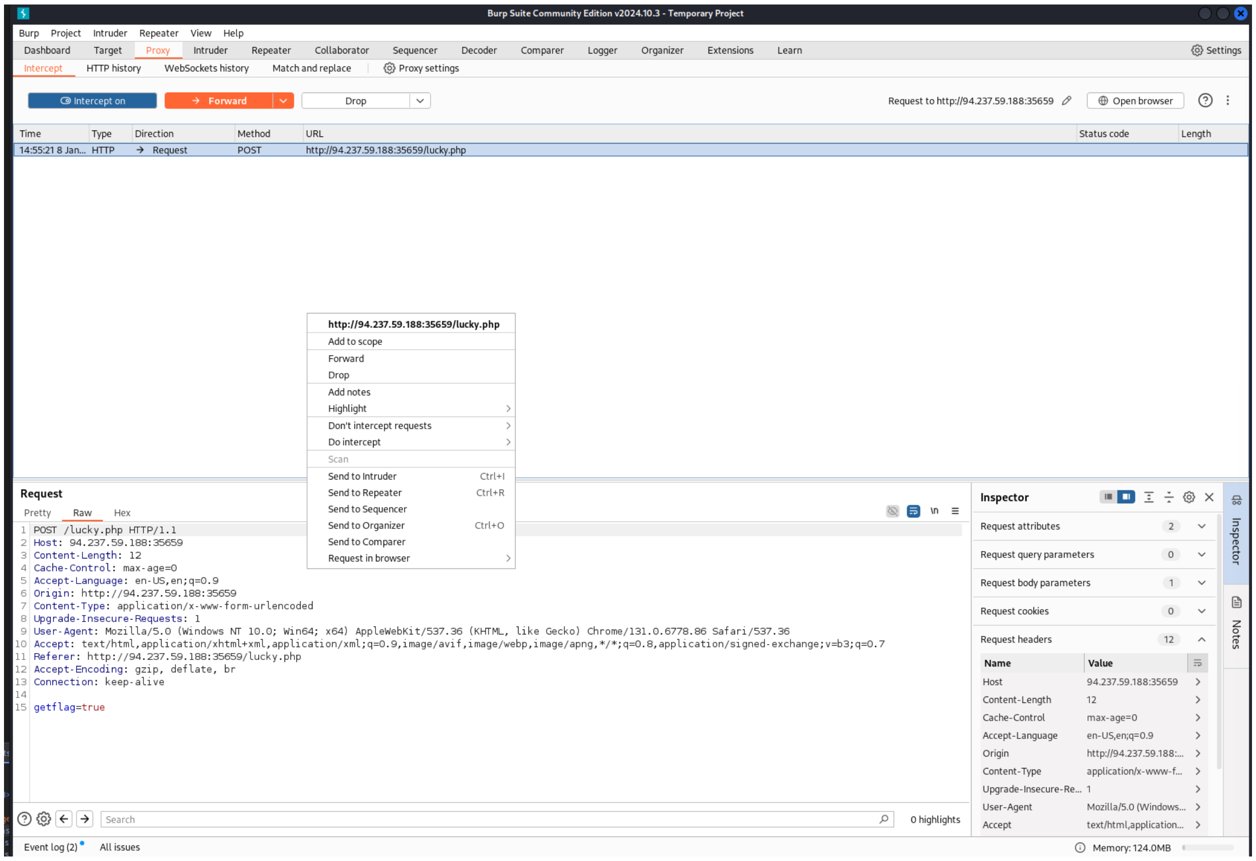
Skills Assessment

The /lucky.php page has a button that appears to be disabled. Try to enable the button, and then click it to get the flag.

Opening the target ip/port to the page that I'm directed to, I find I cannot click the button. Changing the source by removing the disabled tag in the Button class definitions allowed me to click it.

I made sure to have Burp up and running before then.

I right clicked on that request and sent it to repeater



Time	Type	Direction	Method	URL	Status code	Length
14:55:21 8 Jan...	HTTP	→ Request	POST	http://94.237.59.188:35659/lucky.php		

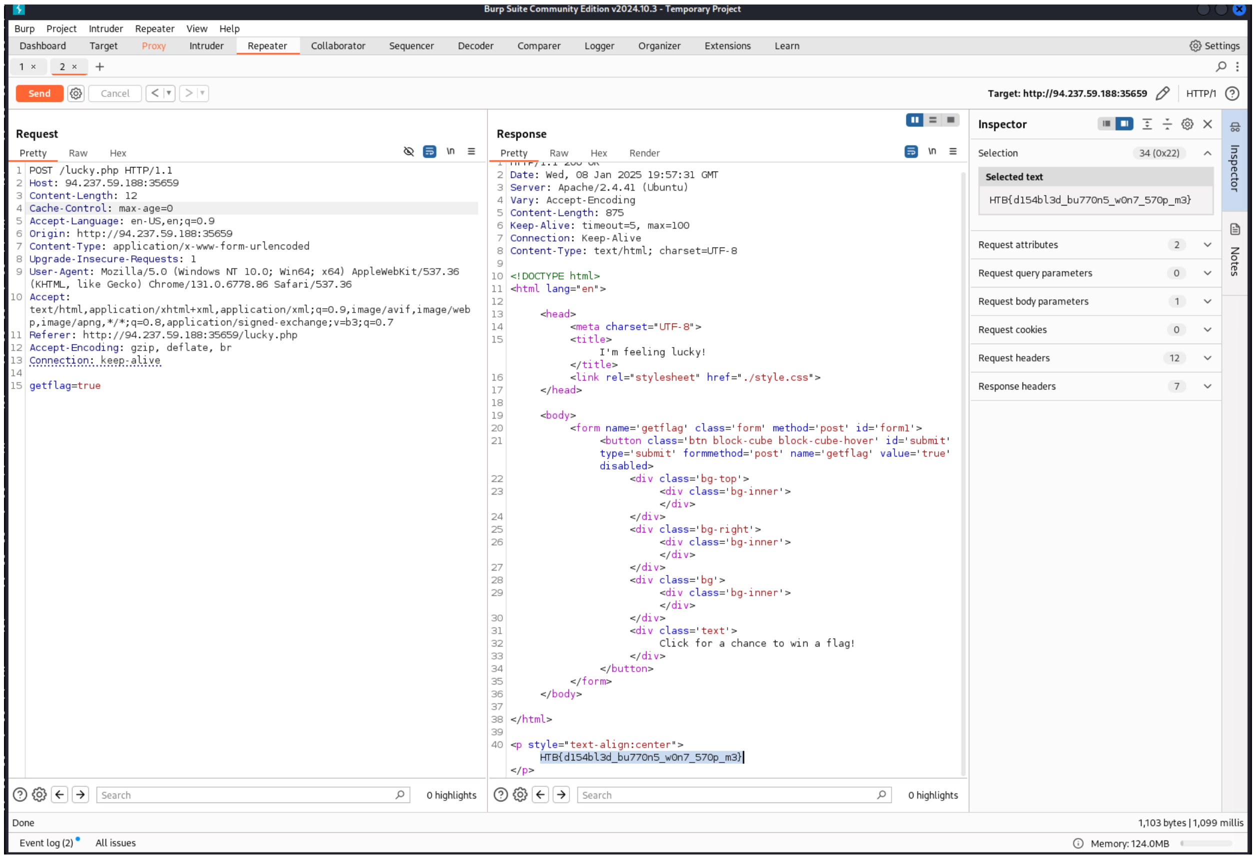
```
POST /lucky.php HTTP/1.1
Host: 94.237.59.188:35659
Content-Length: 12
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://94.237.59.188:35659
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://94.237.59.188:35659/lucky.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

getflag=true
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	0
Request headers	12

Name	Value
Host	94.237.59.188:35659
Content-Length	12
Cache-Control	max-age=0
Accept-Language	en-US,en;q=0.9
Origin	http://94.237.59.188:...
Content-Type	application/x-www-f...
Upgrade-Insecure-Re...	1
User-Agent	Mozilla/5.0 (Windows...
Accept	text/html,application...

Right clicked on the post request in repeater and then clicked on copy request as curl command

Clicking the send button on that post request multiple times yo do get the flag in the body of the servers response


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: http://94.237.59.188:35659
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 34 (0x22)
Selected text
HTB{d154bl3d_bu770n5_w0n7_570p_m3}
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 12
Response headers 7
Done
1,103 bytes | 1,099 millis
Event log (2) All issues
Memory: 124.0MB

```
POST /lucky.php HTTP/1.1
Host: 94.237.59.188:35659
Content-Length: 12
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://94.237.59.188:35659
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://94.237.59.188:35659/lucky.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

getflag=true
```

```
HTTP/1.1 200 OK
Date: Wed, 08 Jan 2025 19:57:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 875
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">

    <head>
        <meta charset="UTF-8">
        <title>
            I'm feeling lucky!
        </title>
        <link rel="stylesheet" href="./style.css">
    </head>

    <body>
        <form name='getflag' class='form' method='post' id='form1'>
            <button class='btn block-cube block-cube-hover' id='submit'
            type='submit' formmethod='post' name='getflag' value='true'
            disabled>
                <div class='bg-top'>
                    <div class='bg-inner'>
                    </div>
                </div>
                <div class='bg-right'>
                    <div class='bg-inner'>
                    </div>
                </div>
                <div class='bg'>
                    <div class='bg-inner'>
                    </div>
                </div>
                <div class='text'>
                    Click for a chance to win a flag!
                </div>
            </button>
        </form>
    </body>

</html>

<p style="text-align:center">
    HTB{d154bl3d_bu770n5_w0n7_570p_m3}
</p>
```

I fiddled around with trying to copy the post request as curl and then using a bash loop to automatically send the post request x number of times. I wasn't able to get this to work in the way I wanted as I was only receiving the HTTP response headers, and not the bodies in the server responses to my curl command.

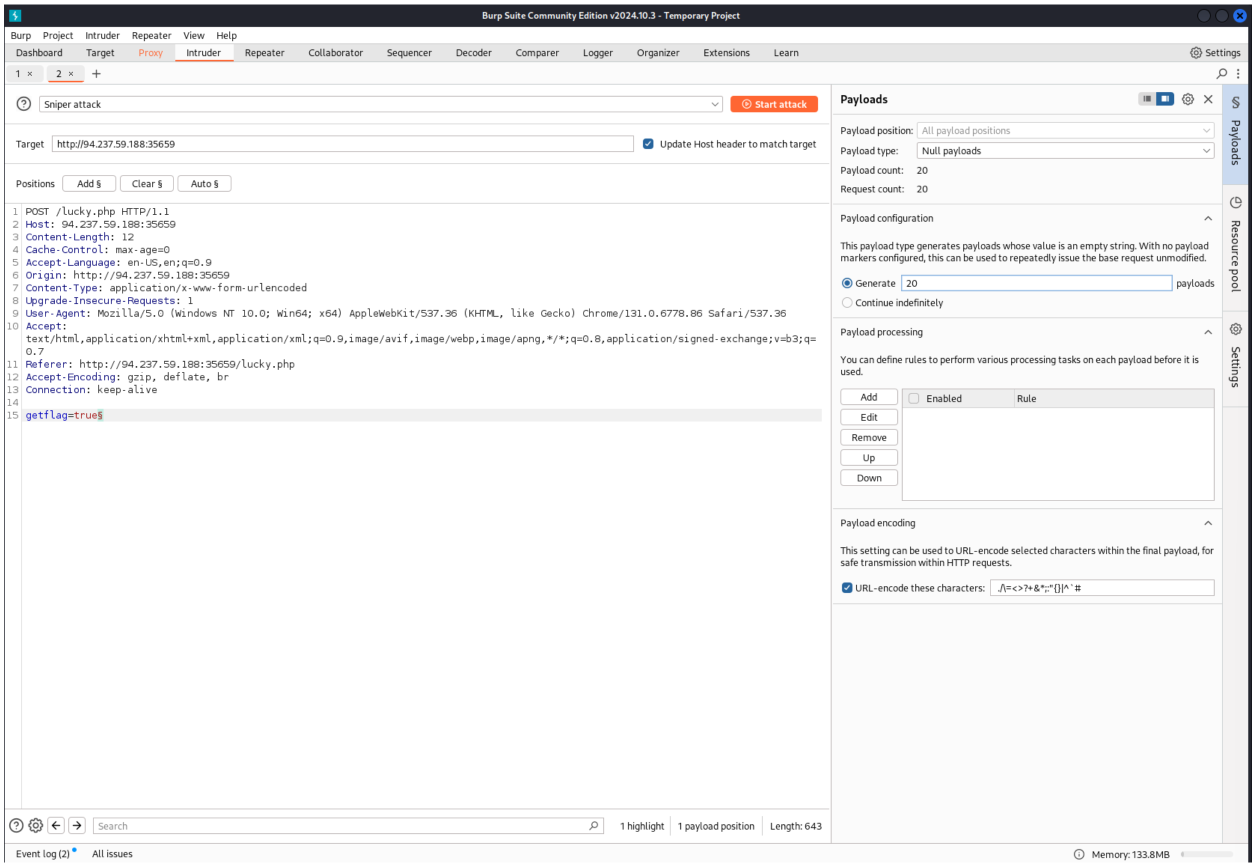
```
curl command:
 curl --path-as-is -i -s -k -X $'POST' \
    -H $'Host: 94.237.59.188:35659' -H $'Content-Length: 12' -H
    --data-binary $'getflag=true' \
    $'http://94.237.59.188:35659/lucky.php'
```

```
-XHTTP/1.1 200 OK
Date: Wed, 08 Jan 2025 20:13:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 338
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

little bash loop to run that 10 times
for i in {1..10}; do
curl --path-as-is -i -s -k -w -X $'POST' \
    -H $'Host: 94.237.59.188:35659' -H $'Content-Length: 12' -H
    --data-binary $'getflag=true' \
    $'http://94.237.59.188:35659/lucky.php'
done
```

Another means of automation I found doing some research online was using intruder with a null payload to just send the same request x number of times and that did end up working as a means of automation

On the repeater screen, right click on the post request and send to intruder

Add a marker for the payload anywhere to get the options to come up


Burp Suite Community Edition v2024.10.3 - Temporary Project

Sniper attack

Target: http://94.237.59.188:35659 — Update Host header to match target: ✓

```
POST /lucky.php HTTP/1.1
Host: 94.237.59.188:35659
Content-Length: 12
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://94.237.59.188:35659
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://94.237.59.188:35659/lucky.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

getflag=true§
```

1 highlight | 1 payload position | Length: 643

Payloads

Payload position: All payload positions
Payload type: Null payloads
Payload count: 20
Request count: 20

Payload configuration

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

[✓ Generate] 20 payloads
Continue indefinitely

Payload processing

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

Payload encoding

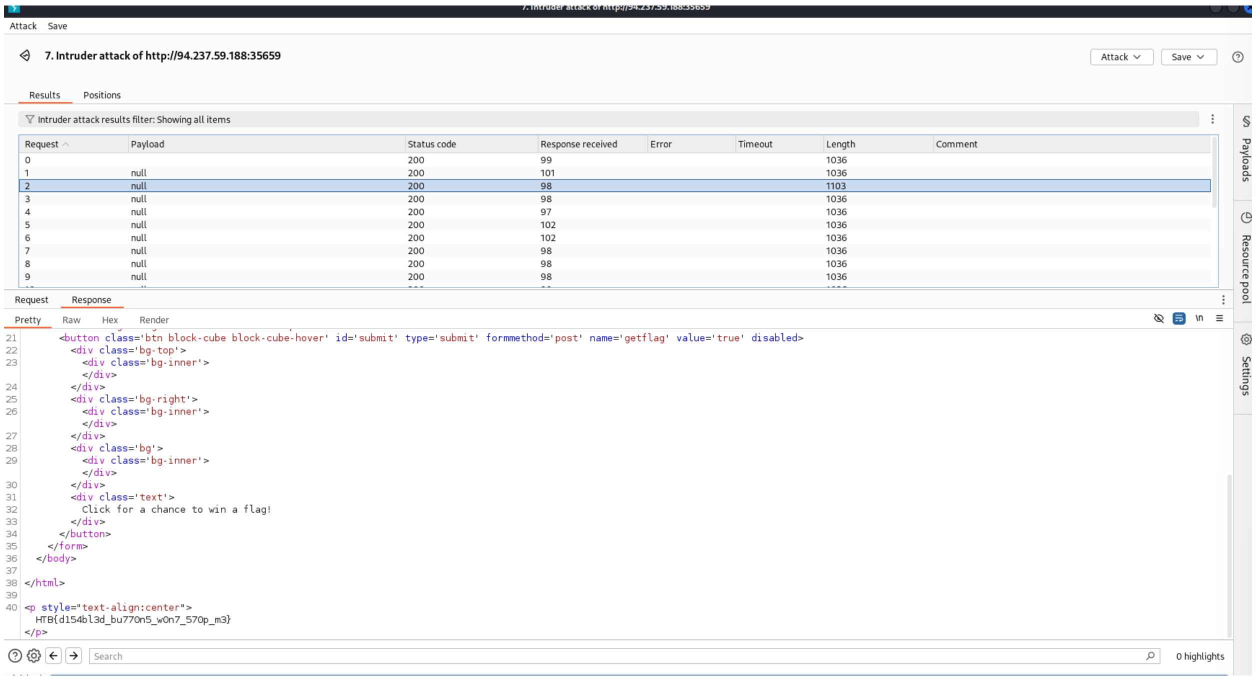
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

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

Memory: 133.8MB

In this instance I told it to send the post request 20 times

Then in the attack window you can just sort by length and the different size page will be the one with the added flag text making it bigger and you can just look at the response (not the request window) to get the flag


7. Intruder attack of http://94.237.59.188:35659

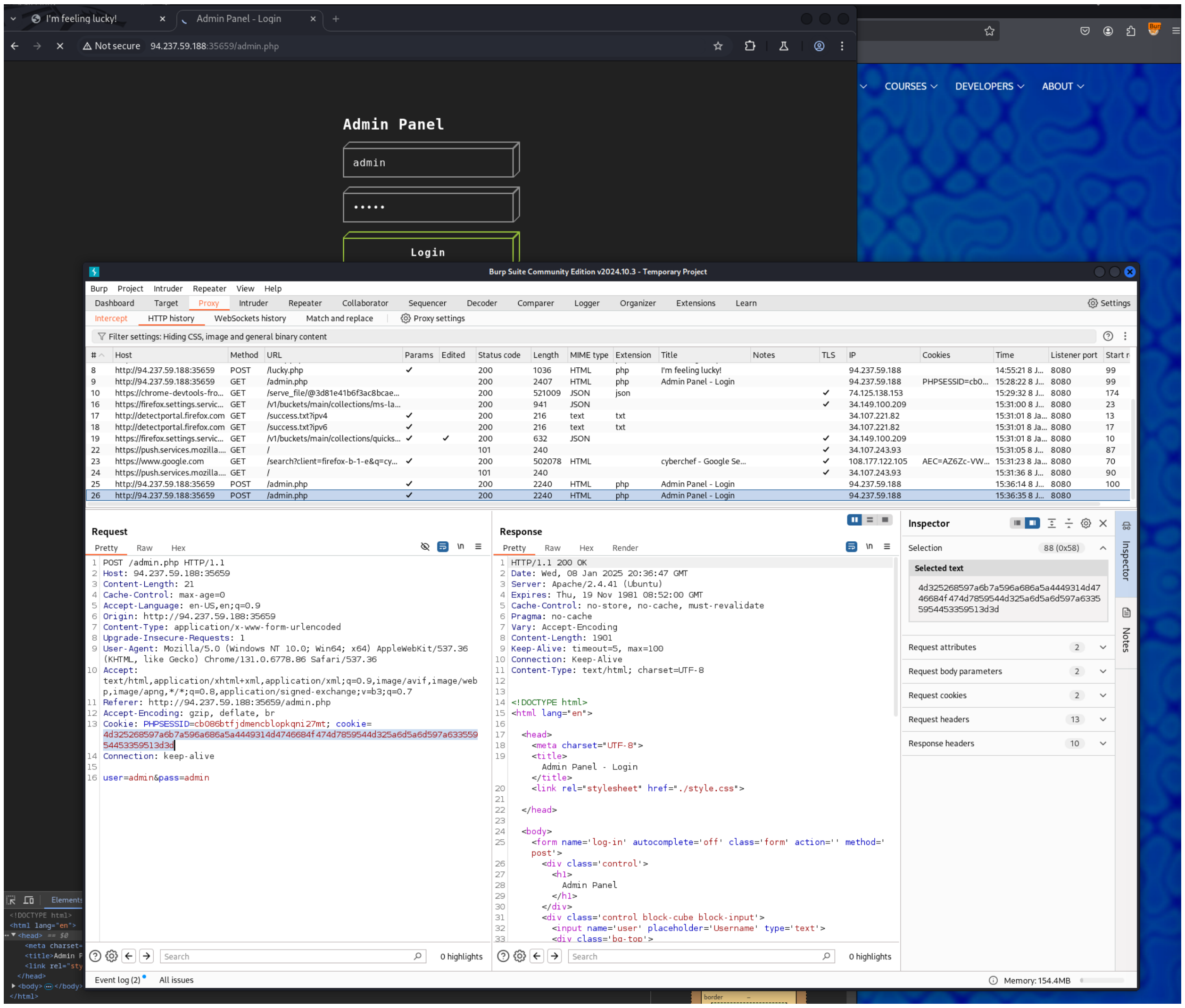
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	99			1036	
1	null	200	101			1036	
2	null	200	98			1103	
3	null	200	98			1036	
4	null	200	97			1036	
5	null	200	102			1036	
6	null	200	102			1036	
7	null	200	98			1036	
8	null	200	98			1036	
9	null	200	98			1036	

```
      <button class='btn block-cube block-cube-hover' id='submit' type='submit' formmethod='post' name='getflag' value='true' disabled>
        <div class='bg-top'>
          <div class='bg-inner'>
          </div>
        </div>
        <div class='bg-right'>
          <div class='bg-inner'>
          </div>
        </div>
        <div class='bg'>
          <div class='bg-inner'>
          </div>
        </div>
        <div class='text'>
          Click for a chance to win a flag!
        </div>
      </button>
    </form>
  </body>

</html>

<p style="text-align:center">
  HTB{d154bl3d_bu770n5_w0n7_570p_m3}
</p>
```

The /admin.php page uses a cookie that has been encoded multiple times. Try to decode the cookie until you get a value with 31-characters. Submit the value as the answer.

Making sure my proxy is set up to intercept and then visiting the admin page



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start r
8	http://94.237.59.188:35659	POST	/lucky.php	✓		200	1036	HTML	php	I'm feeling lucky!			94.237.59.188		14:55:21 8 J...	8080	99
9	http://94.237.59.188:35659	GET	/admin.php			200	2407	HTML	php	Admin Panel - Login			94.237.59.188	PHPSESSID=cb0...	15:28:22 8 J...	8080	99
10	https://chrome-devtools-fro...	GET	/serve_file/@3d81e41b6f3ac8bcae...			200	521009	JSON	json			✓	74.125.138.153		15:29:32 8 J...	8080	174
16	https://firefox.settings.servic...	GET	/v1/buckets/main/collections/ms-la...			200	941	JSON				✓	34.149.100.209		15:31:00 8 J...	8080	23
17	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	216	text	txt				34.107.221.82		15:31:01 8 Ja...	8080	13
18	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	216	text	txt				34.107.221.82		15:31:01 8 Ja...	8080	17
19	https://firefox.settings.servic...	GET	/v1/buckets/main/collections/quicks...	✓	✓	200	632	JSON				✓	34.149.100.209		15:31:01 8 Ja...	8080	10
22	https://push.services.mozilla....	GET	/			101	240					✓	34.107.243.93		15:31:05 8 J...	8080	87
23	https://www.google.com	GET	/search?client=firefox-b-1-e&q=cy...	✓		200	502078	HTML		cyberchef - Google Se...		✓	108.177.122.105	AEC=AZ6Zc-VW...	15:31:23 8 Ja...	8080	70
24	https://push.services.mozilla....	GET	/			101	240					✓	34.107.243.93		15:31:36 8 J...	8080	90
25	http://94.237.59.188:35659	POST	/admin.php	✓		200	2240	HTML	php	Admin Panel - Login			94.237.59.188		15:36:14 8 J...	8080	100
26	http://94.237.59.188:35659	POST	/admin.php	✓		200	2240	HTML	php	Admin Panel - Login			94.237.59.188		15:36:35 8 J...	8080	

Request

```
POST /admin.php HTTP/1.1
Host: 94.237.59.188:35659
Content-Length: 21
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://94.237.59.188:35659
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://94.237.59.188:35659/admin.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=cb086btfjdmencblopkqni27mt; cookie=
4d325268597a6b7a596a686a5a4449314d4746684f474d7859544d325a6d5a6d597a633559
54453359513d3d
Connection: keep-alive

user=admin&pass=admin
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 08 Jan 2025 20:36:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1901
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="UTF-8">
    <title>
      Admin Panel - Login
    </title>
    <link rel="stylesheet" href="./style.css">

  </head>

  <body>
    <form name='log-in' autocomplete='off' class='form' action='' method='
    post'>
      <div class='control'>
        <h1>
          Admin Panel
        </h1>
      </div>
      <div class='control block-cube block-input'>
        <input name='user' placeholder='Username' type='text'>
        <div class='bg-top'>
```

Inspector

Selection 88 (0x58)

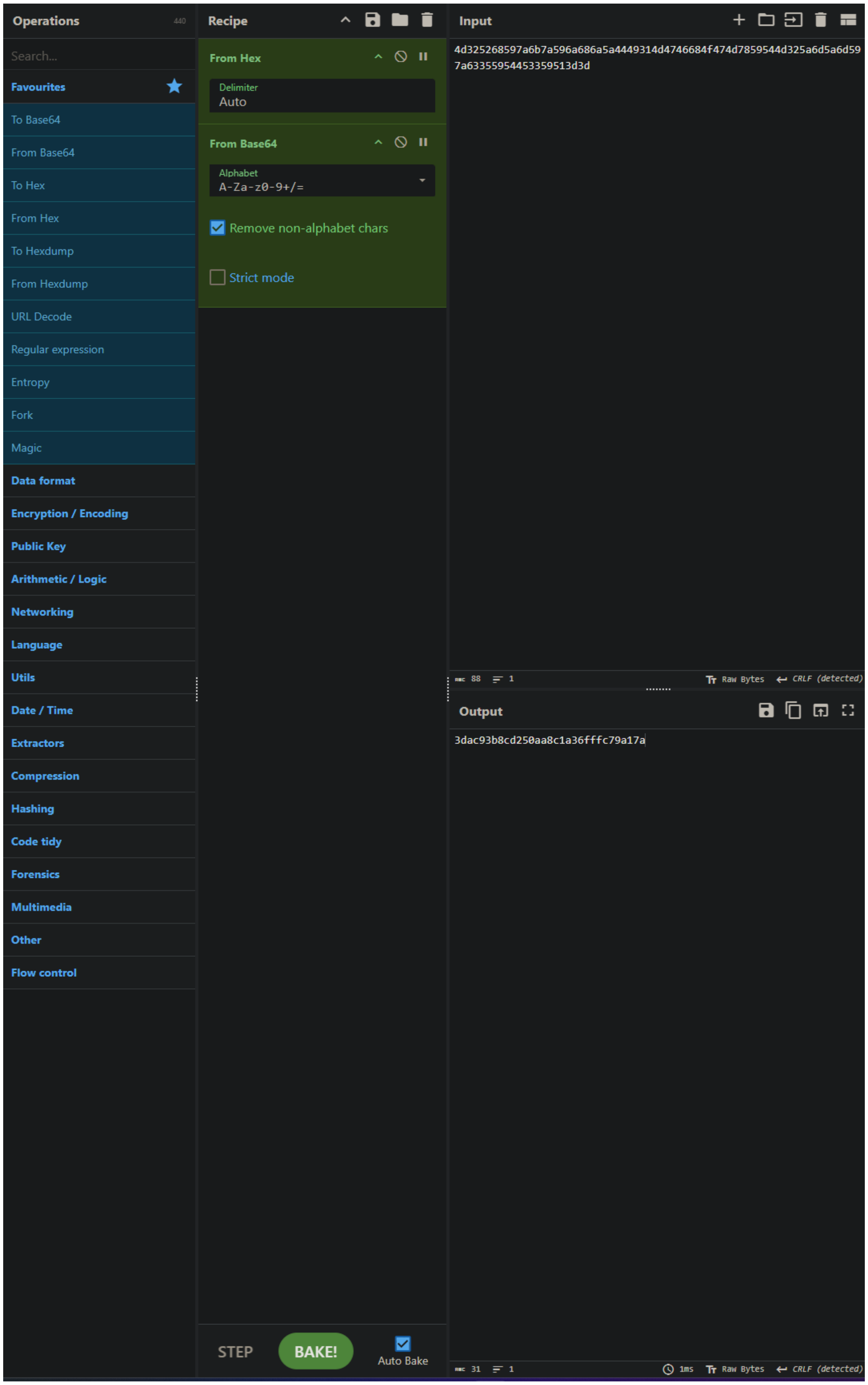
Selected text

```
4d325268597a6b7a596a686a5a4449314d4746684f474d7859544d325a6d5a6d597a6335595445335
9513d3d
```

Request attributes	2
Request body parameters	2
Request cookies	2
Request headers	13
Response headers	10

I'm feeling lucky!
Admin Panel - Login
Not secure 94.237.59.188:35659/admin.php
COURSES
DEVELOPERS
ABOUT
Admin Panel
admin
Login
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Pretty Raw Hex Render
0 highlights
Event log (2) All issues
Memory: 154.4MB

Putting that string into cyber chef and playing around with it for a bit till I determine it to be hexadecimal and then it becomes apparent its base64 encoded from the ==. Chefchef is nice because it tells you the length at the bottom of the output as well. It being 31 marks we've likely found the answer



Recipe

From Hex
Delimiter: Auto

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars
☐ Strict mode

Input

```
4d325268597a6b7a596a686a5a4449314d4746684f474d7859544d325a6d5a6d59
7a63355954453359513d3d
```

88 1 Raw Bytes CRLF (detected)

Output

```
3dac93b8cd250aa8c1a36fffc79a17a
```

31 1 1ms Raw Bytes CRLF (detected)

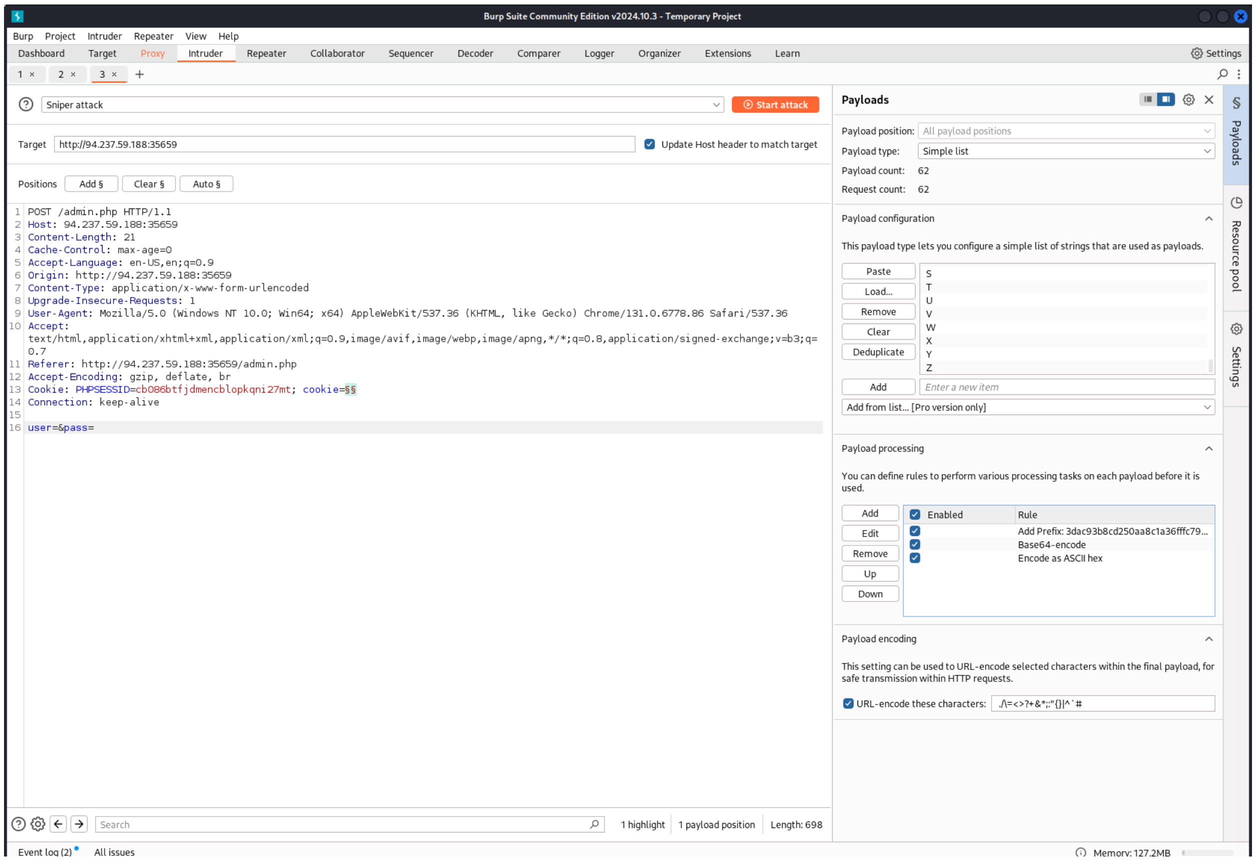
Once you decode the cookie, you will notice that it is only 31 characters long, which appears to be an md5 hash missing its last character. So, try to fuzz the last character of the decoded md5 cookie with all alpha-numeric characters, while encoding each request with the encoding methods you identified above. (You may use the "alphanum-case.txt" wordlist from Seclist for the payload)

Using the same post request from before that I got the cookie in, I send that to intruder

Finding the location of the word list they wanted me to use

```
find /usr/share/wordlists/seclists/* -name alphanum-case.txt

/usr/share/wordlists/seclists/Fuzzing/alphanum-case.txt
```

At this point I used intruder and inserted the decoded string as a prefix to the payload and encoded the entire payload doing the inverse of our cyber chef operation from the previous question.



Sniper attack

Target: http://94.237.59.188:35659

Update Host header to match target: ✓

```
POST /admin.php HTTP/1.1
Host: 94.237.59.188:35659
Content-Length: 21
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://94.237.59.188:35659
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://94.237.59.188:35659/admin.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=cb086btfjdmencblopkqni27mt; cookie=§§
Connection: keep-alive

user=&pass=
```

Payloads

Payload position: All payload positions
Payload type: Simple list
Payload count: 62
Request count: 62

Payload configuration

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

```
S
T
U
V
W
X
Y
Z
```

Payload processing

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

Enabled	Rule
✓	Add Prefix: 3dac93b8cd250aa8c1a36fffc79...
✓	Base64-encode
✓	Encode as ASCII hex

Payload encoding

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

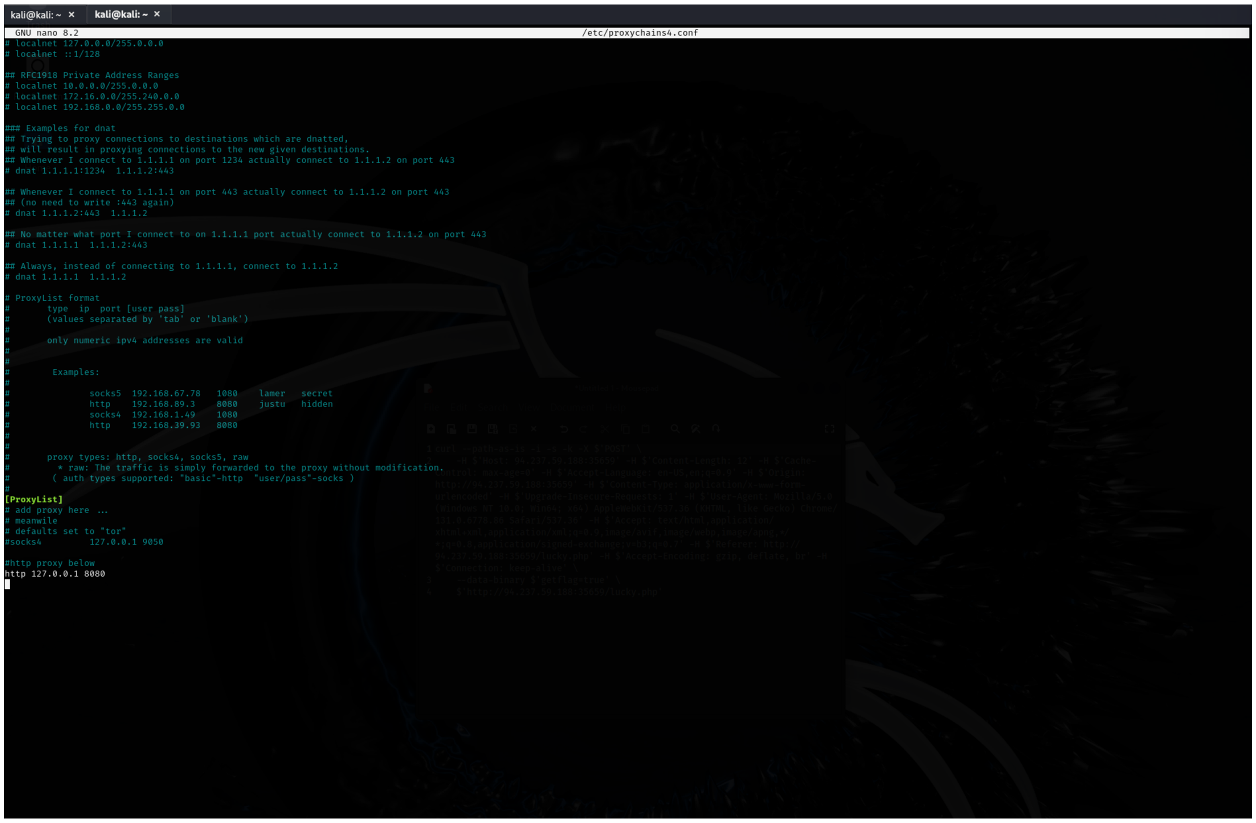
✓ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

1 highlight | 1 payload position | Length: 698

Doing so, I get the flag in one of the request that vary in length by fuzzing for the right cookie.

You are using the 'auxiliary/scanner/http/coldfusion_locale_traversal' tool within Metasploit, but it is not working properly for you. You decide to capture the request sent by Metasploit so you can manually verify it and repeat it. Once you capture the request, what is the 'XXXXX' directory being called in '/XXXXX/administrator/..'?

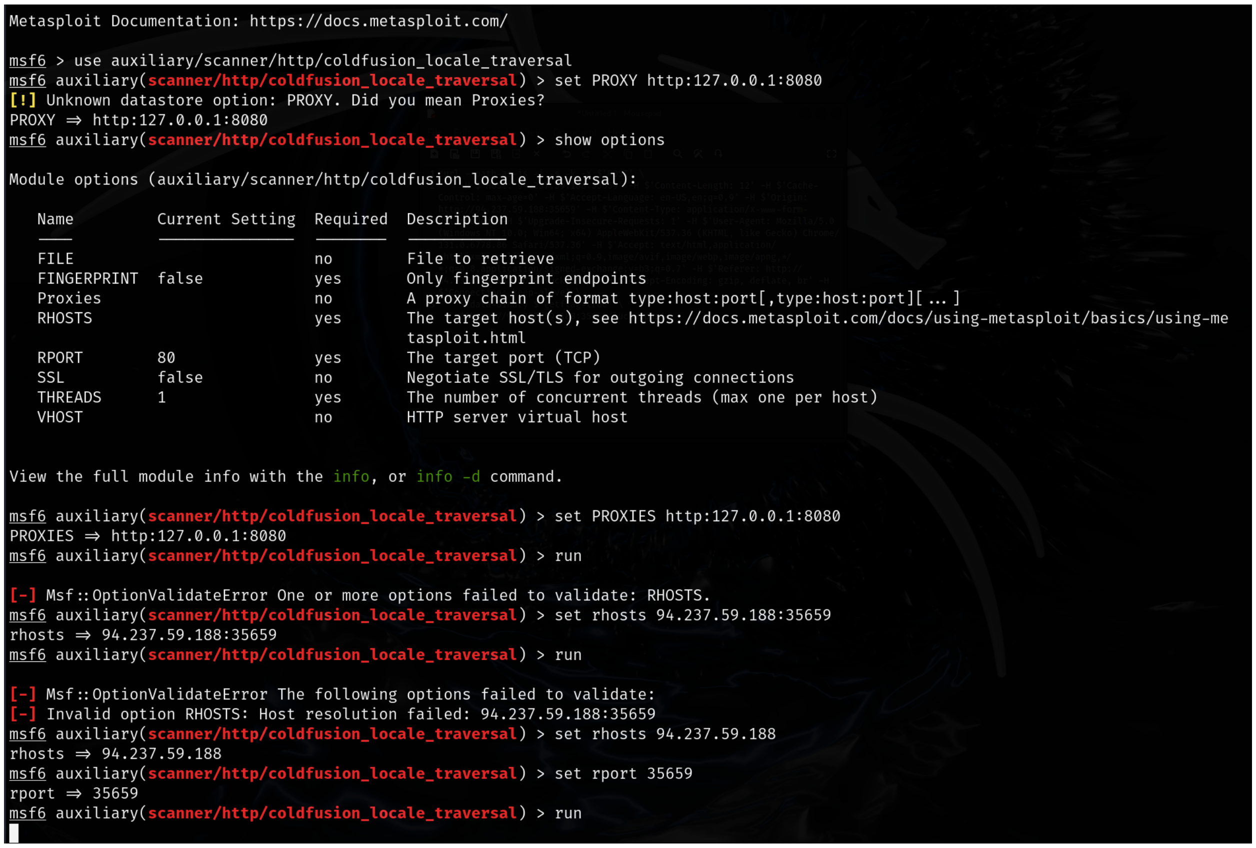
Making sure my proxychains is still setup from earlier in the module (that last line being the added config, you can also uncomment out the quite line to make the tool less noisy)



```
kali@kali: ~        kali@kali: ~
  GNU nano 8.2                                   /etc/proxychains4.conf
# localnet 127.0.0.0/255.0.0.0
# localnet ::1/128

## RFC1918 Private Address Ranges
# localnet 10.0.0.0/255.0.0.0
# localnet 172.16.0.0/255.240.0.0
# localnet 192.168.0.0/255.255.0.0

### Examples for dnat
## Trying to proxy connections to destinations which are dnatted,
## will result in proxying connections to the new given destinations.
## Whenever I connect to 1.1.1.1 on port 1234 actually connect to 1.1.1.2 on port 443
# dnat 1.1.1.1:1234  1.1.1.2:443

## Whenever I connect to 1.1.1.1 on port 443 actually connect to 1.1.1.2 on port 443
## (no need to write :443 again)
# dnat 1.1.1.2:443  1.1.1.2

## No matter what port I connect to on 1.1.1.1 port actually connect to 1.1.1.2 on port 443
# dnat 1.1.1.1  1.1.1.2:443

## Always, instead of connecting to 1.1.1.1, connect to 1.1.1.2
# dnat 1.1.1.1  1.1.1.2

# ProxyList format
#       type  ip  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#       only numeric ipv4 addresses are valid
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5, raw
#         * raw: The traffic is simply forwarded to the proxy without modification.
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050

#http proxy below
http 127.0.0.1 8080
```

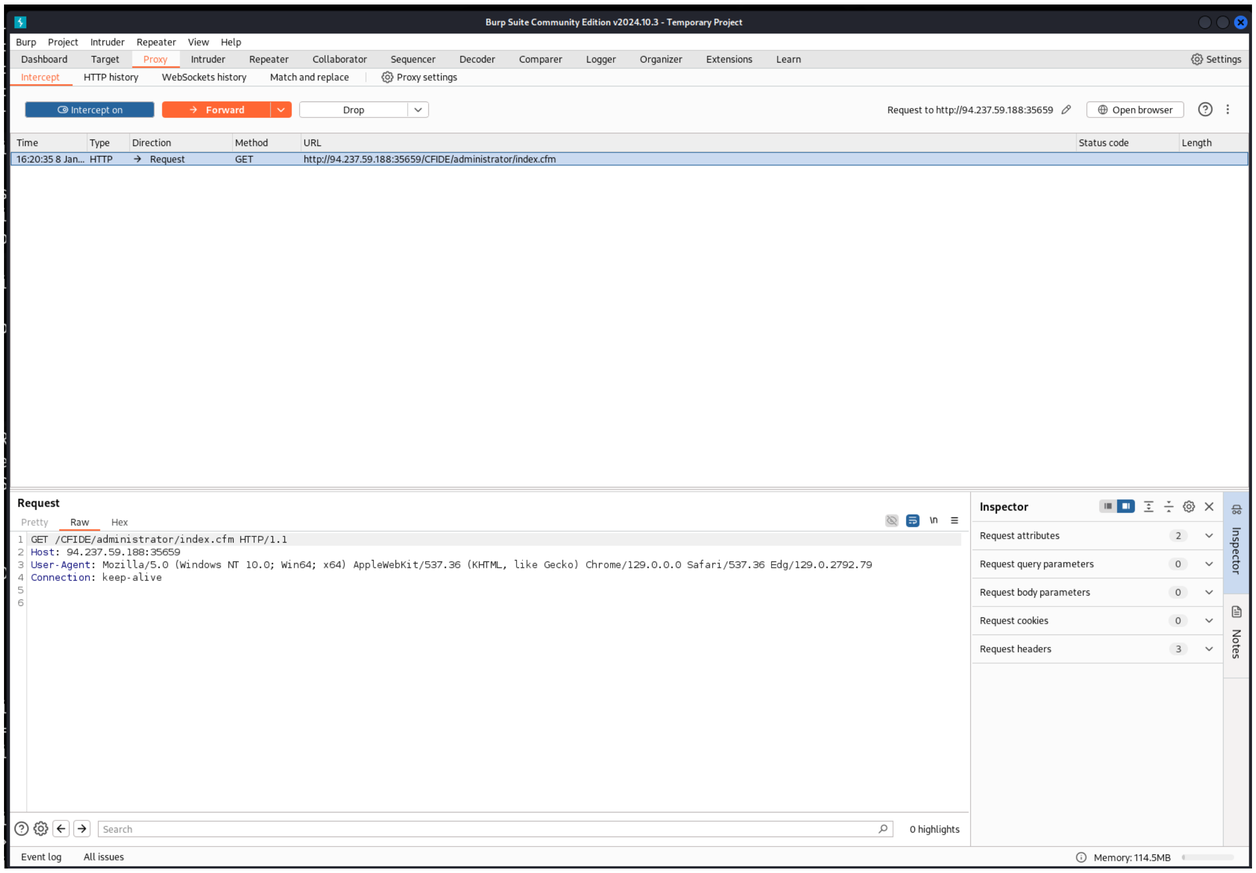
Opening Metasploit, setting and configuring the module they wanted me to use

Opened up burp, and made sure to turn intercept on so it would catch this request going through its proxy port



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/http/coldfusion_locale_traversal
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > set PROXY http:127.0.0.1:8080
[!] Unknown datastore option: PROXY. Did you mean Proxies?
PROXY ⇒ http:127.0.0.1:8080
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > show options

Module options (auxiliary/scanner/http/coldfusion_locale_traversal):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE                          no        File to retrieve
   FINGERPRINT  false            yes       Only fingerprint endpoints
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
                                           tasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   THREADS      1                yes       The number of concurrent threads (max one per host)
   VHOST                         no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > set PROXIES http:127.0.0.1:8080
PROXIES ⇒ http:127.0.0.1:8080
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > run

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > set rhosts 94.237.59.188:35659
rhosts ⇒ 94.237.59.188:35659
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > run

[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: 94.237.59.188:35659
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > set rhosts 94.237.59.188
rhosts ⇒ 94.237.59.188
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > set rport 35659
rport ⇒ 35659
msf6 auxiliary(scanner/http/coldfusion_locale_traversal) > run
█
```

When you run the tool, burp should catch the request


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://94.237.59.188:35659
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 3
Notes
Search
0 highlights
Event log All issues
Memory: 114.5MB

Time	Type	Direction	Method	URL	Status code	Length
16:20:35 8 Jan...	HTTP	→ Request	GET	http://94.237.59.188:35659/CFIDE/administrator/index.cfm		

Request

Pretty Raw Hex

```
GET /CFIDE/administrator/index.cfm HTTP/1.1
Host: 94.237.59.188:35659
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/129.0.2792.79
Connection: keep-alive


```