

[illegible]

Name	Attacking Basic Auth with Burp Suite
URL	<a href="https://attackdefense.com/challengedetails?cid=1896">https://attackdefense.com/challengedetails?cid=1896</a>
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

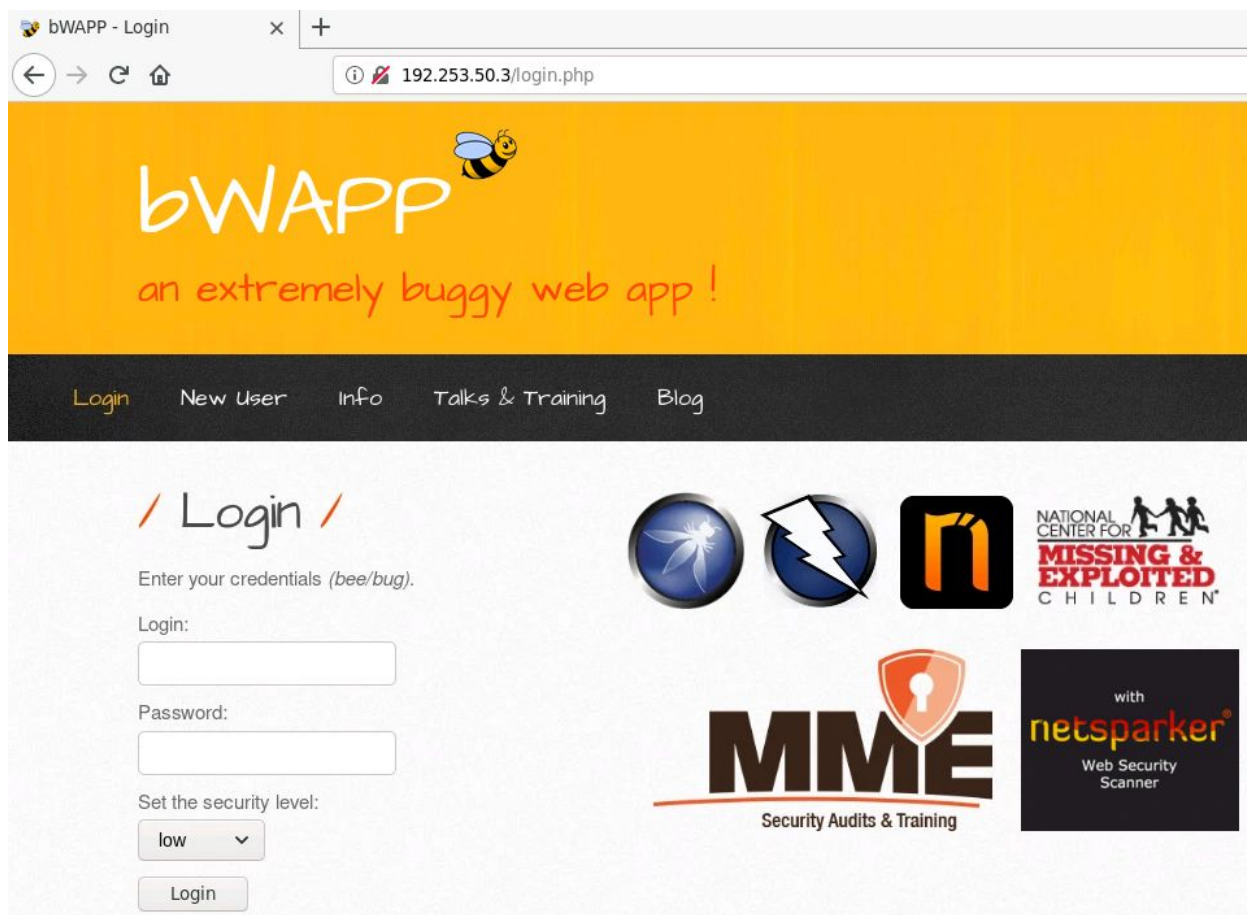
```
root@attackdefense:~# nmap 192.253.50.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 18:29 IST
Nmap scan report for target-1 (192.253.50.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:FD:32:03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

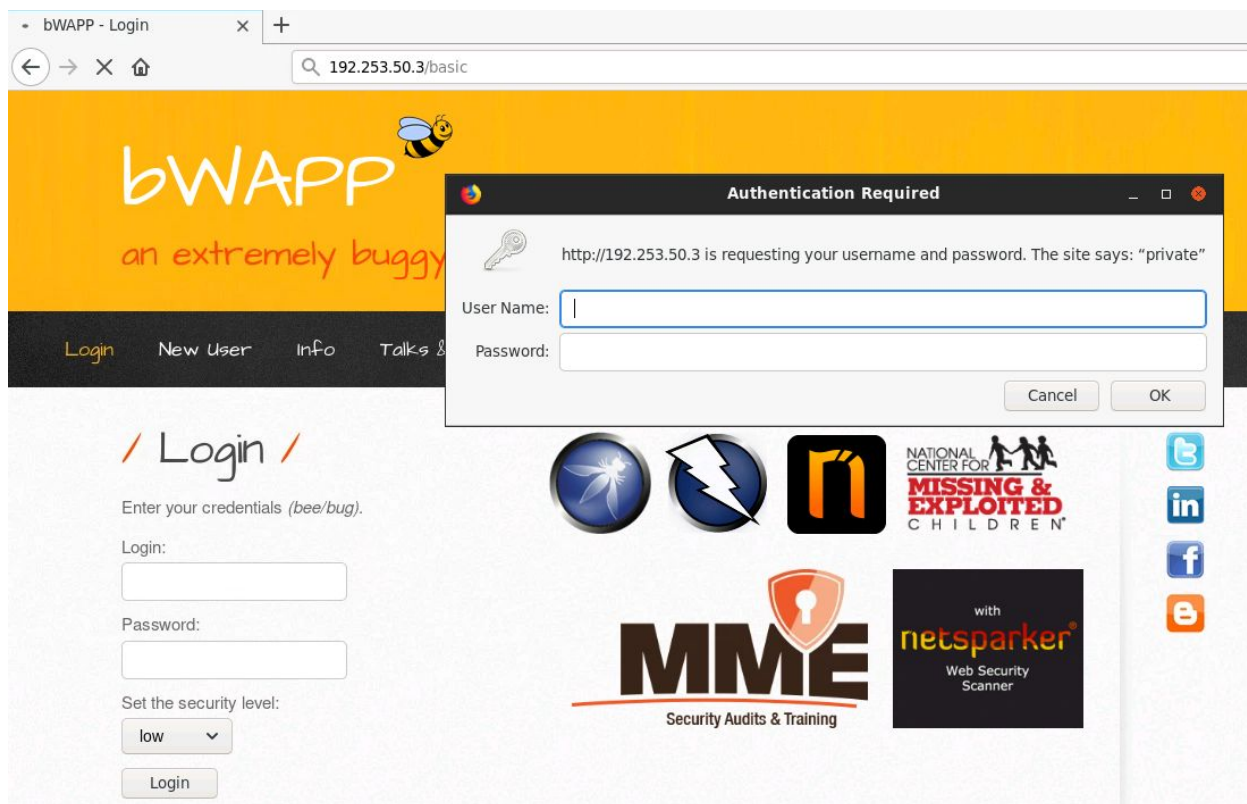


bWAPP application is hosted on the target machine.

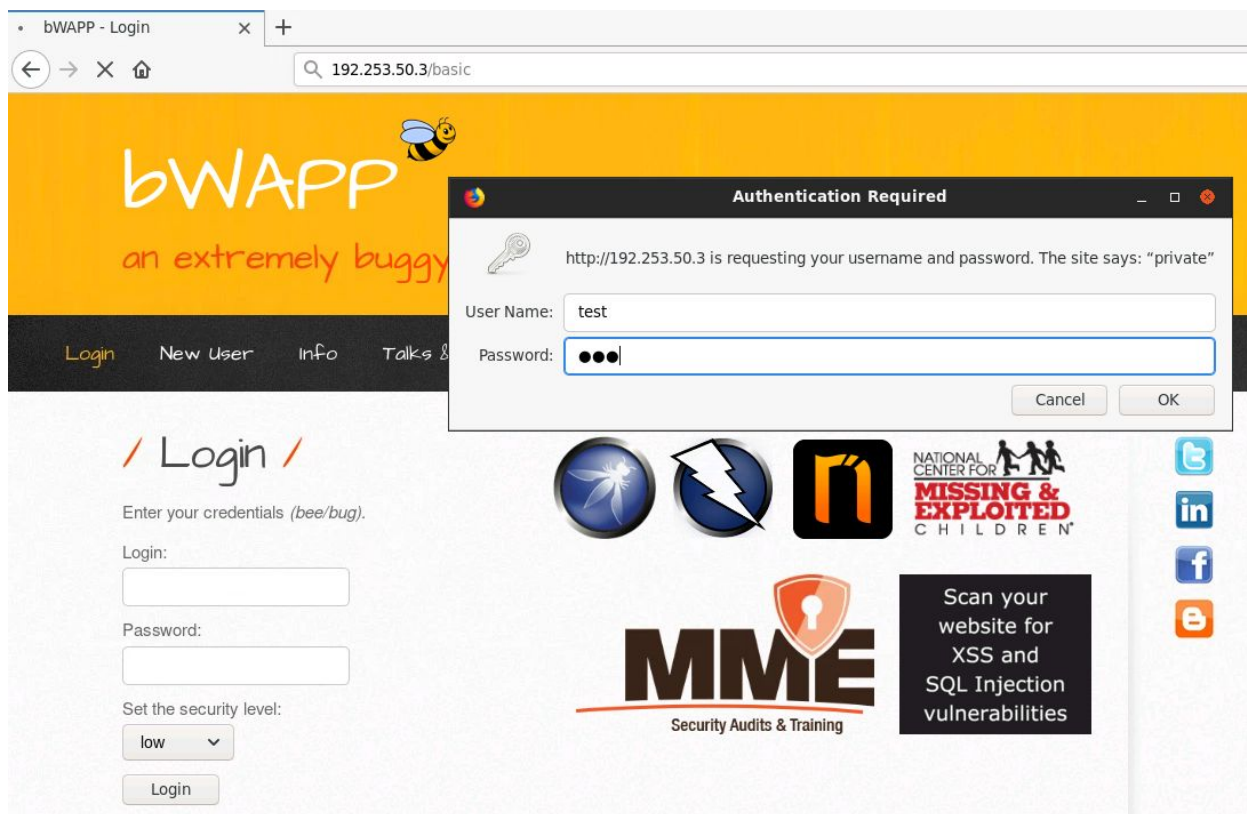
Access the /basic directory:

**URL:** http://192.253.50.3/basic

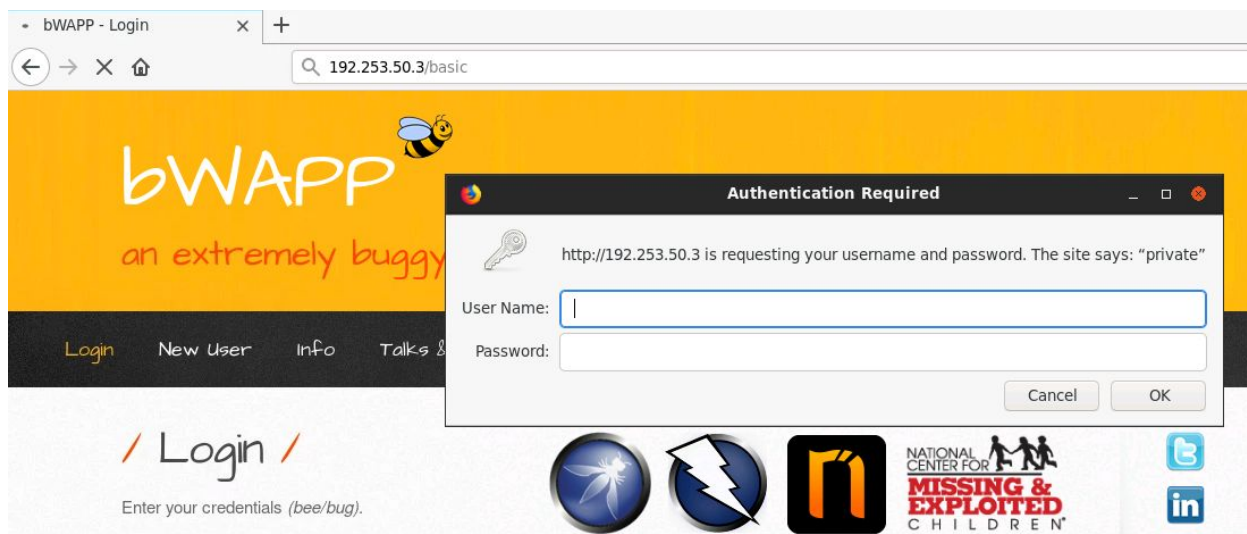




Enter some random username - password combination.



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



Click on the "Cancel" button:

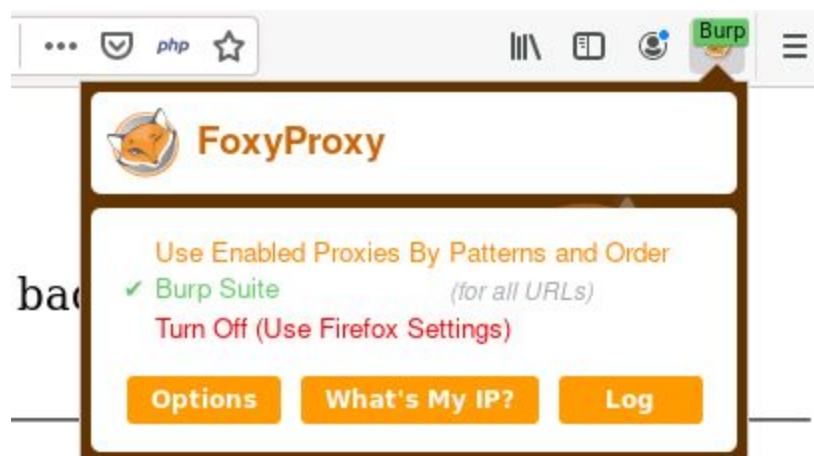


### Step 3: Using Burp Suite to crack the Basic Auth:

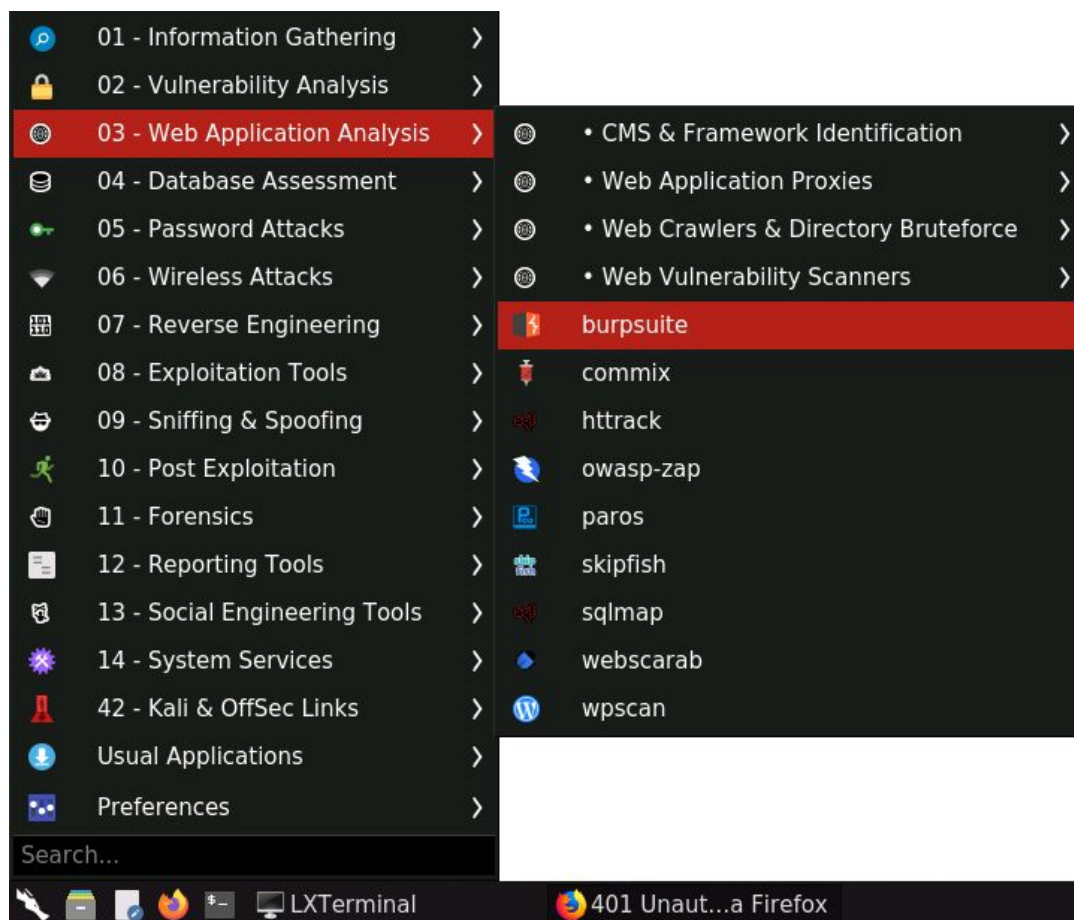
Click on the FoxyProxy plugin icon on the top-right of the browser.



Select Burp Suite option from the list:



Start Burp Suite:





**Burp Suite Community Edition v2020.1**

② 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.*

☒ **Temporary project**

---

☐ **New project on disk**

Name:

File:

---

☐ **Open existing project**

Name	File
------	------

File:

☒ Pause Automated Tasks

Click Next

**Burp Suite Community Edition v2020.1**

② Select the configuration that you would like to load for this project.

☒ **Use Burp defaults**

---

☐ **Use options saved with project**

---

☐ **Load from configuration file**

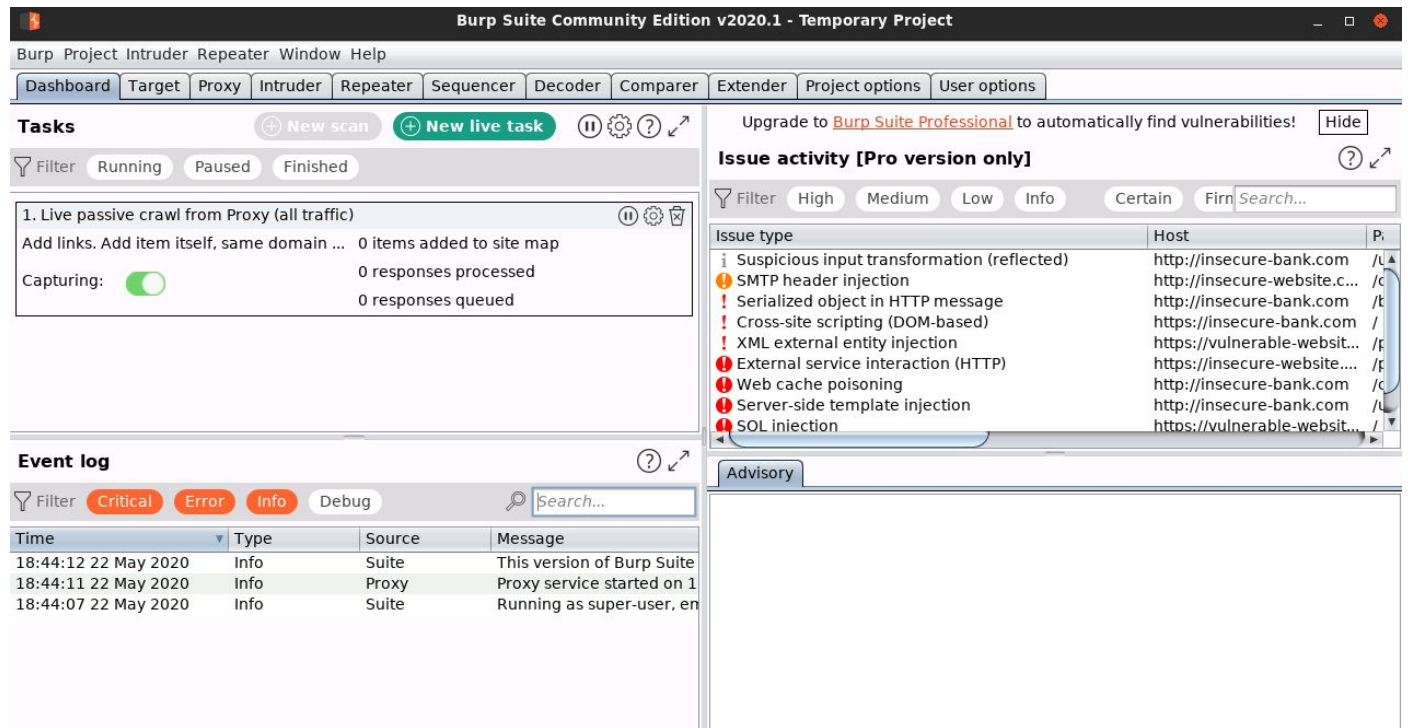
File
------

File:

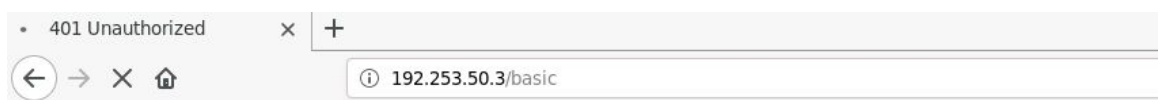
☐ Default to the above in future

☐ Disable extensions

Click on Start Burp



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

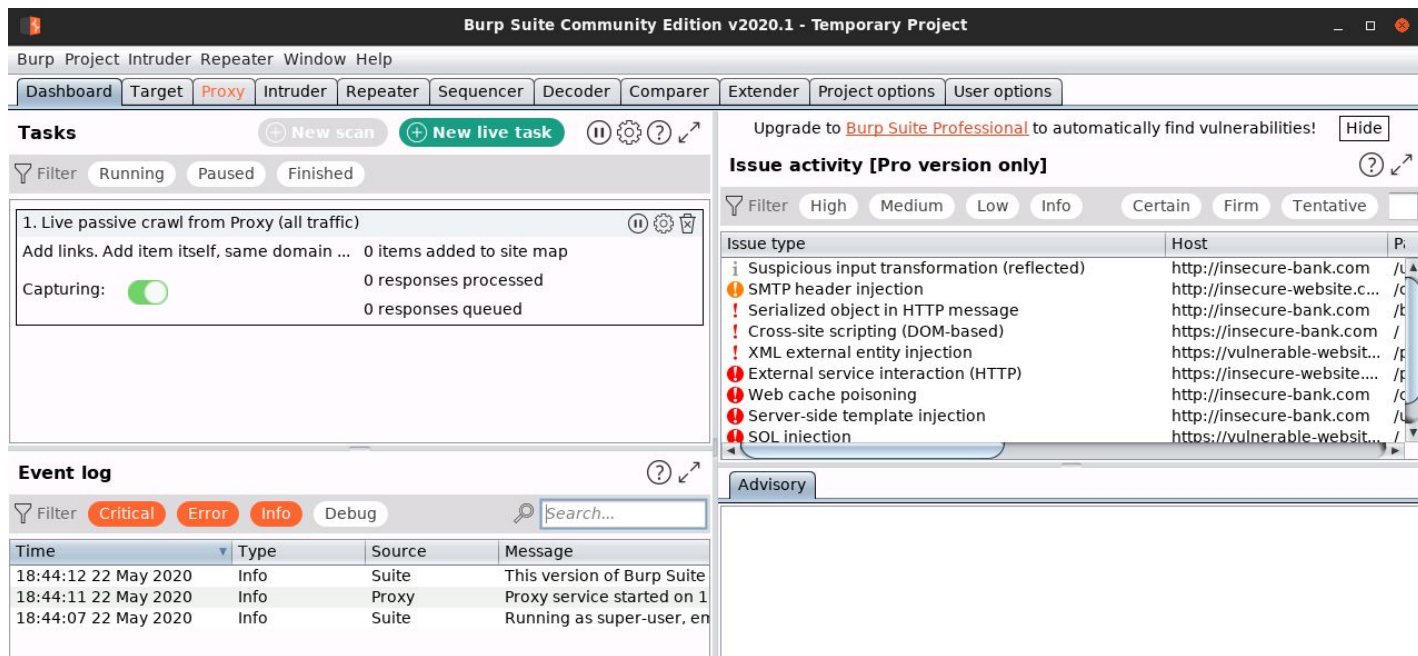


## Unauthorized

This server could not verify that you are authorized to access the document doesn't understand how to supply the credentials required.

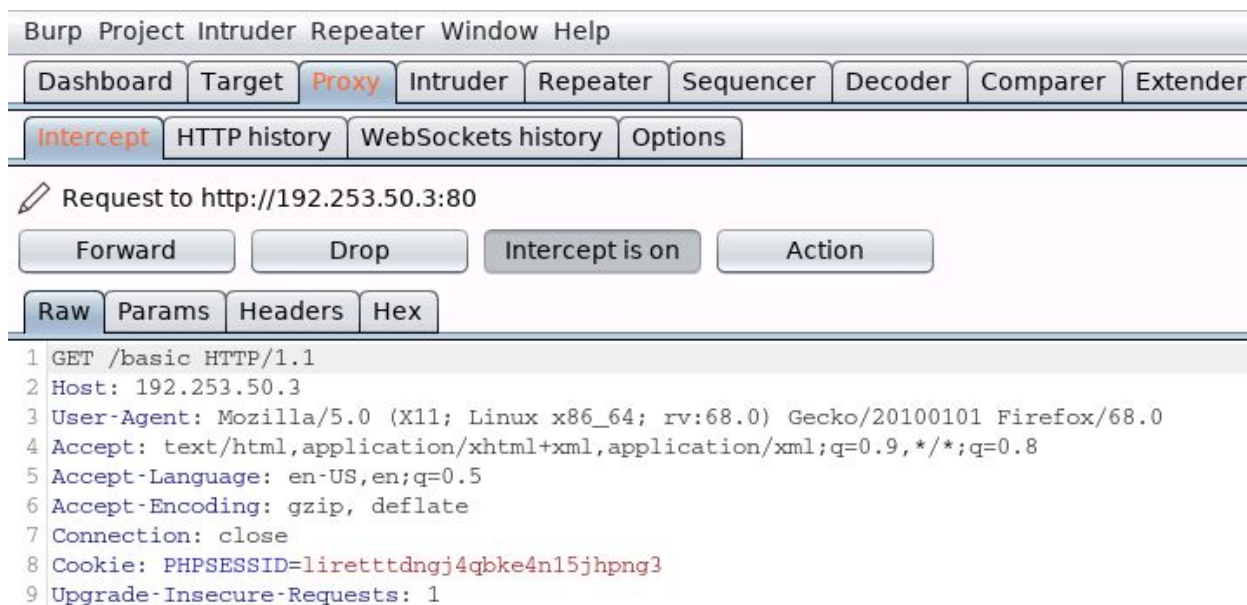
*Apache/2.4.7 (Ubuntu) Server at 192.253.50.3 Port 80*

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



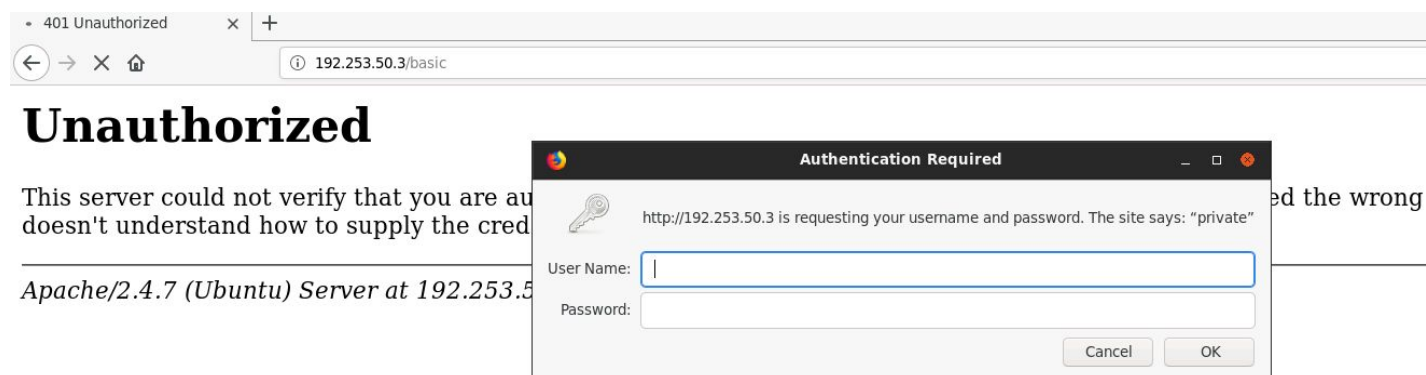
Notice that the Proxy button in Burp Suite lit up (orange).

Click on the Proxy button



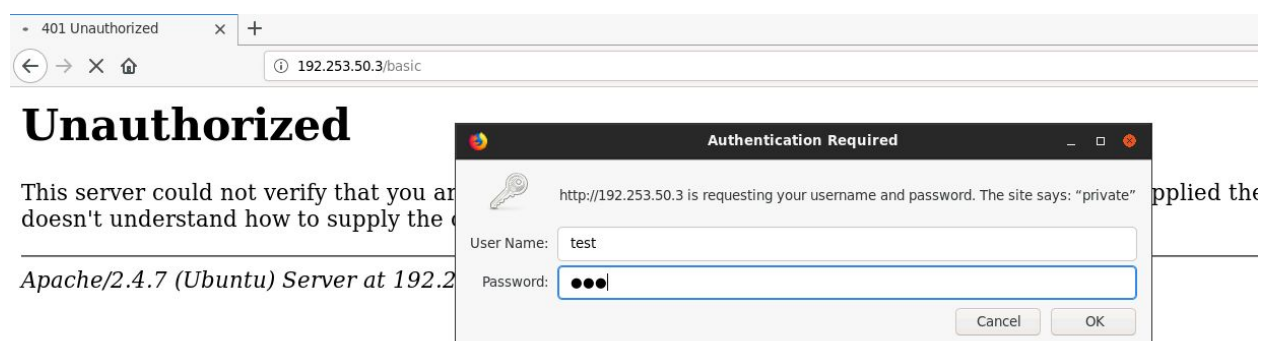
Notice the request being made by the browser.

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



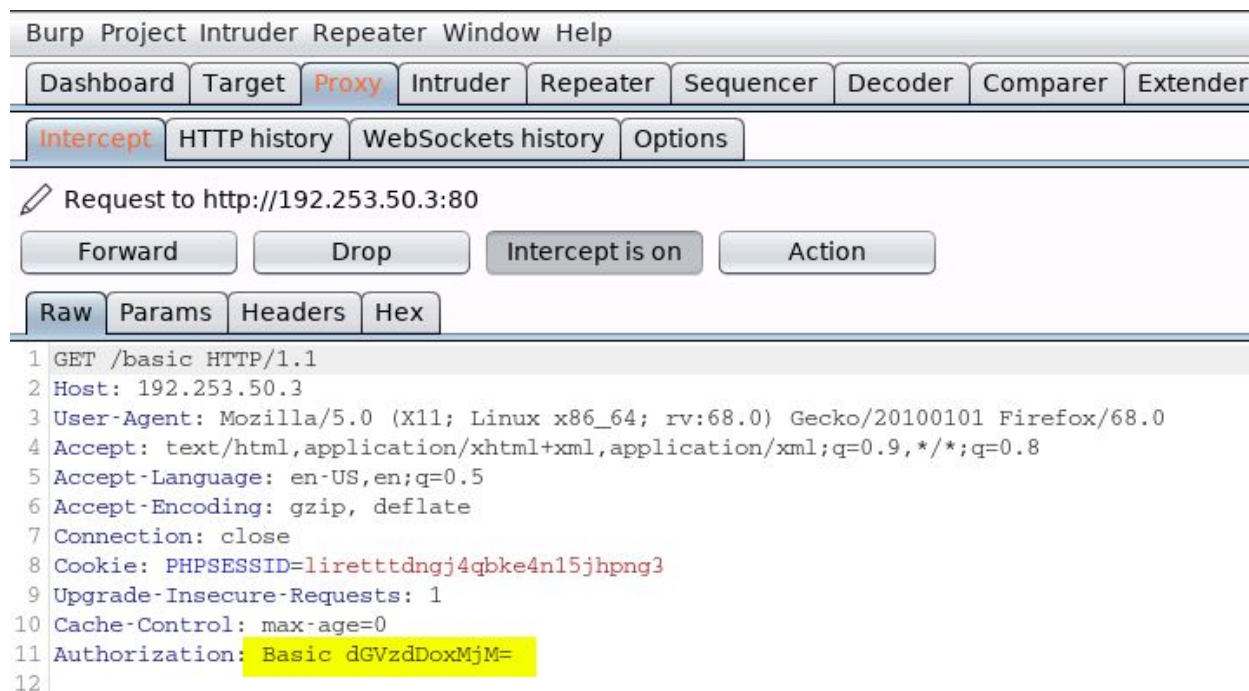
Notice that the application is prompting for credentials.

Enter some random credentials and press Ok.



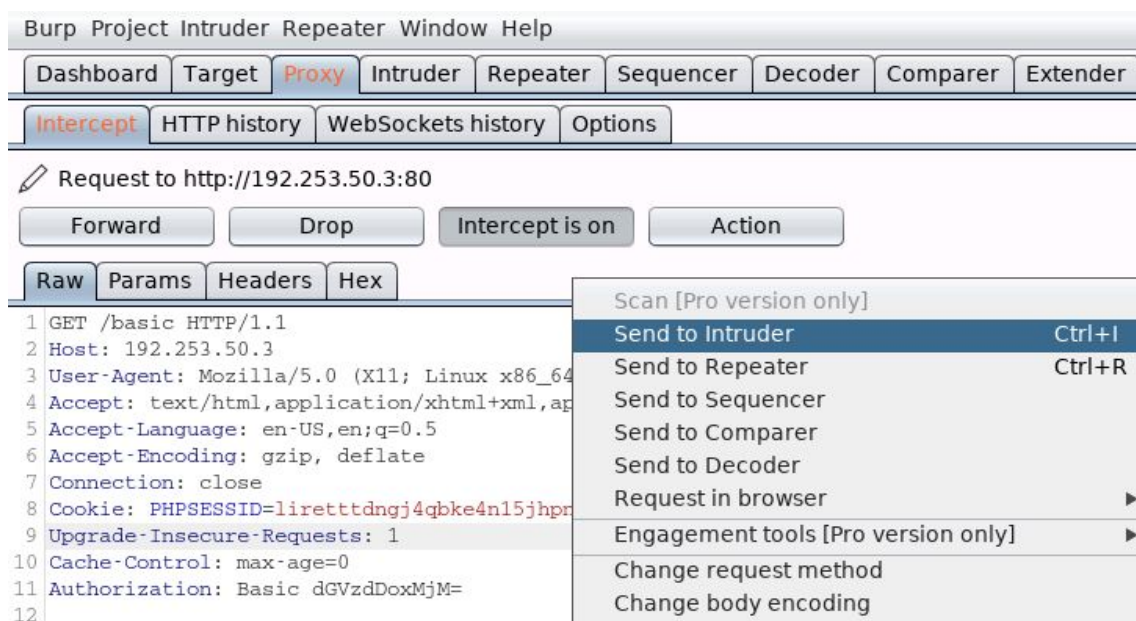
Intercepted request:



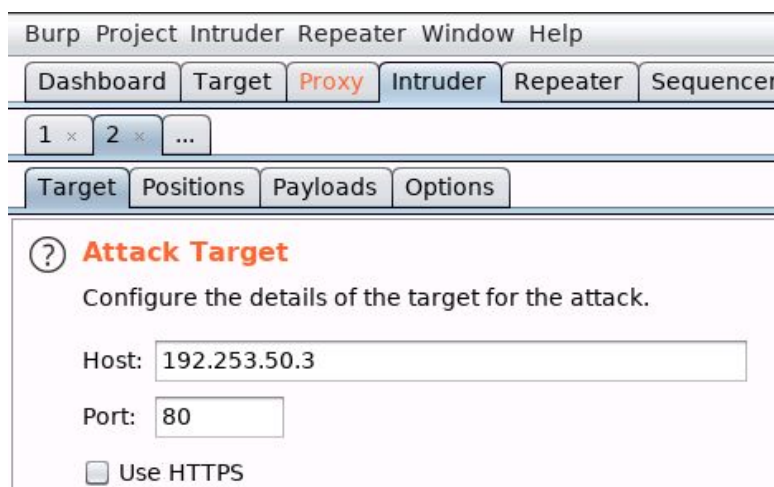


Notice the Authorization header. The “/basic” directory uses Basic Auth.

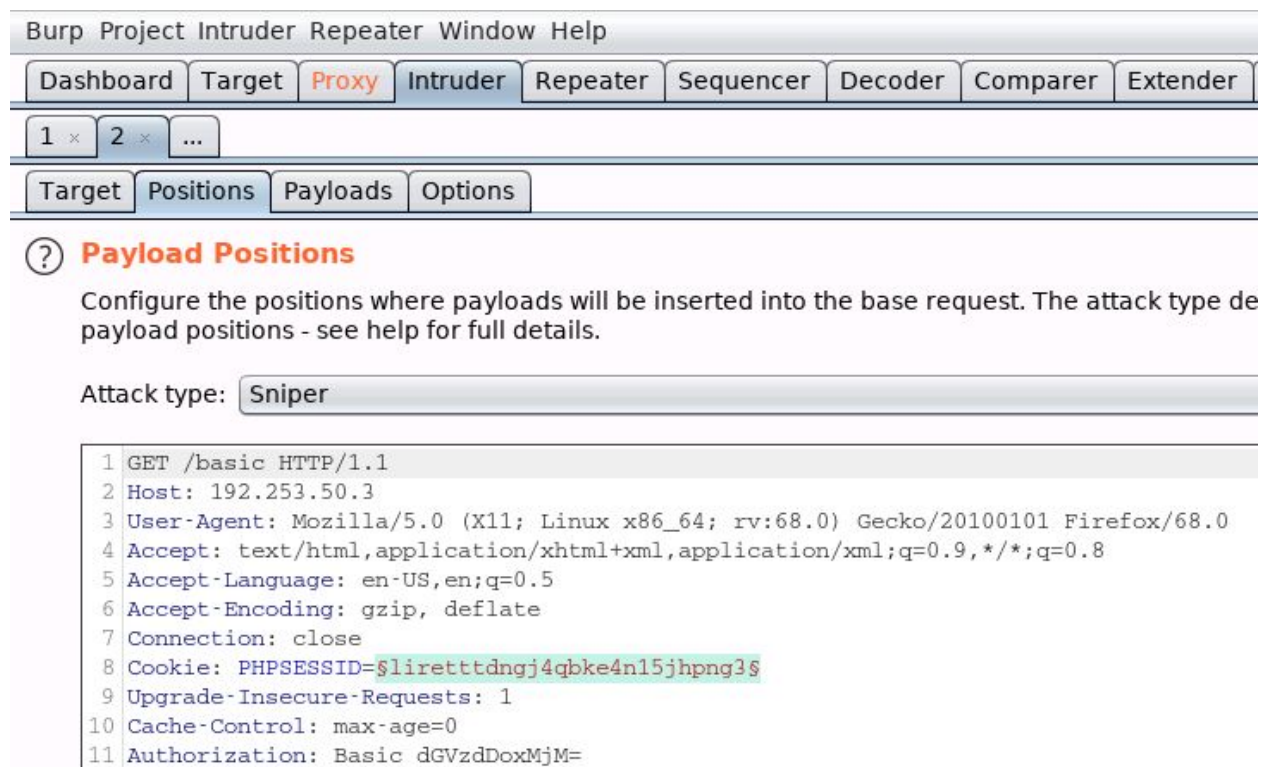
Send the intercepted request to intruder.



Navigate to the Intruder tab in Burp Suite:



Navigate to the Positions sub-tab in the Intruder tab



Base64 decode the Basic Auth:

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions **Payloads** Options

**Payload Positions** Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

```
1 GET /basic HTTP/1.1
2 Host: 192.253.50.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=$liretttdngj4qbke4n15jhpng3$
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Authorization: Basic dGVzdDoxMjM=
12
13
```

Send to Repeater Ctrl+R  
Scan defined insertion points [Pro version only]  
Convert selection  
URL-encode as you type  
Cut Ctrl+X  
Copy Ctrl+C  
Paste Ctrl+V  
Base64  
Construct string  
Base64-decode Ctrl+Shift+B  
Base64-encode Ctrl+B

0 matches Clear

Right click and decode the base64 encoded basic auth:



Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender

1 x 2 x ...

Target Positions Payloads Options

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

```

1 GET /basic HTTP/1.1
2 Host: 192.253.50.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=$liretttdngj4qbke4n15jhpng3$
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Authorization: Basic test:123

```

The credentials passed to the login prompt are shown.

Replace the credentials with a parameter to be substituted:

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions Payloads Options

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

**Start attack**

```

1 GET /basic HTTP/1.1
2 Host: 192.253.50.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=$liretttdngj4qbke4n15jhpng3$
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Authorization: Basic creds
12

```

Add \$

Clear \$

Auto \$

Refresh

Click on the Add Button on the right side:



Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions **Payloads** Options

### ? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

```
1 GET /basic HTTP/1.1
2 Host: 192.253.50.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=$liretttdngj4qbke4n15jhpng3$
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Authorization: Basic $creds$
```

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

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Extender P

1 x 2 x ...

Target Positions **Payloads** Options

### ? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type are available for each payload set, and each payload type can be customized in different ways.

Payload set: **1** Payload count: 0

Payload type: **Simple list** Request count: 0

### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

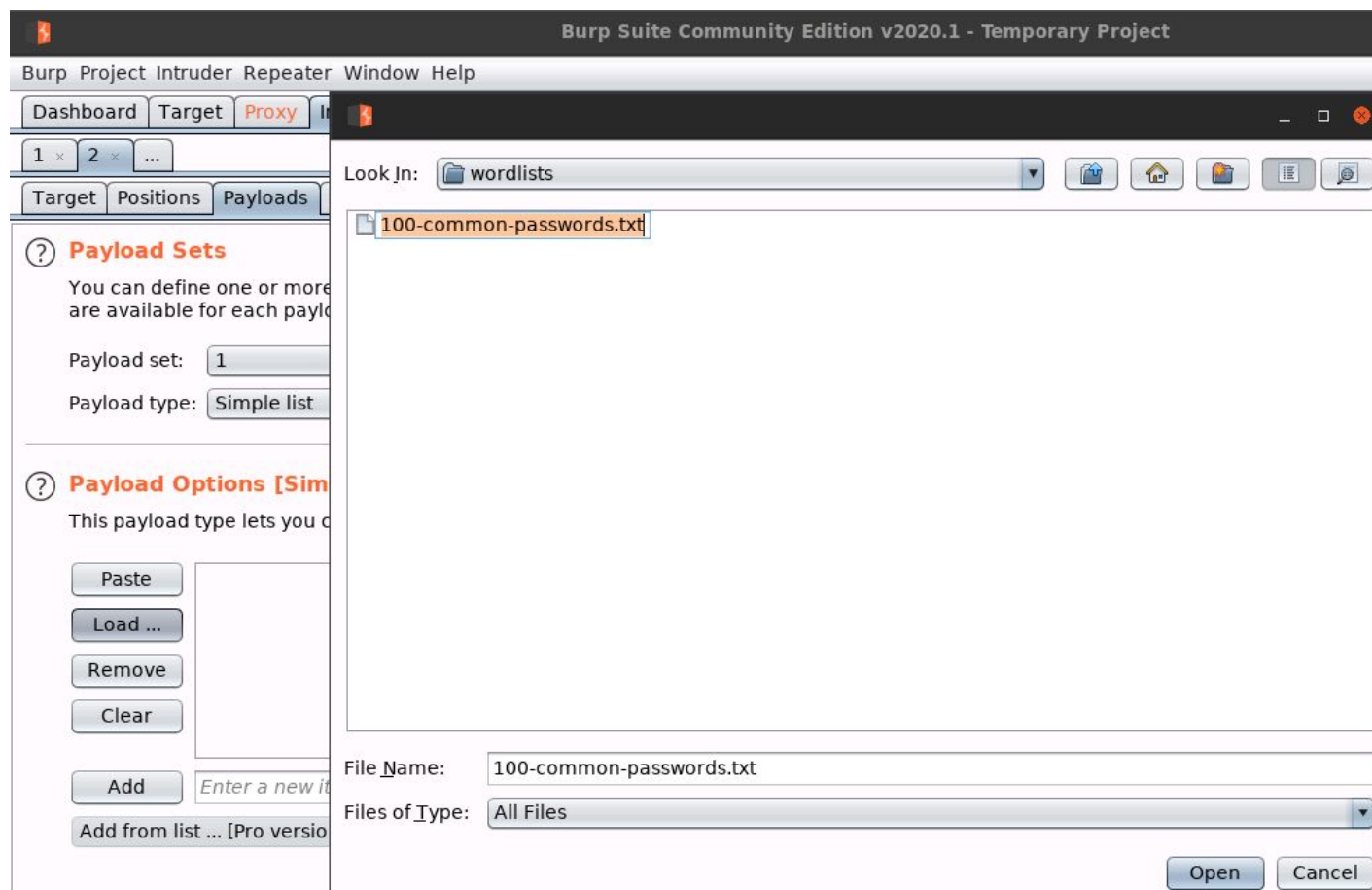
Paste

Load ...

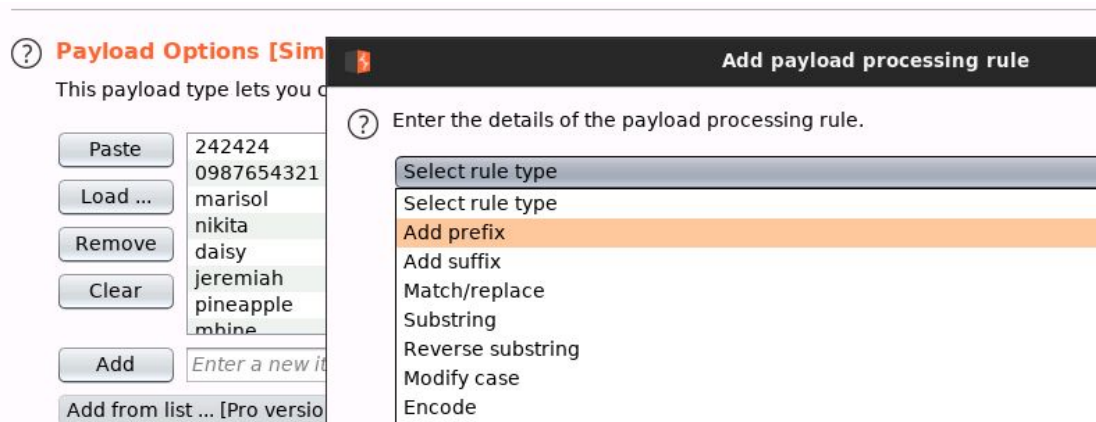
Remove

Clear

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

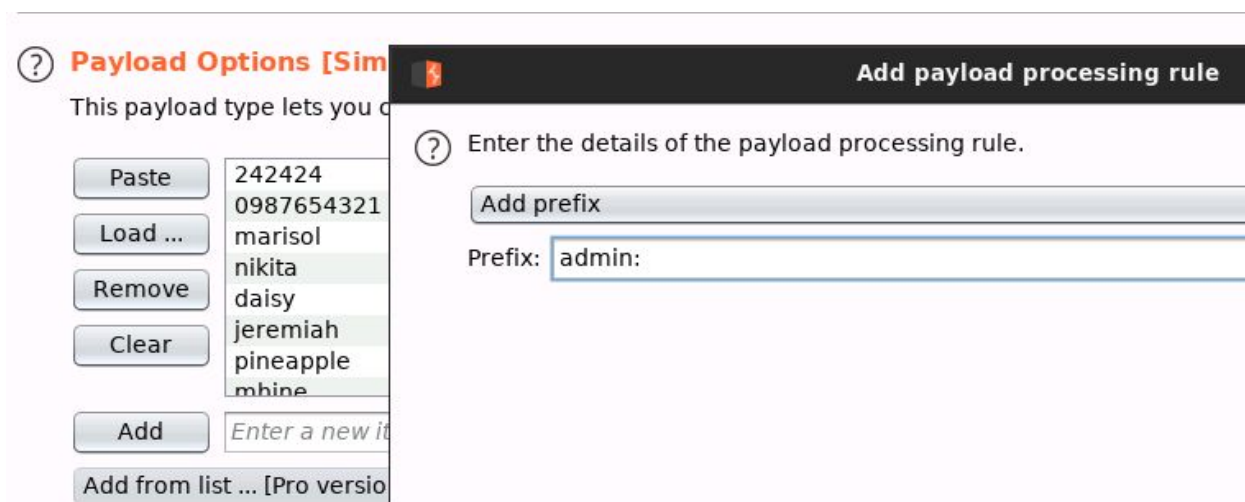


In the Payload Processing section click on the “Add” button.



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:

### ? Payload Processing

You can define rules to perform

Add

Edit

Remove

Up

Down

Enabled	Rule
<input checked="" type="checkbox"/>	Ac

### Add payload processing rule

? Enter the details of the payload processing rule.

Encode

Base64-encode

Select the Encode Rule as Base64-encode

Next, click on the “Start Attack” button:

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

1 × 2 × ...

Target
Positions
Payloads
Options

### ? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

Payload count:

100

Payload type:

Simple list

Request count:

200

### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Start attack

This would start the dictionary attack against the target webapp:

Intruder attack 1

Attack Save Columns

Results

Target

Positions

Payloads

Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			401	<input type="checkbox"/>	<input type="checkbox"/>	681	
1	1	YWRtaW46MjQyNDI0	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
2	1	YWRtaW46MDk4NzY1NDMyMQ...	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
3	1	YWRtaW46bWFyaXNvbA==	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
4	1	YWRtaW46bmlraXRh	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
5	1	YWRtaW46ZGFpc3k=	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
6	1	YWRtaW46amVyZW1pYWg=	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
7	1	YWRtaW46cGluZW1pYWg=	401	<input type="checkbox"/>	<input type="checkbox"/>	681	



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

Attack Save Columns

Results

Target

Positions

Payloads

Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
165	2	YWRtaW46Y29va2llMQ==	301	<input type="checkbox"/>	<input type="checkbox"/>	536	
0			401	<input type="checkbox"/>	<input type="checkbox"/>	681	
1	1	YWRtaW46MjQyNDI0	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
2	1	YWRtaW46MDk4NzY1NDMyMQ...	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
3	1	YWRtaW46bWFyaXNvbA==	401	<input type="checkbox"/>	<input type="checkbox"/>	681	
4	1	YWRtaW46bmlraXRh	401	<input type="checkbox"/>	<input type="checkbox"/>	681	

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

Double click on the request entry:

Result 165 | Intruder attack 1

Position: 2

Payload: YWRtaW46Y29va2llMQ==

Status: 301

Length: 536

Timer: 0

RequestResponse

RawParamsHeadersHex

1 GET /basic HTTP/1.1

2 Host: 192.253.50.3

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Cookie: PHPSESSID=liretttdngj4qbke4n15jhpng3

9 Upgrade-Insecure-Requests: 1

10 Authorization: Basic YWRtaW46Y29va2llMQ%3d%3d

**Result 165 | Intruder attack 1**

Position: 2  
Payload: YWRtaW46Y29va2llMQ==  
Status: 301  
Length: 536  
Timer: 0

Request Response

Raw Params Headers Hex

```
1 GET /basic HTTP/1.1
2 Host: 192.253.50.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=liretttdngj4qbke4n15jh
9 Upgrade-Insecure-Requests: 1
10 Authorization: Basic YWRtaW46Y29va2llMQ%
11
12
```

Scan [Pro version only]  
Send to Intruder Ctrl+I  
Send to Repeater Ctrl+R  
Send to Sequencer  
Send to Comparer  
Send to Decoder  
Show response in browser  
Request in browser

? < + > Type a search term

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

**Burp Suite Community Edition v2020.1 - Temporary Project**

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

YWRtaW46Y29va2llMQ%3d%3d

☒ Text ☐ Hex ?

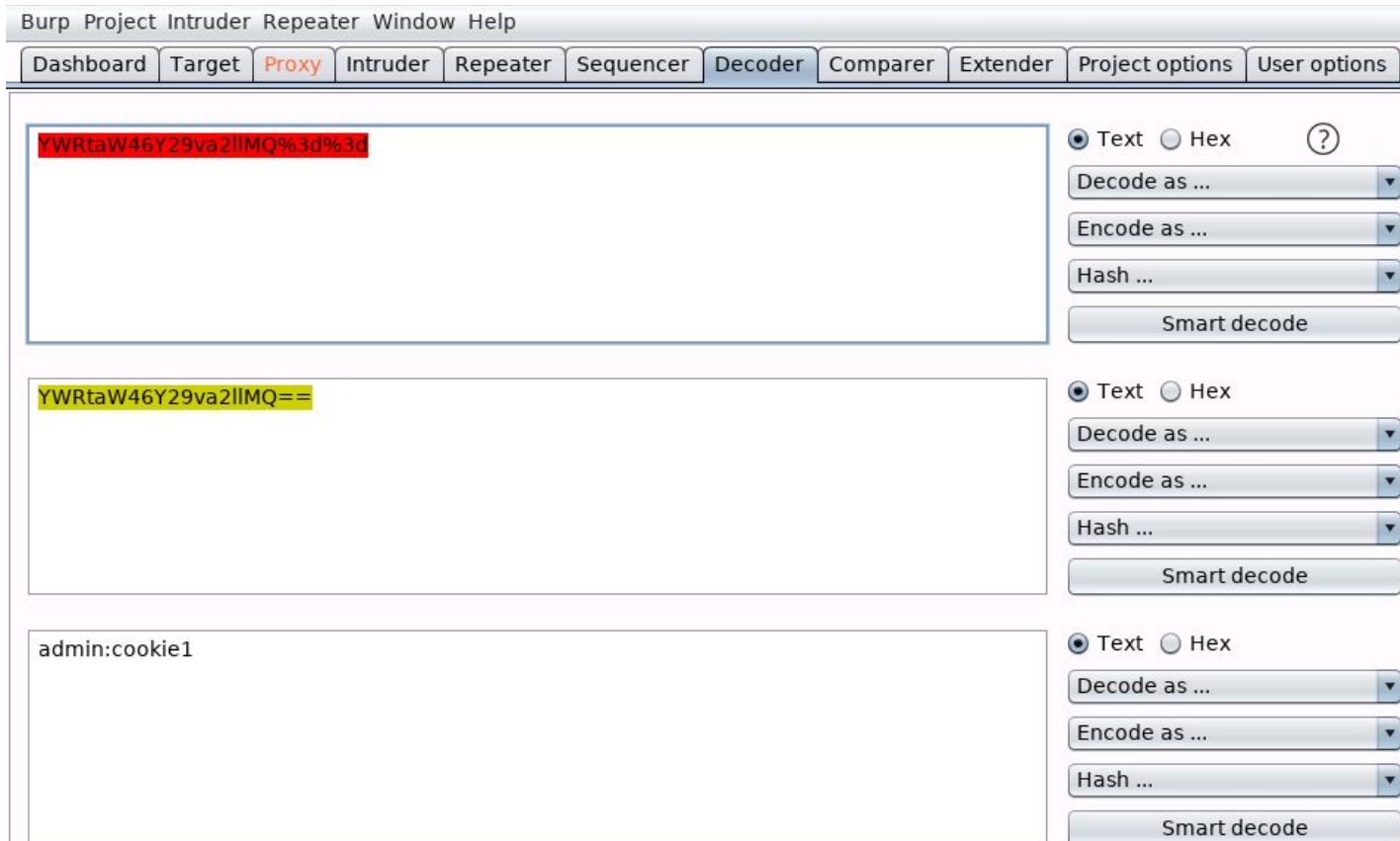
Decode as ...

Encode as ...

Hash ...

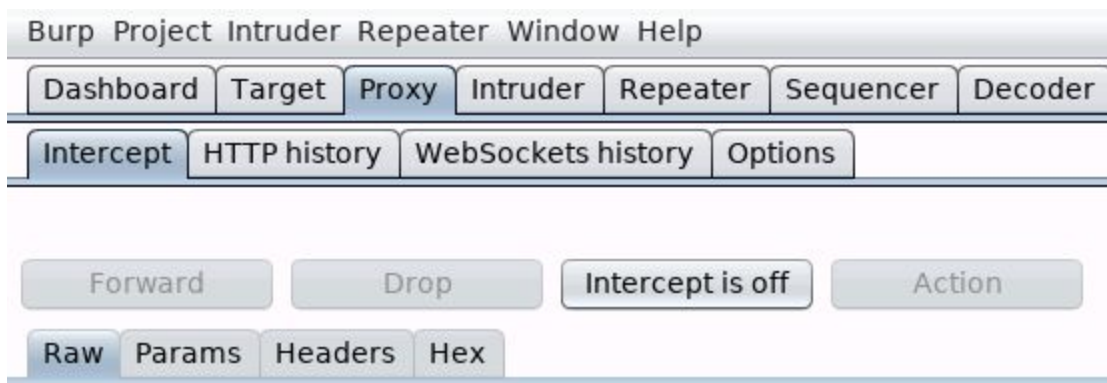
Smart decode

URL decode the credentials followed by base64-decode:

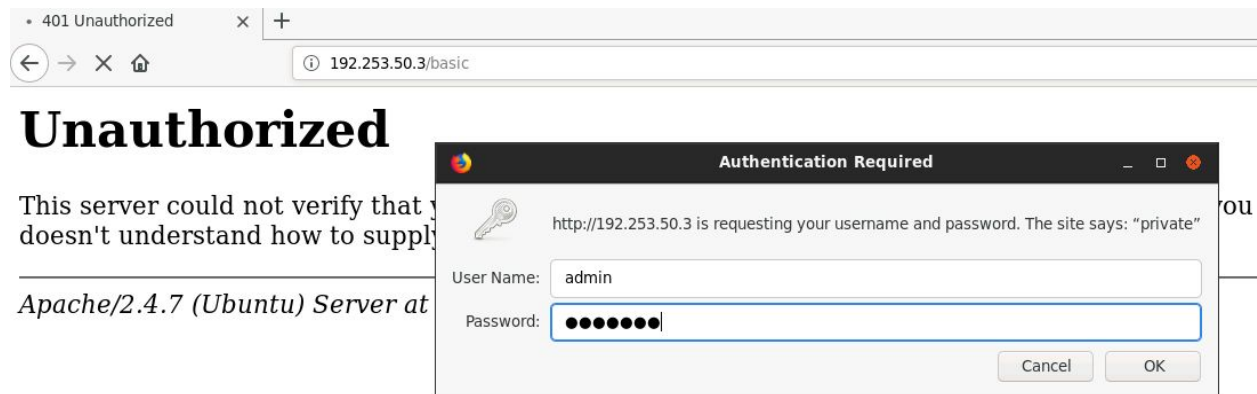


**Username:** admin  
**Password:** cookie1

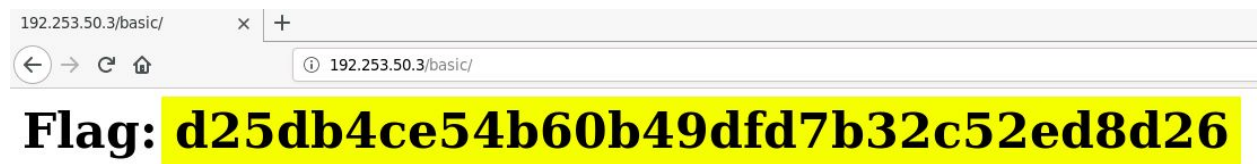
Now, turn off the intercept mode in Burp Suite:



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>)