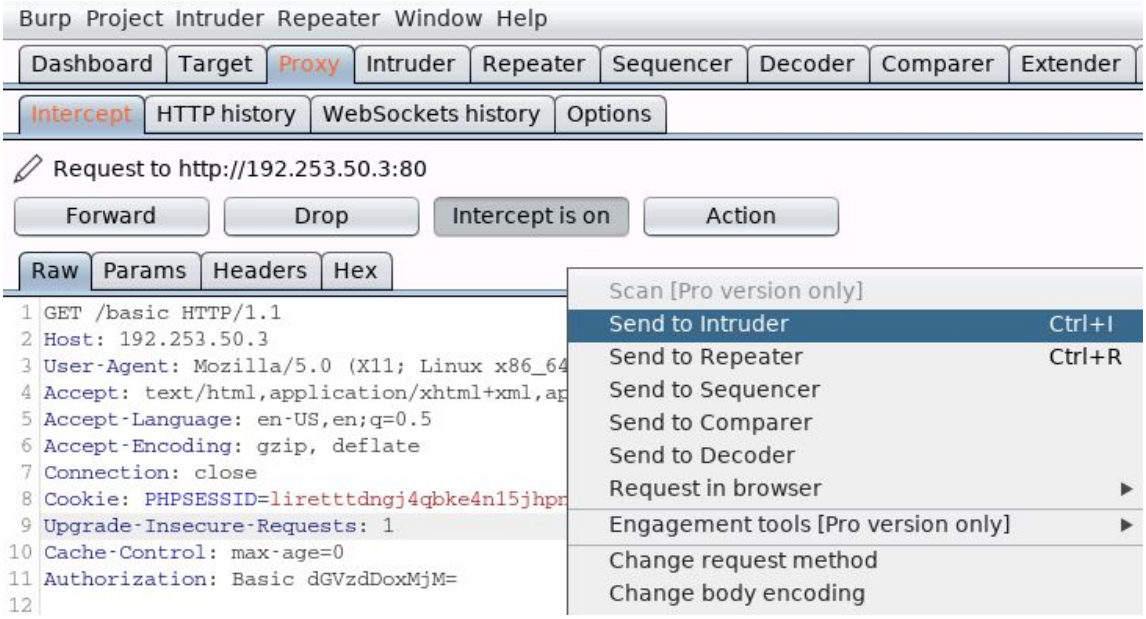


Intercepted request:

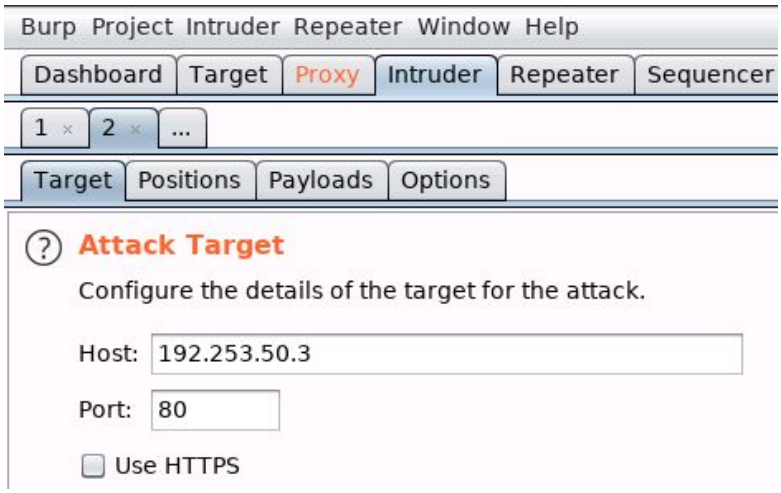


Notice the Authorization header. The “/basic” directory uses Basic Auth.

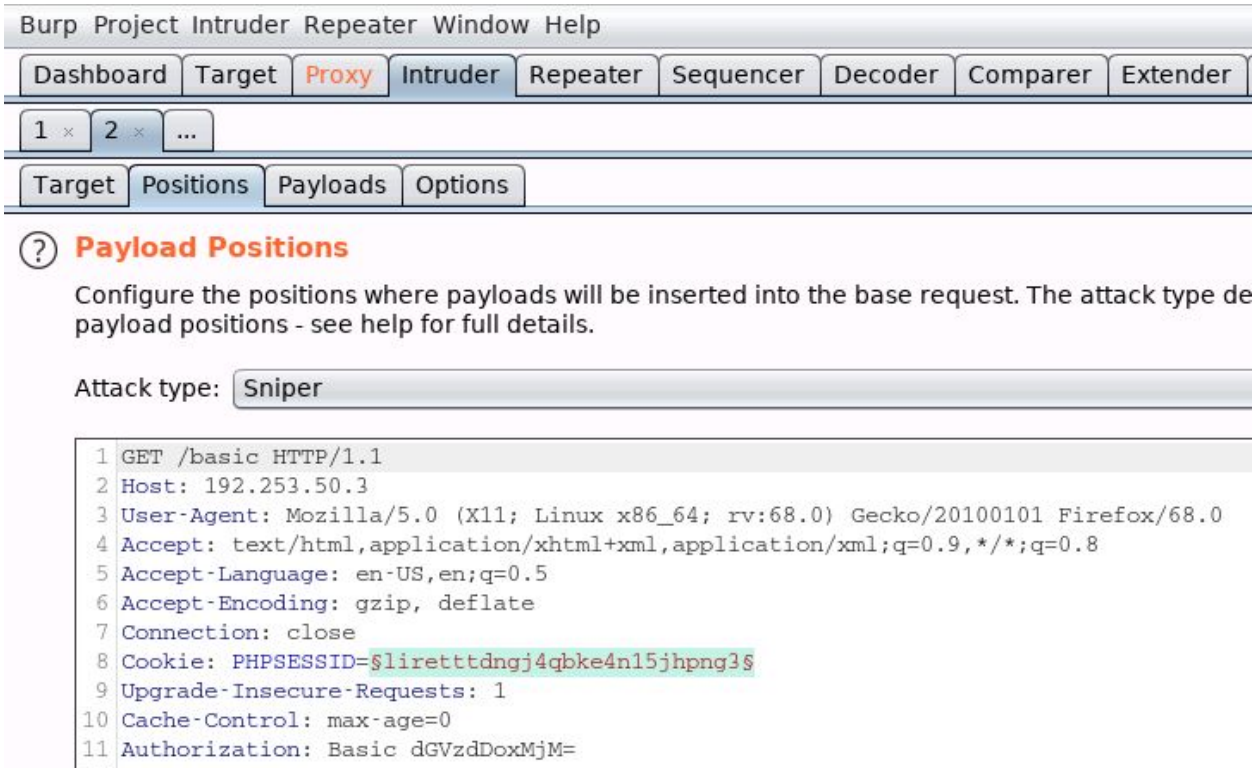
Send the intercepted request to intruder.



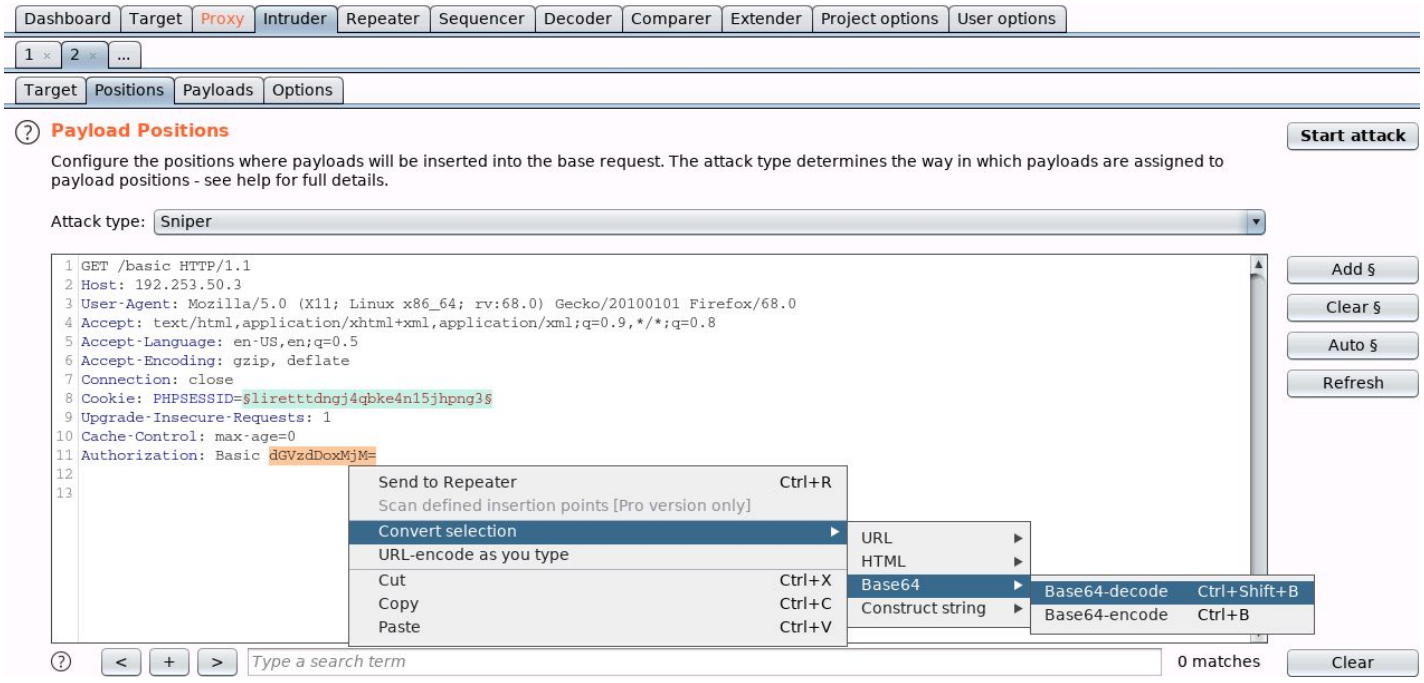
Navigate to the Intruder tab in Burp Suite:



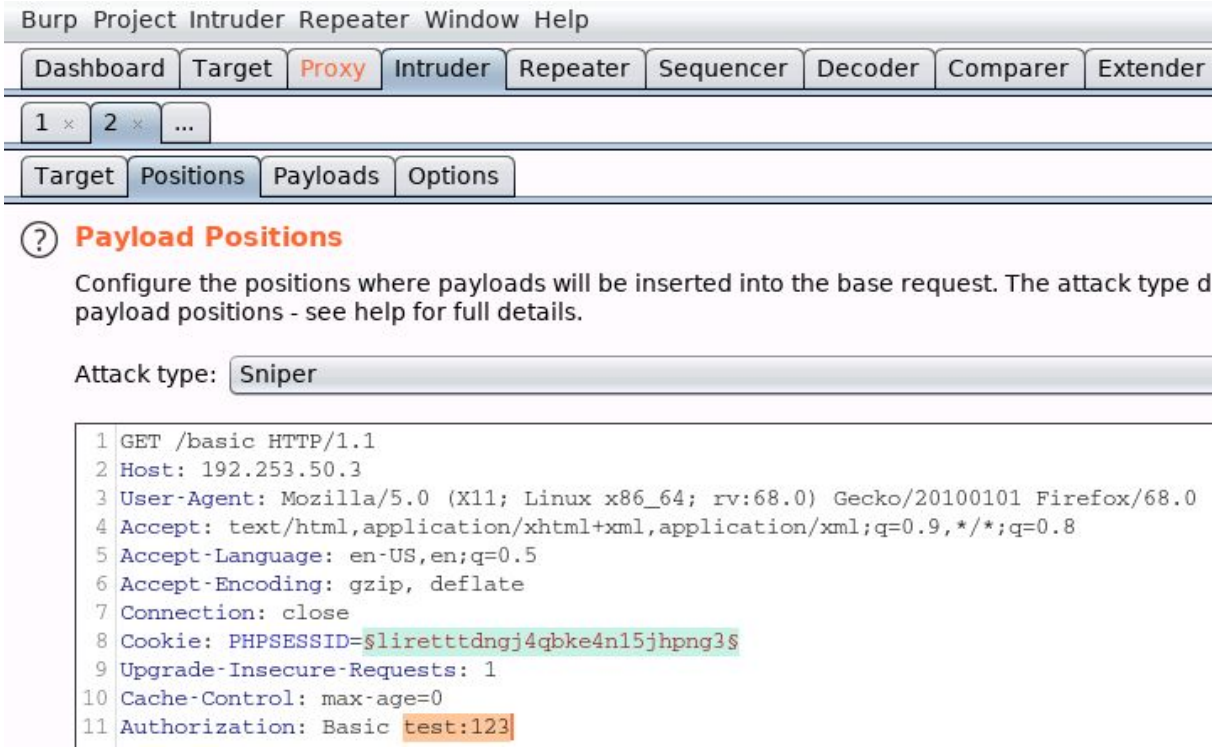
Navigate to the Positions sub-tab in the Intruder tab



Base64 decode the Basic Auth:

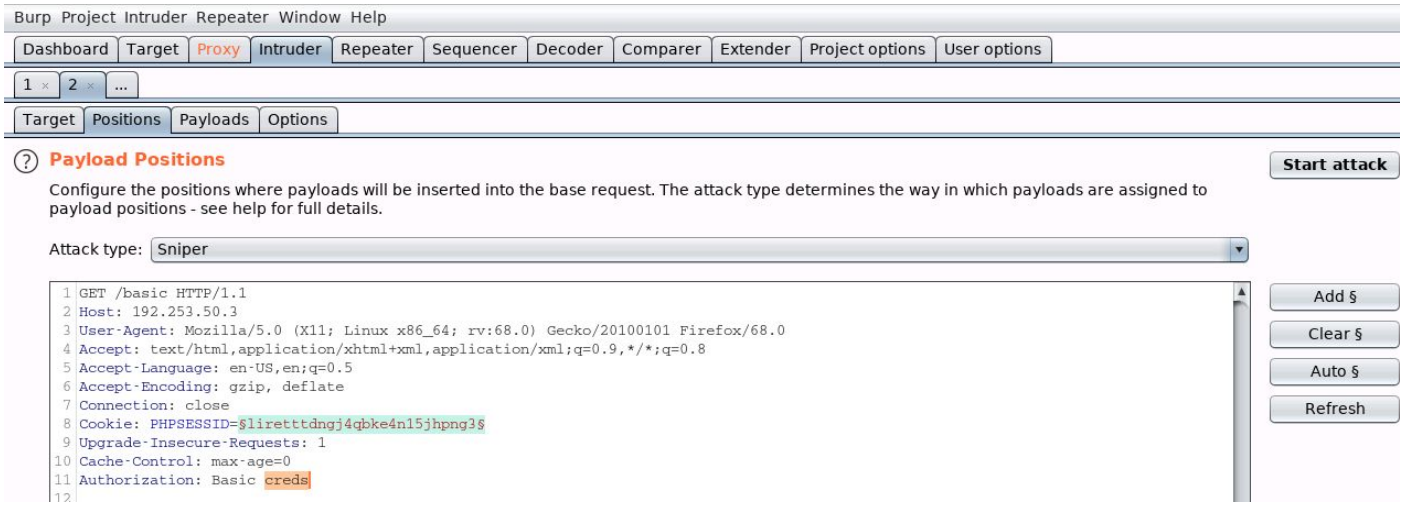


Right click and decode the base64 encoded basic auth:

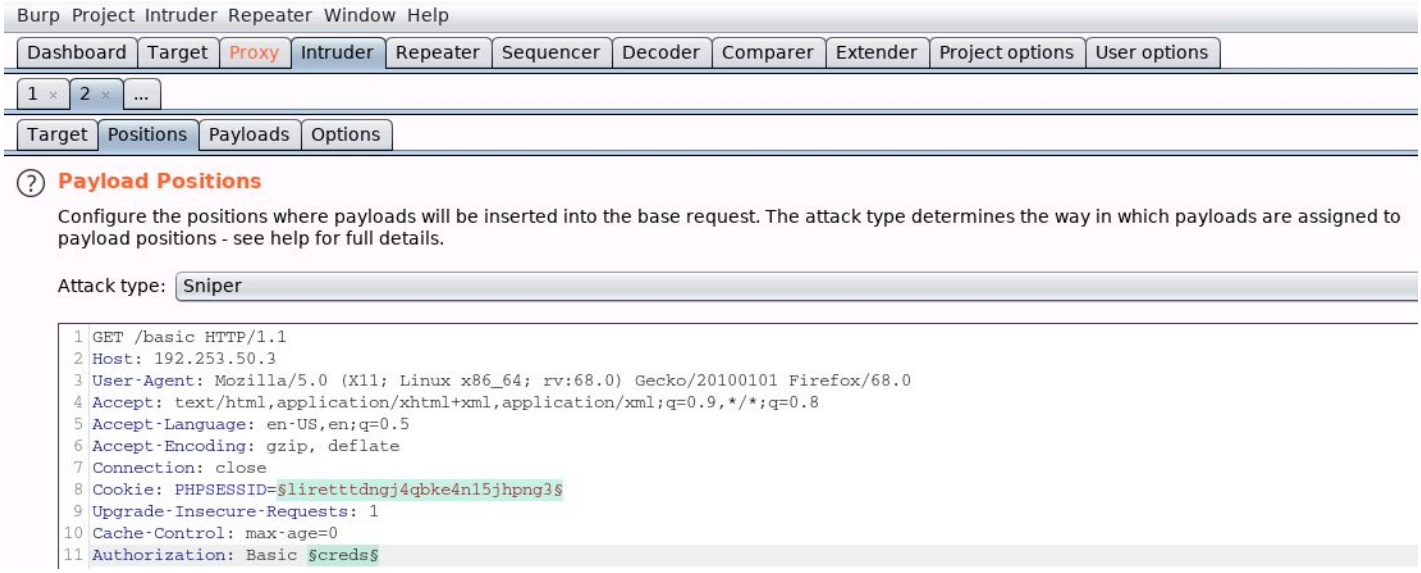


The credentials passed to the login prompt are shown.

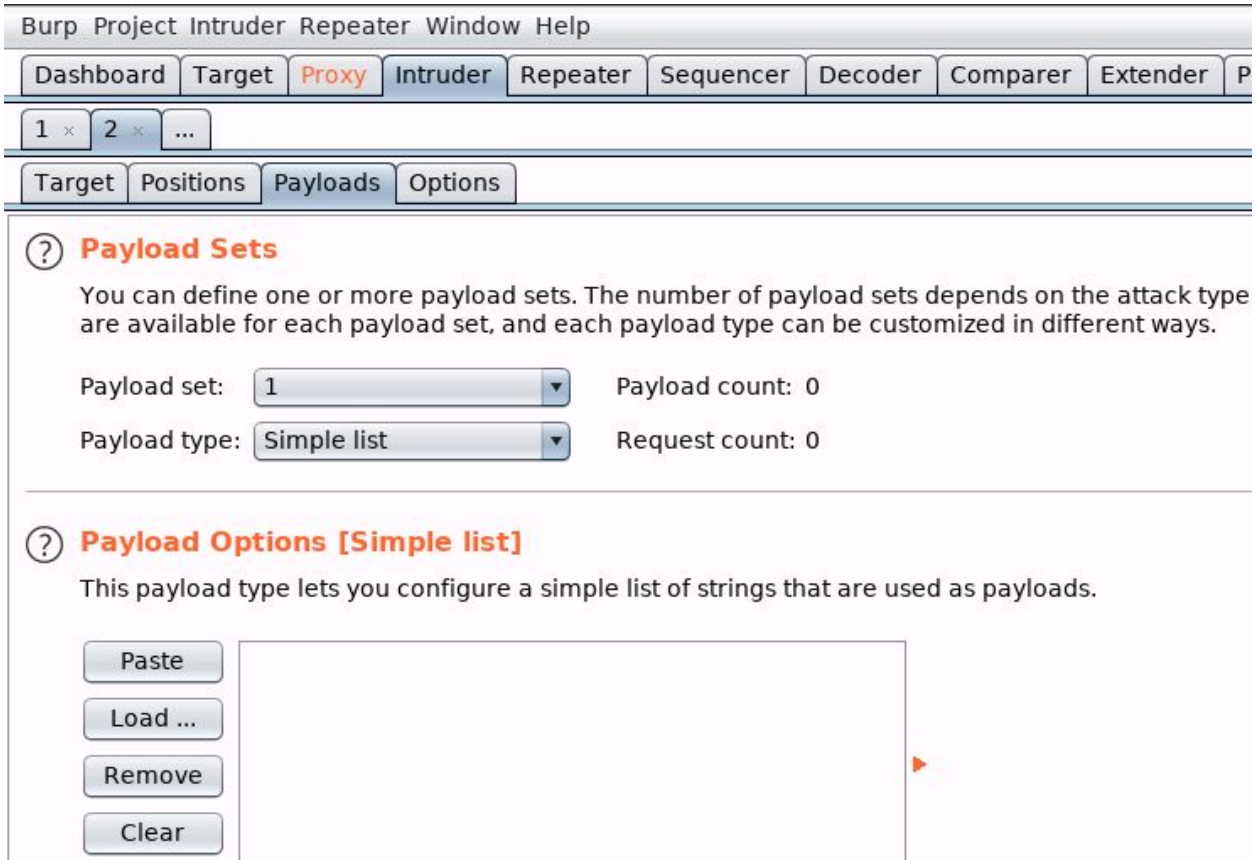
Replace the credentials with a parameter to be substituted:



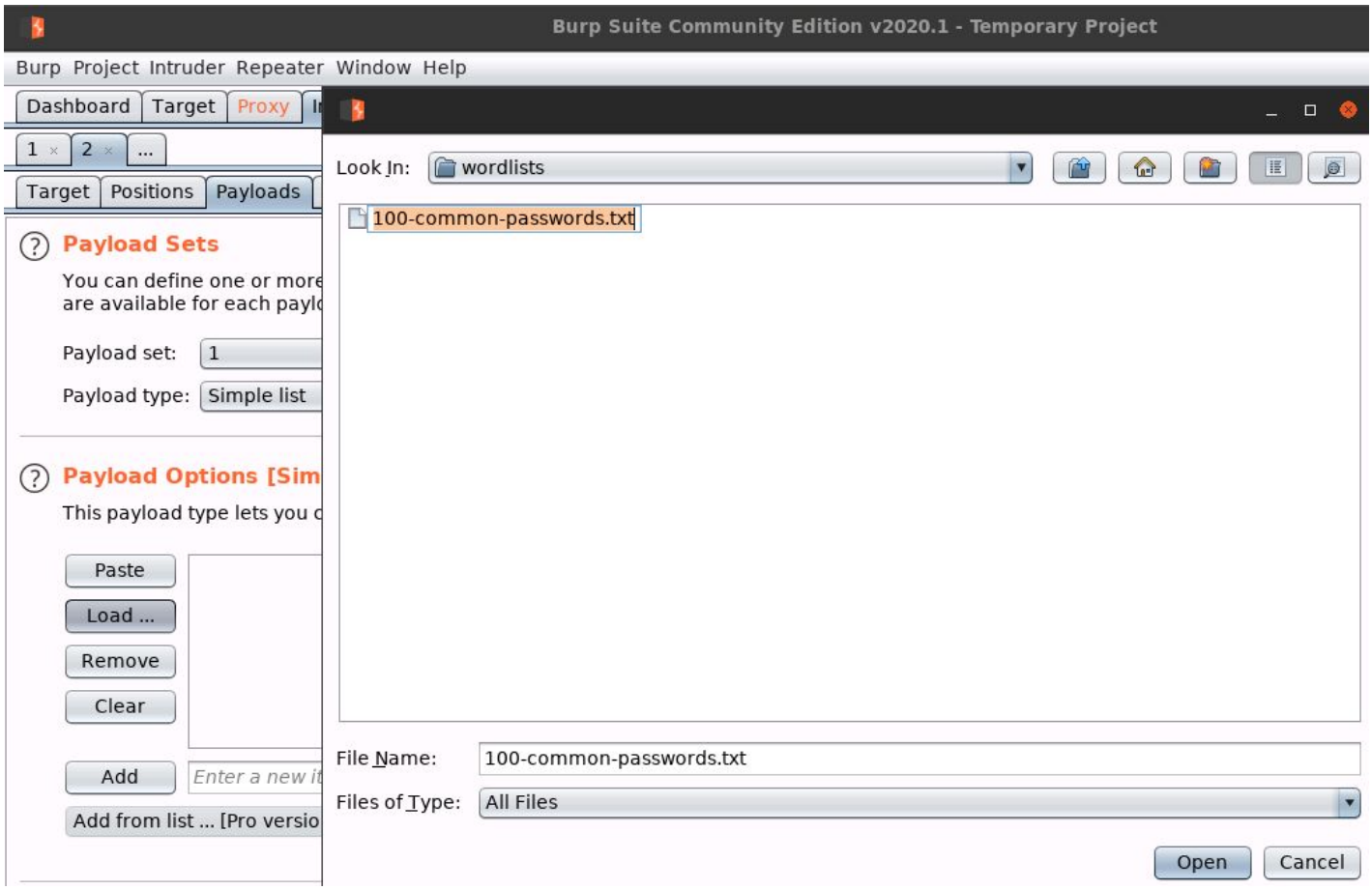
Click on the Add Button on the right side:



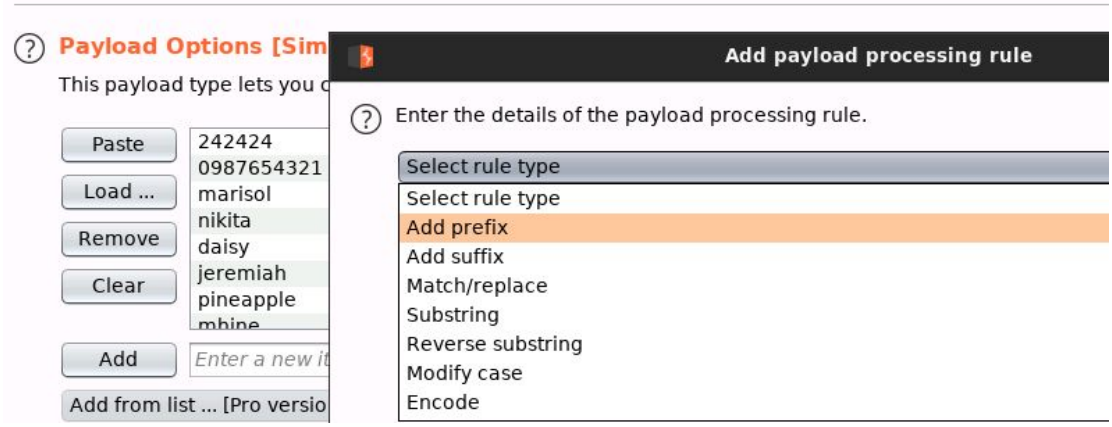
Navigate to the Payloads tab and load the 100-common-passwords.txt list



Click on the Load button to load the password list located at /root/Desktop/wordlists/100-common-passwords.txt:

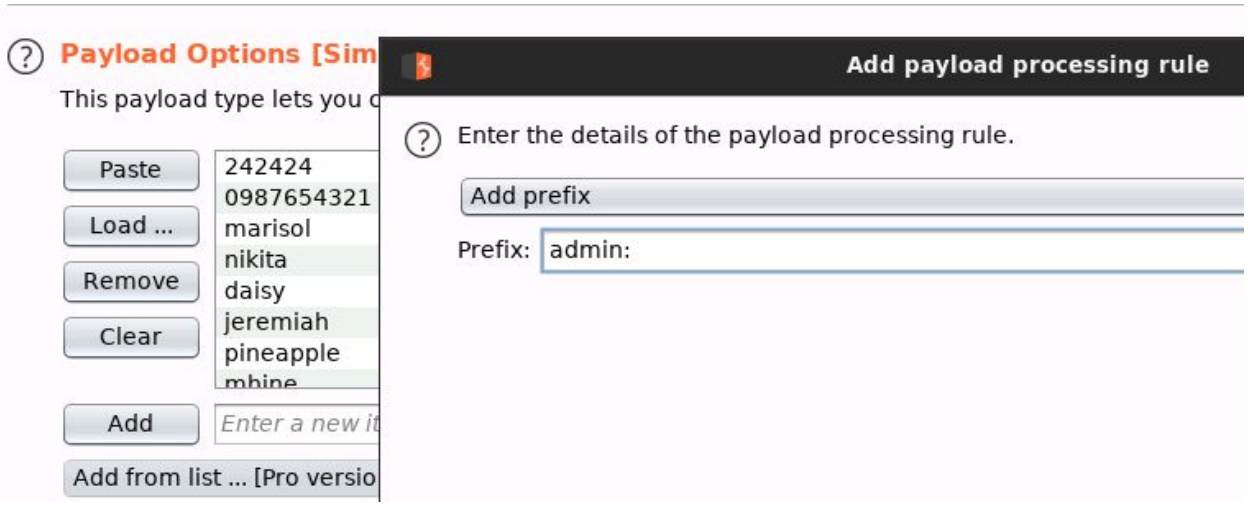


In the Payload Processing section click on the “Add” button.



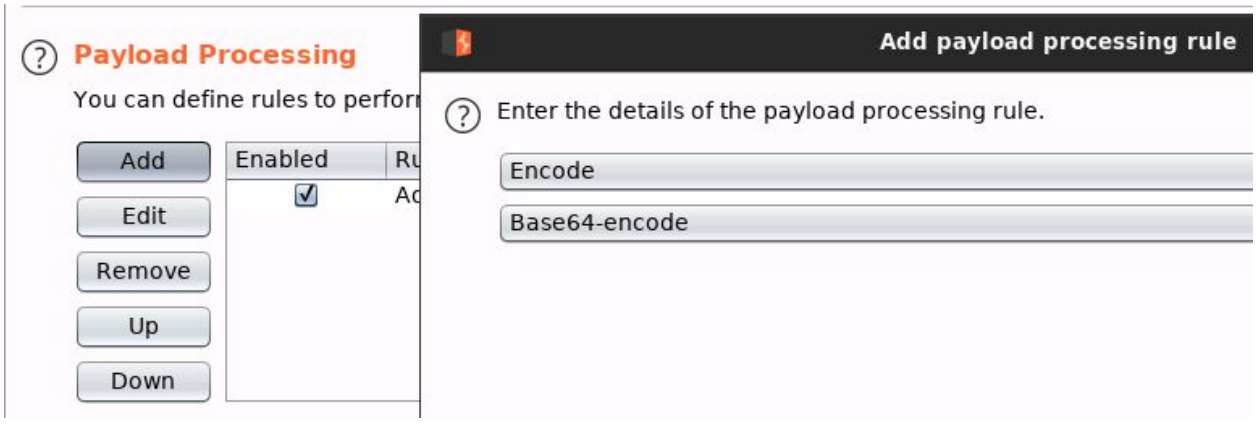
Select “Add Prefix”

Set the Prefix to “admin:”:



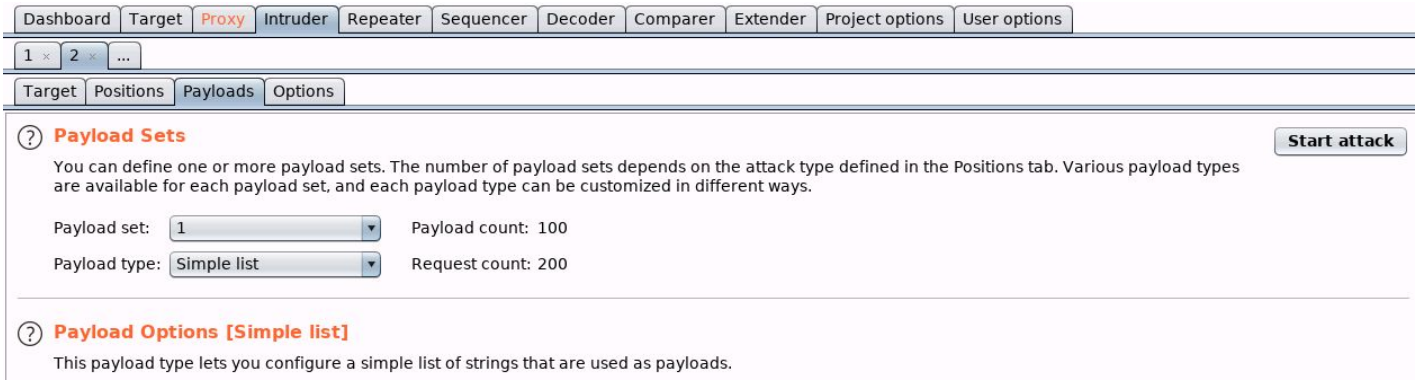
So, now “admin:” would be appended to each password from the list.

Add another Payload Processing option to encode the payload to base64:

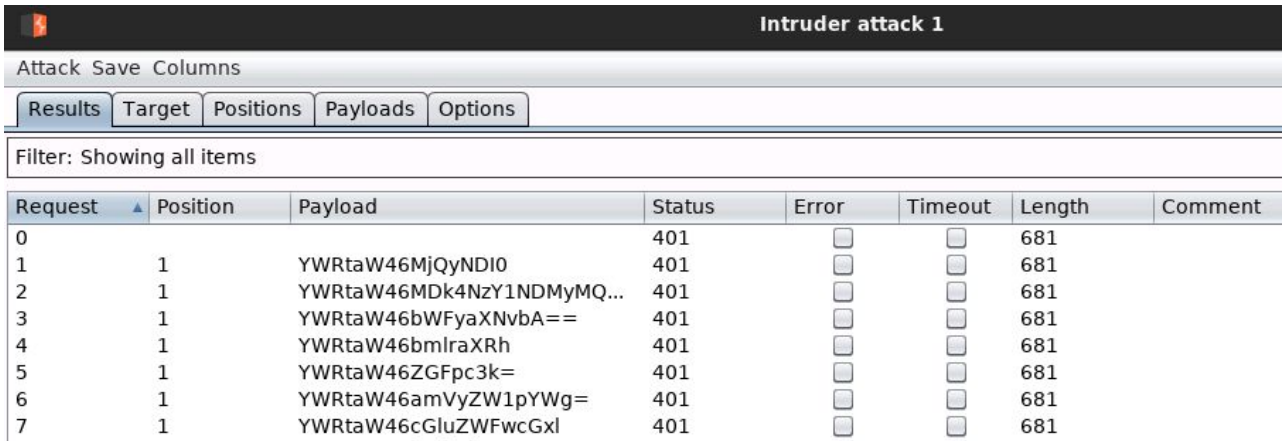


Select the Encode Rule as Base64-encode

Next, click on the “Start Attack” button:

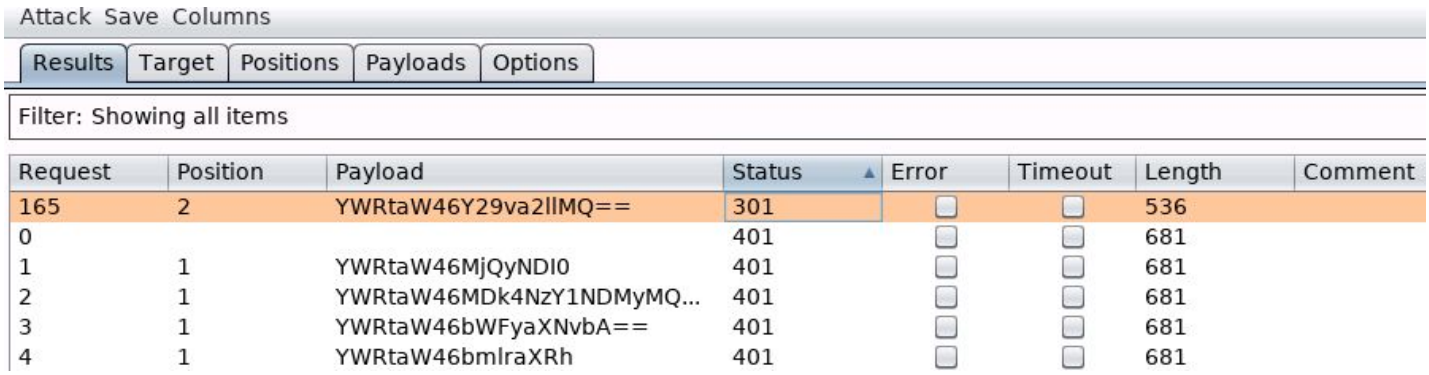


This would start the dictionary attack against the target webapp:



Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			401			681	
1	1	YWRtaW46MjQyNDI0	401			681	
2	1	YWRtaW46MDk4NzY1NDMyMQ...	401			681	
3	1	YWRtaW46bWFyaXNvbA==	401			681	
4	1	YWRtaW46bmlraXRh	401			681	
5	1	YWRtaW46ZGFpc3k=	401			681	
6	1	YWRtaW46amVyZW1pYWg=	401			681	
7	1	YWRtaW46cGluZWFwcGxl	401			681	

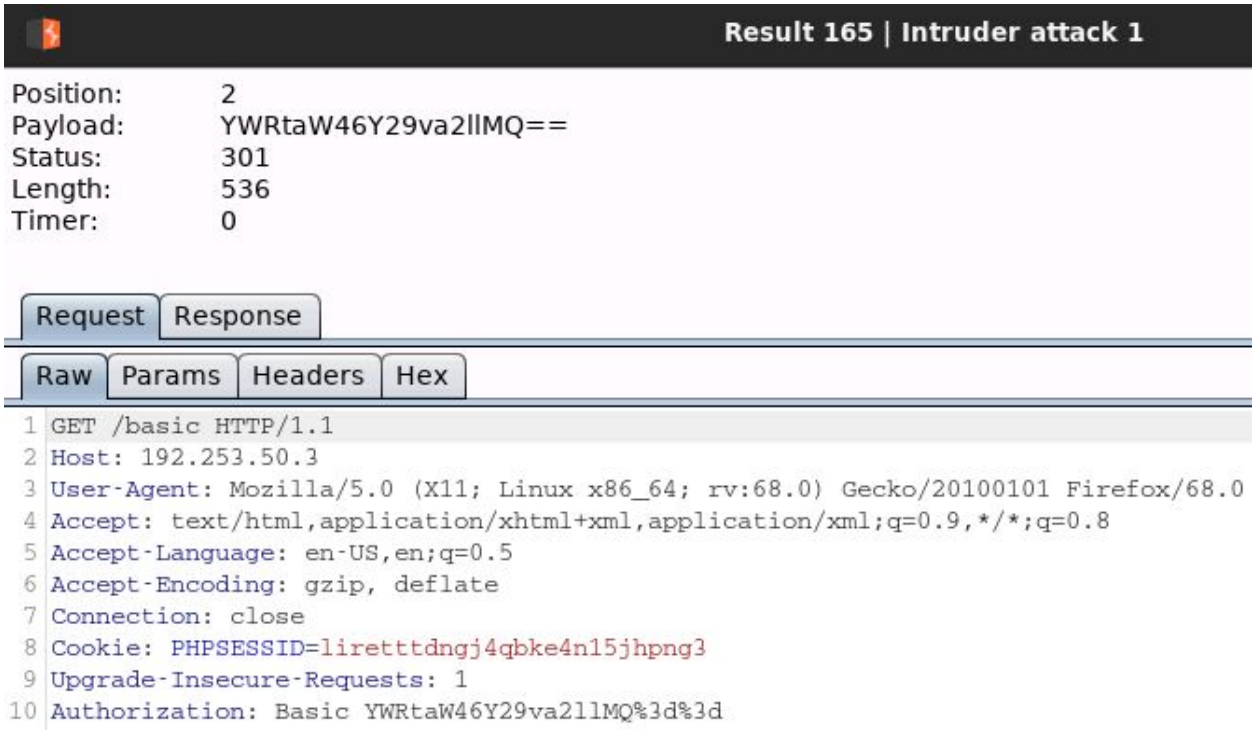
Check the Status codes of the requests and check the payload for the request with a different status code:

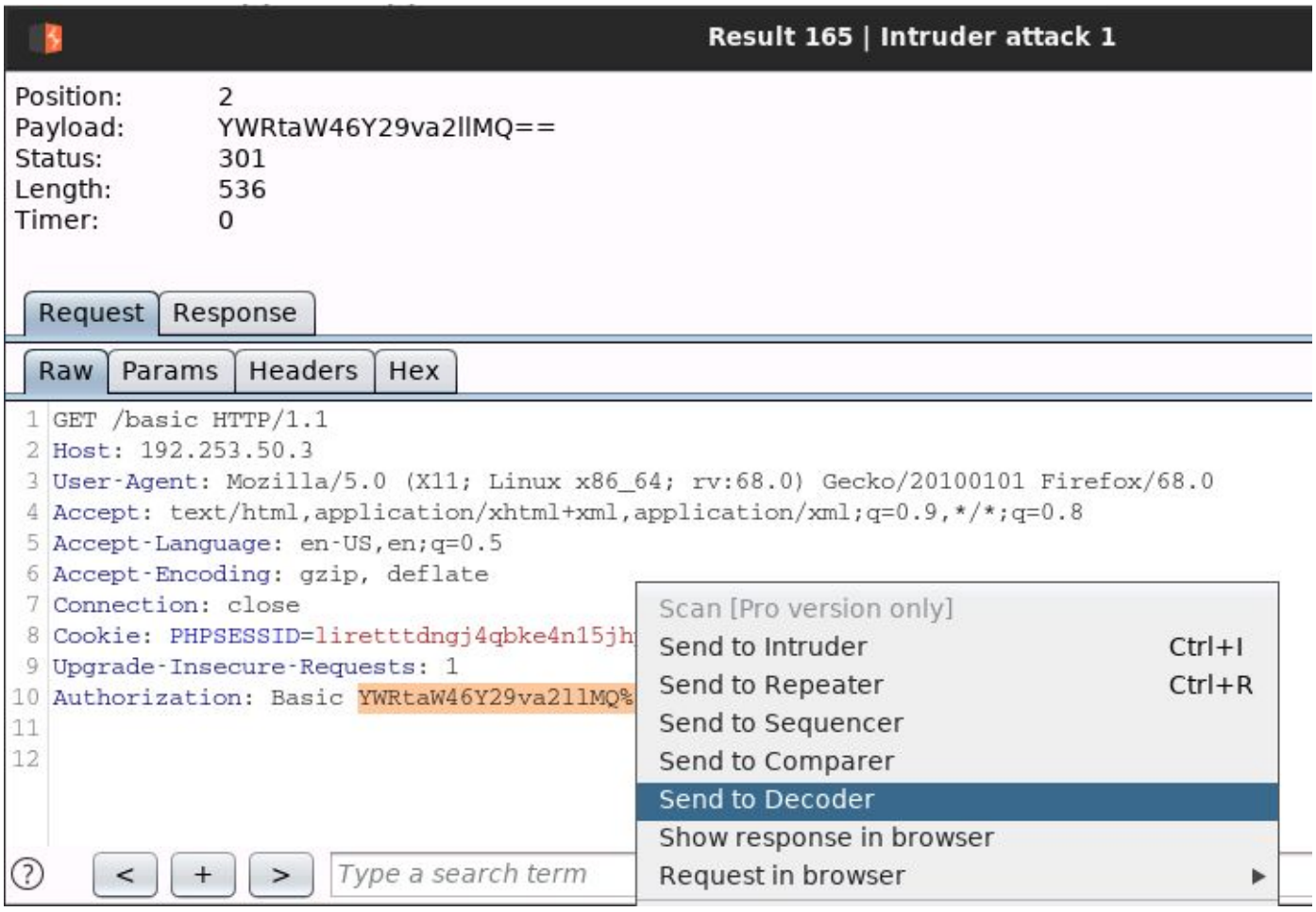


Request	Position	Payload	Status	Error	Timeout	Length	Comment
165	2	YWRtaW46Y29va2llMQ==	301	☐	☐	536	
0			401	☐	☐	681	
1	1	YWRtaW46MjQyNDI0	401	☐	☐	681	
2	1	YWRtaW46MDk4NzY1NDMyMQ...	401	☐	☐	681	
3	1	YWRtaW46bWFyaXNvbA==	401	☐	☐	681	
4	1	YWRtaW46bmlraXRh	401	☐	☐	681	

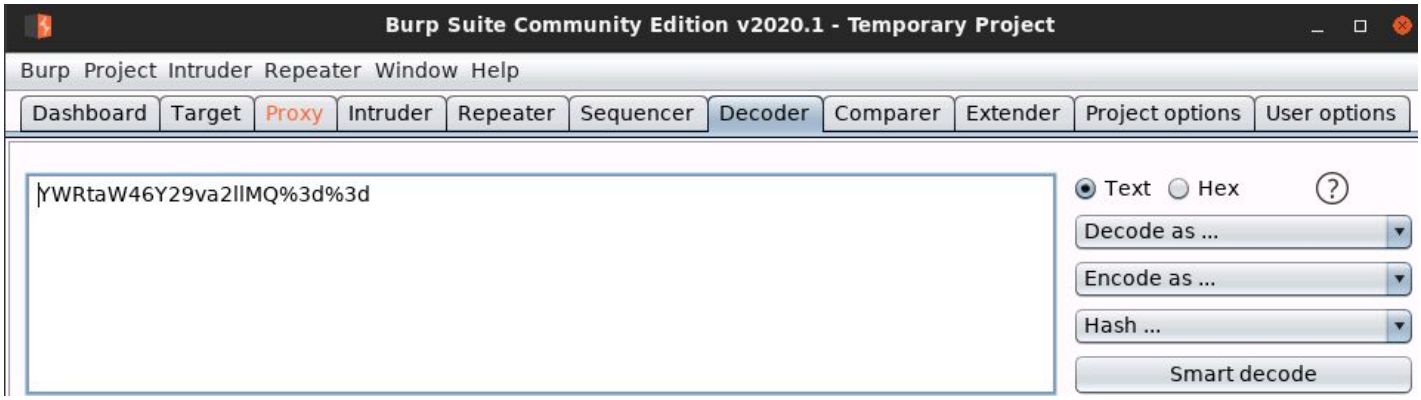
Notice that there is one request with the status code of 301.

Double click on the request entry:

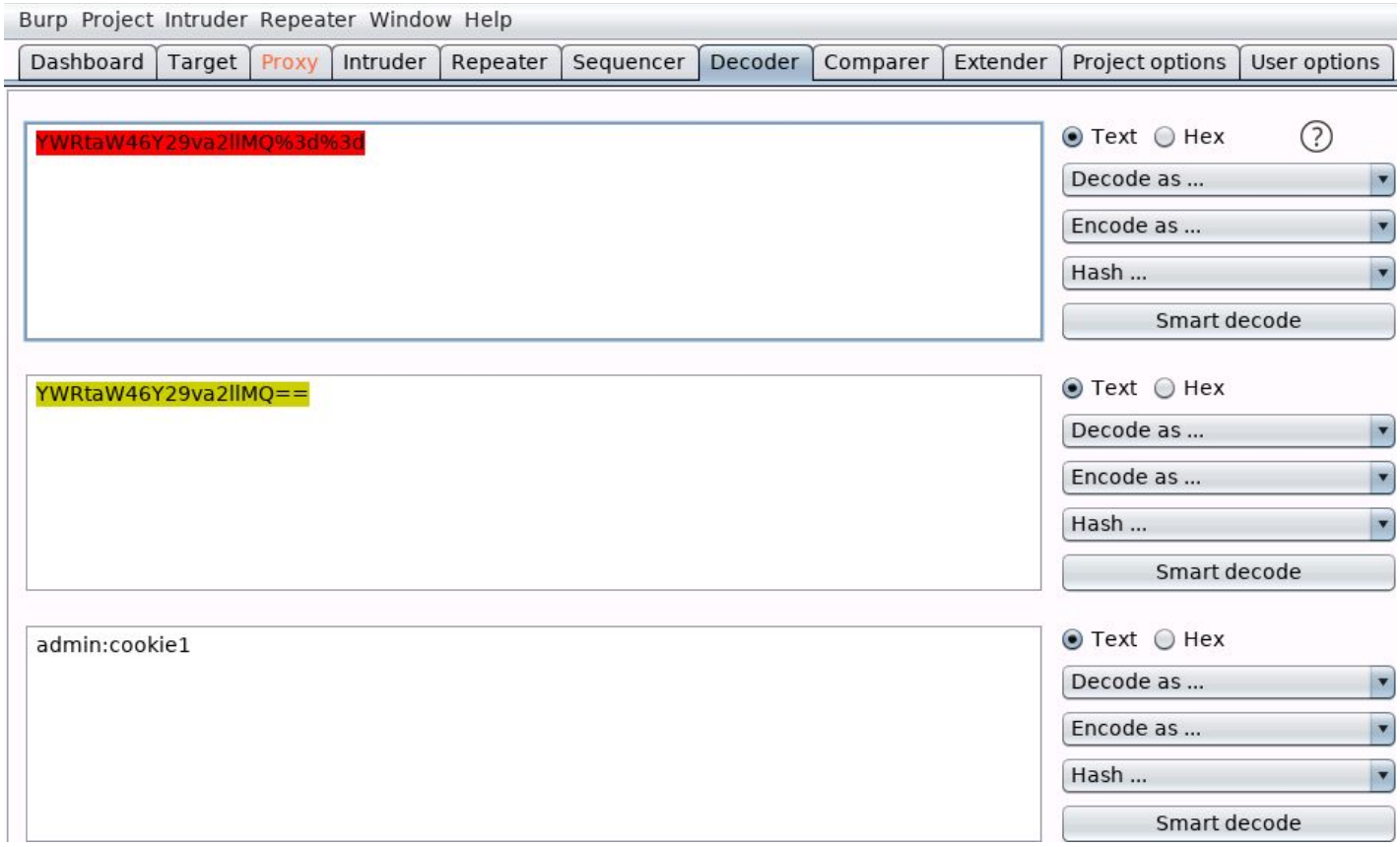




Select the credentials in the Authorization header field and send them to the Decoder tab.

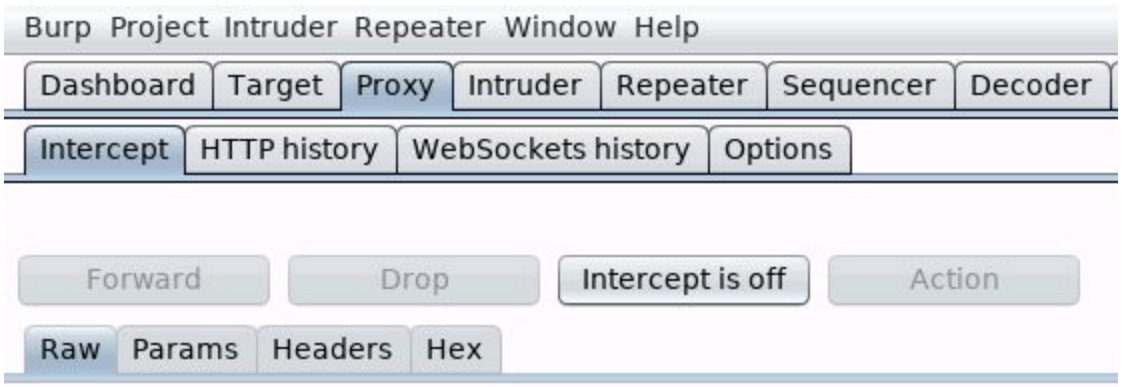


URL decode the credentials followed by base64-decode:

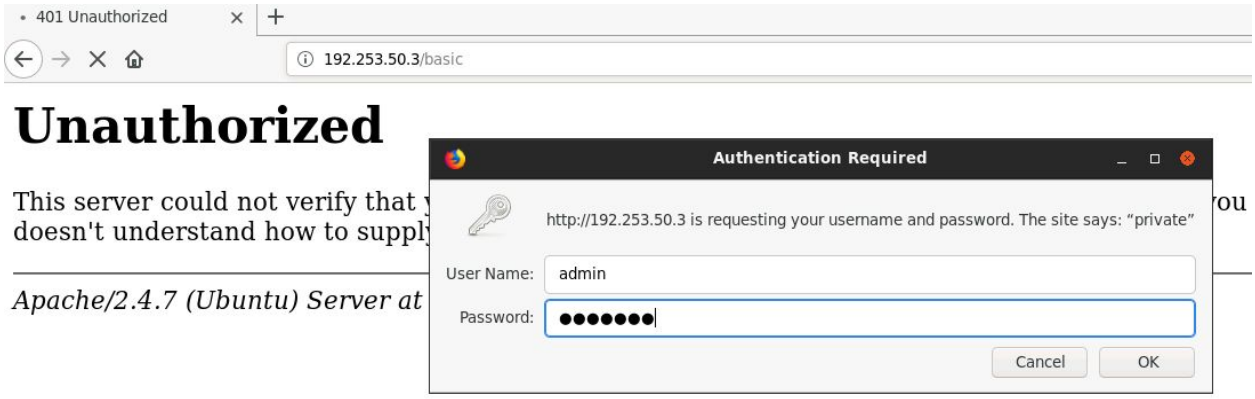


Username: admin
Password: cookie1

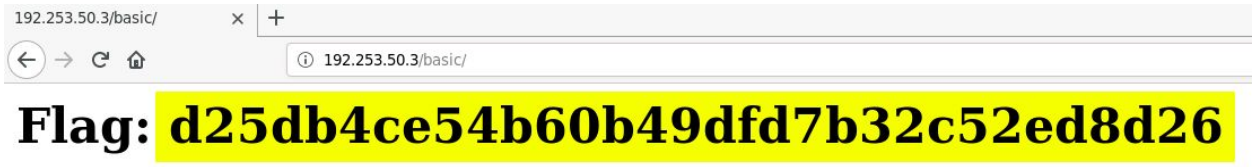
Now, turn off the intercept mode in Burp Suite:



Pass the credentials to the application:



Click OK



The login was successful and the Flag is displayed:

Flag: d25db4ce54b60b49dfd7b32c52ed8d26

References:

1. Burp Suite (https://portswigger.net/support/burp-suite-tools)