

## Web Application Attack



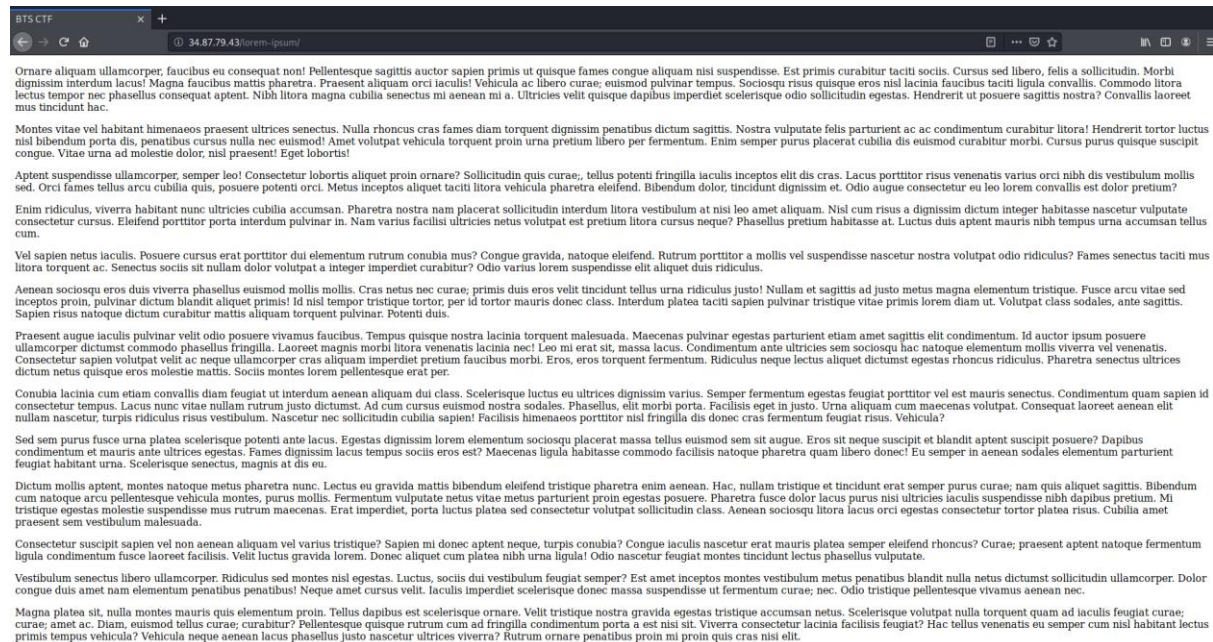
### Machines

- Lorem Ipsum – 10 points
- My First Website – 10 points
- My Second Website – 15 points
- Consoling – 15 points
- Takeover – 25 points

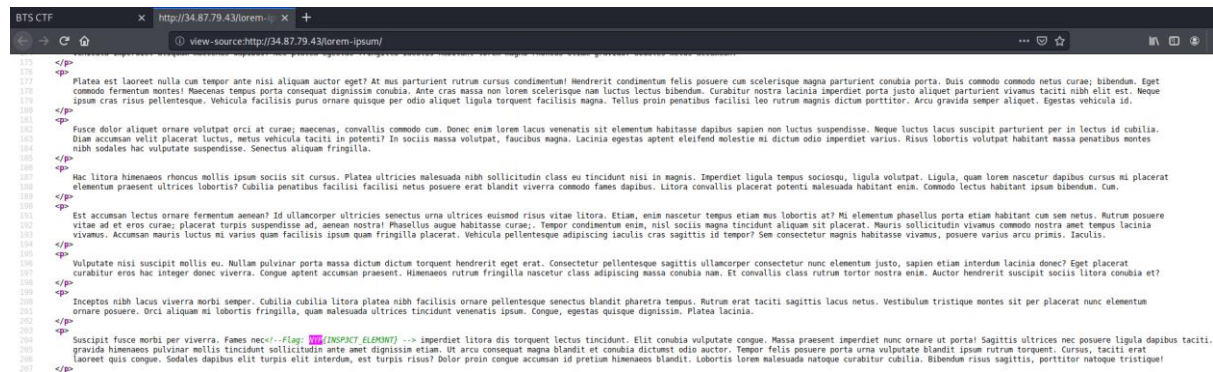
**Total – 75 points**

# 1) Lorem Ipsum (10 points)

1. Surfing <http://34.87.79.43/lorem-ipsum/>, we observe the following webpage.



2. Right click -> View Page Source

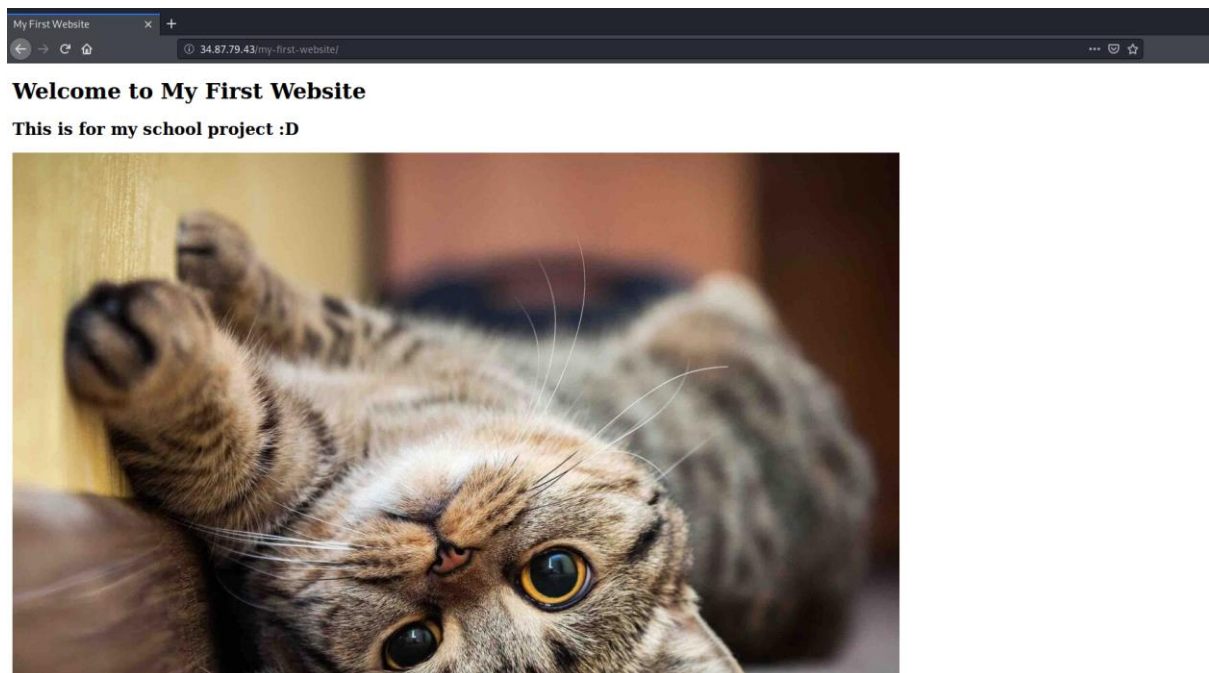


<!-- Flag: NYP{INSP3CT\_ELEM3NT} -->

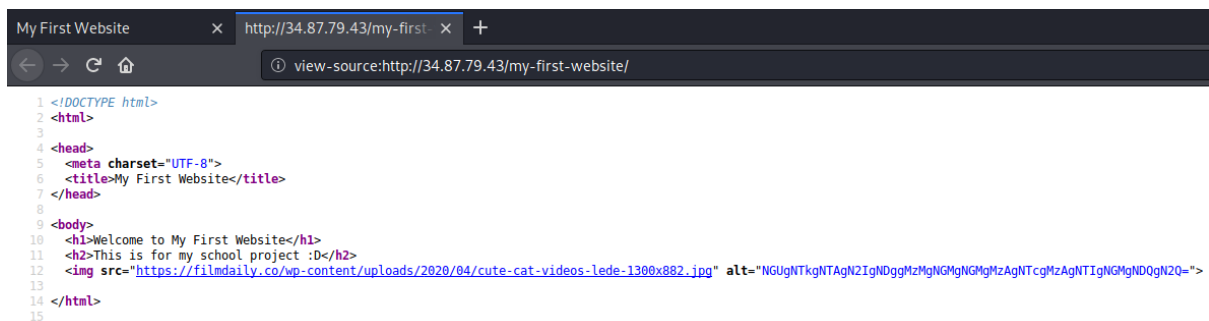
3. First flag is obtained (NYP{INSP3CT\_ELEM3NT})!

## 2) My First Website (10 points)

1. Surfing to <http://34.87.79.43/my-first-website/>, we are presented with the following webpage

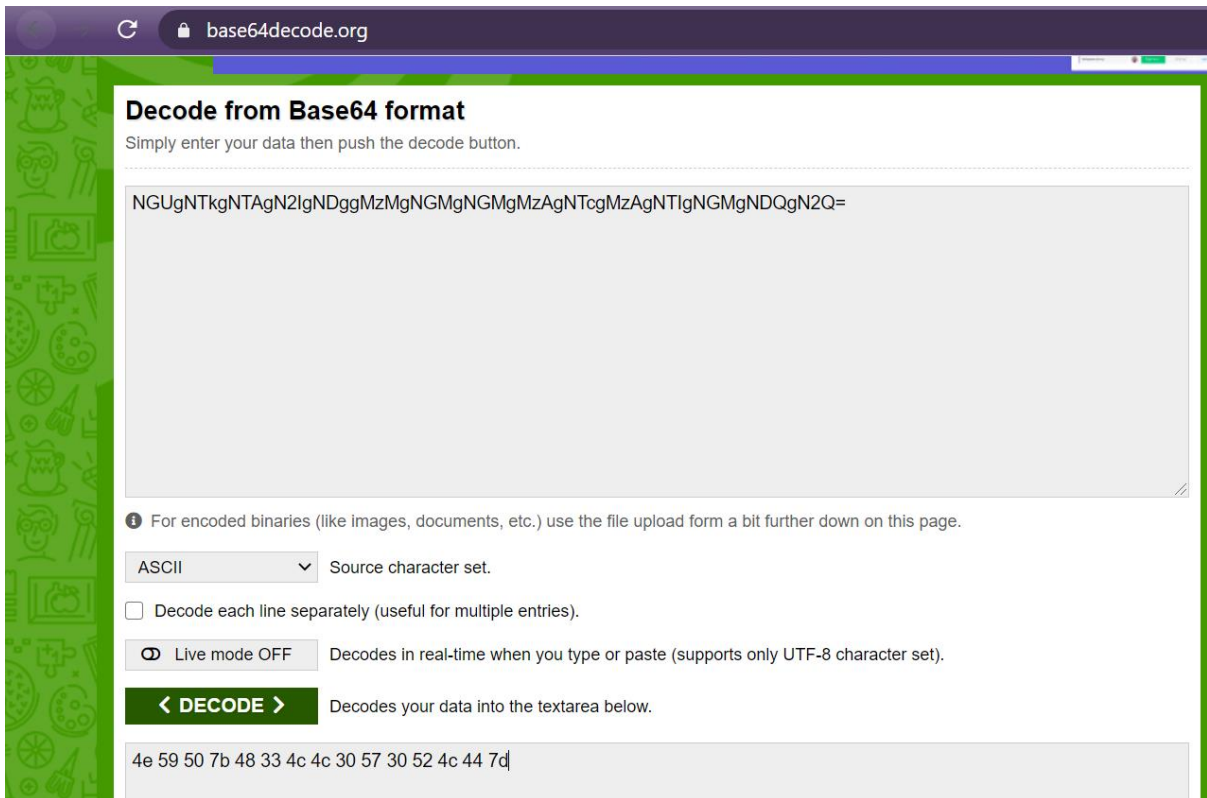


2. Right click -> View Page Source



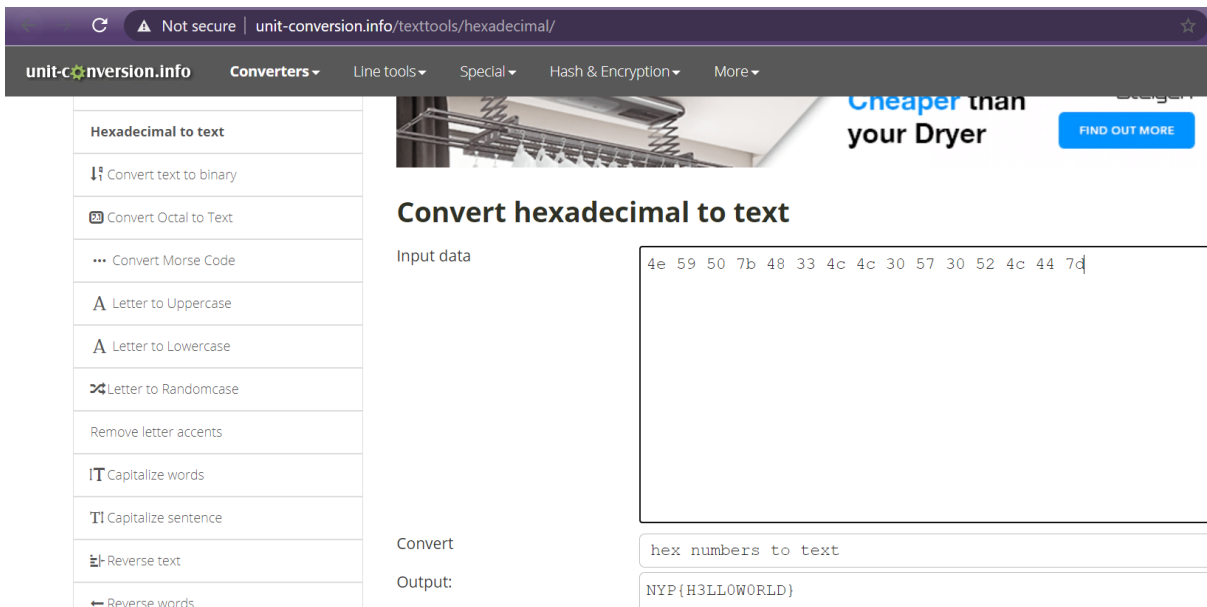
3. From the image above, we obtained a Base64 encoded text  
(NGUgNTkgNTAgNTIgNDggMzMgNGMgNGMgMzAgNTcgMzAgNTIgNGMgNDQgN2Q=)

4. Decode this text and we get a hexadecimal value of 4e 59 50 7b 48 33 4c 4c 30 57 30 52 4c 44 7d



The screenshot shows the base64decode.org website. The main heading is "Decode from Base64 format". Below it, a text area contains the Base64 string: "NGUgNTkgNTAgN2IgNDggMzMgNGMgNGMgMzAgNTcgMzAgNTIgNGMgNDQgN2Q=". Below the text area, there are several options: "Source character set" is set to "ASCII", "Decode each line separately" is unchecked, and "Live mode" is set to "OFF". A green button labeled "< DECODE >" is visible. Below the button, the decoded output is shown in a text area: "4e 59 50 7b 48 33 4c 4c 30 57 30 52 4c 44 7d".

5. Convert the hex value to text and we get NYP{H3LL0WORLD}!

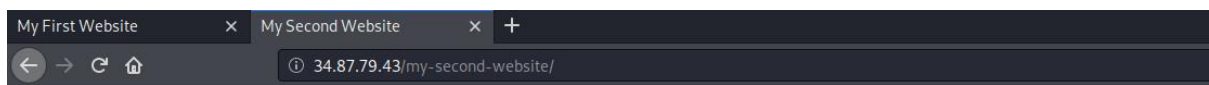


The screenshot shows the unit-conversion.info website. The main heading is "Convert hexadecimal to text". Below it, there is a text area for "Input data" containing the hexadecimal string: "4e 59 50 7b 48 33 4c 4c 30 57 30 52 4c 44 7d". Below the input area, there is a "Convert" button. Below the button, the output is shown in a text area: "NYP{H3LL0WORLD}".



### 3) My Second Website (15 points)

1. Surfing to <http://34.87.79.43/my-second-website/>, we observe the following webpage



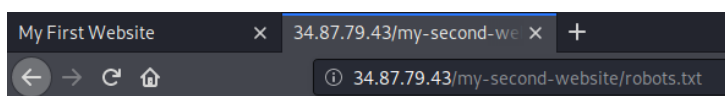
## Welcome to My Second Website

**My first flag was too easy.**

**Now it will be hidden even better, such that even robots cant find it!!!**

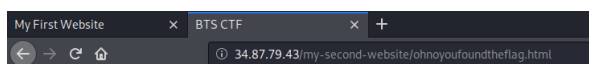


2. Well, that was a very big hint. Surf to <http://34.87.79.43/my-second-website/robots.txt> and we see another hint.



User-agent: \*  
Disallow: /ohnoyoufoundtheflag.html

3. Surf to <http://34.87.79.43/my-second-website/ohnoyoufoundtheflag.html> and we get the flag NYP{ROBOT}

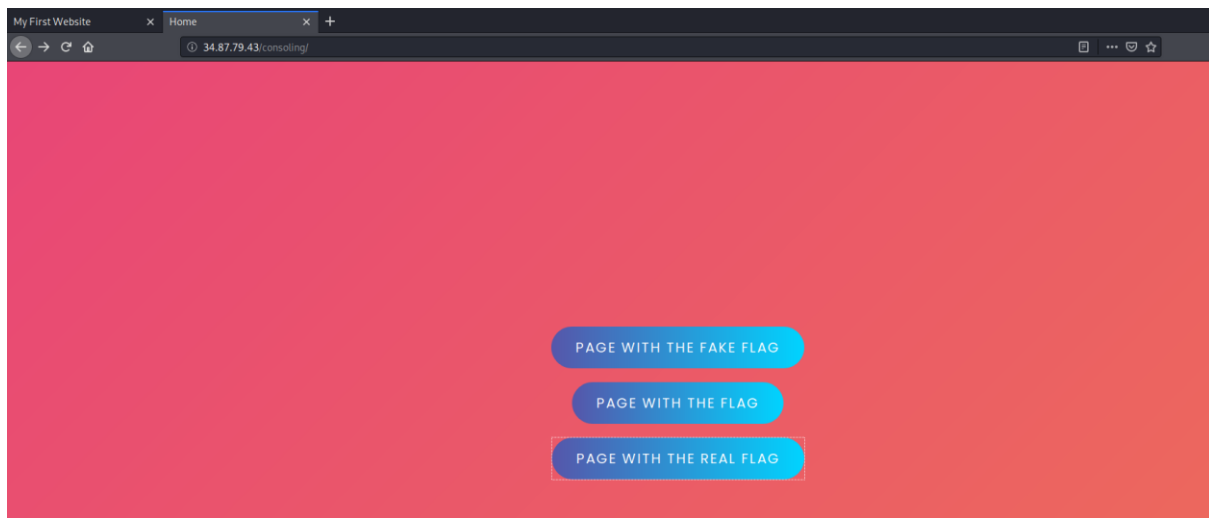


**Wow you are better than a robot!**

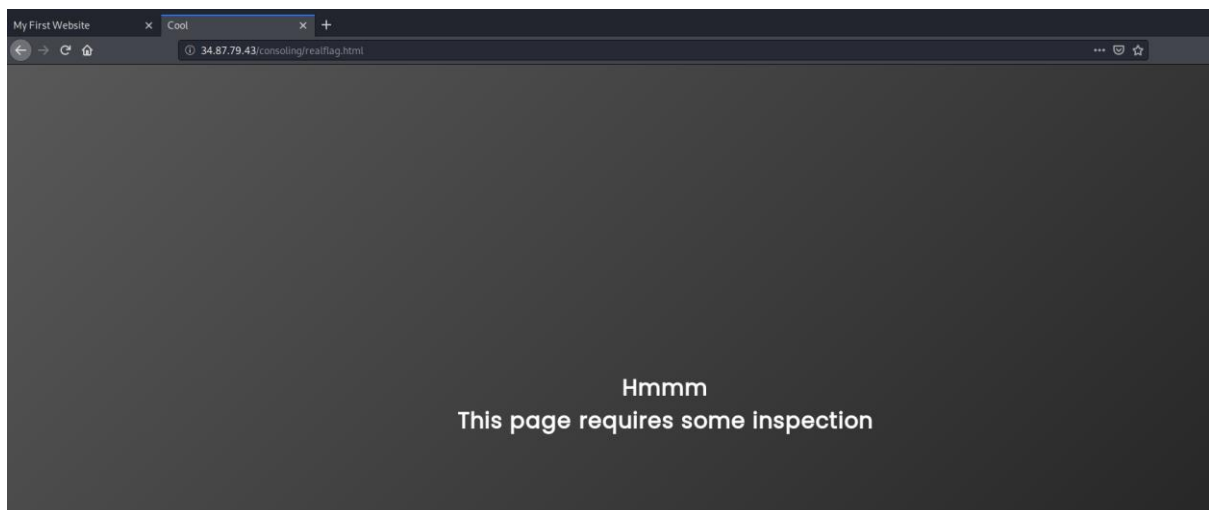
**NYP{ROBOT}**

## 4) Consoling

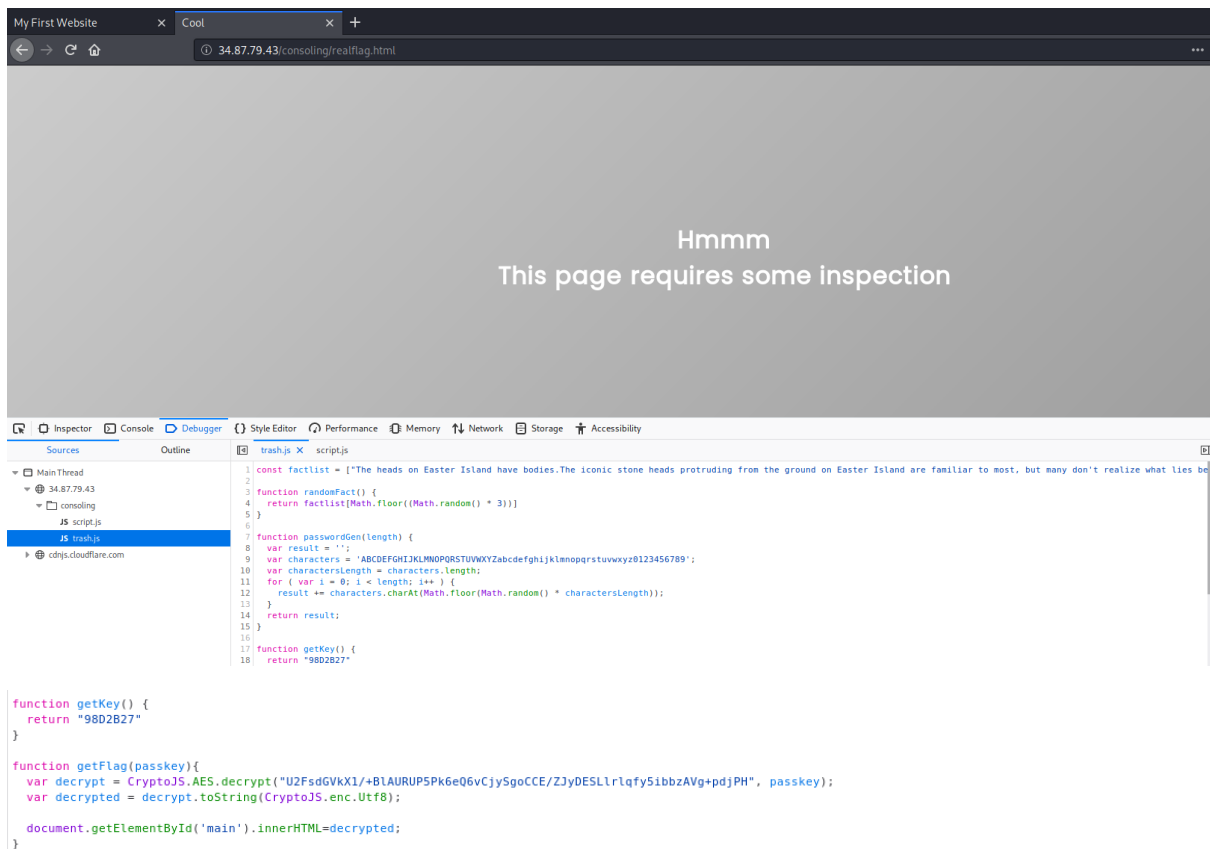
1. Surfing to <http://34.87.79.43/consoling/>, we are presented with the following.



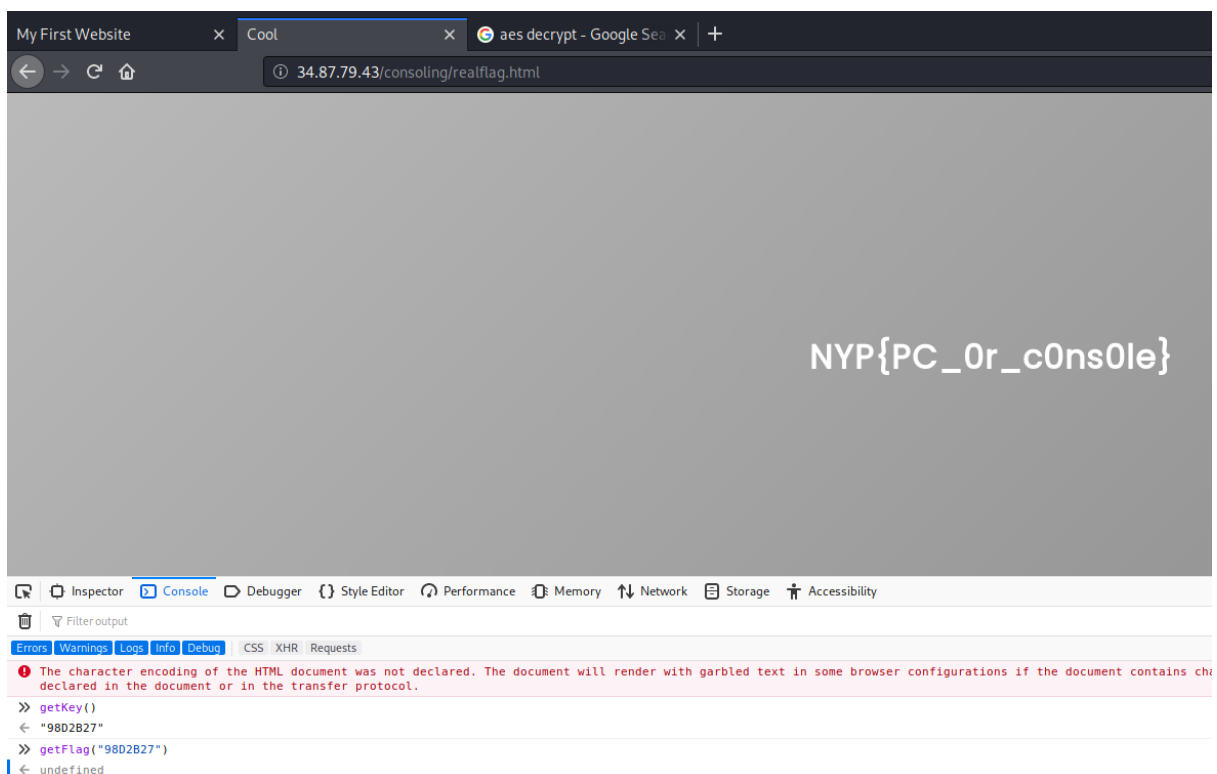
2. Click on “Page with the real flag” and we are redirected to the following webpage  
<http://34.87.79.43/consoling/realflag.html>



3. Right click -> Inspect Element -> Debugger, and we observe a “trash.js” file

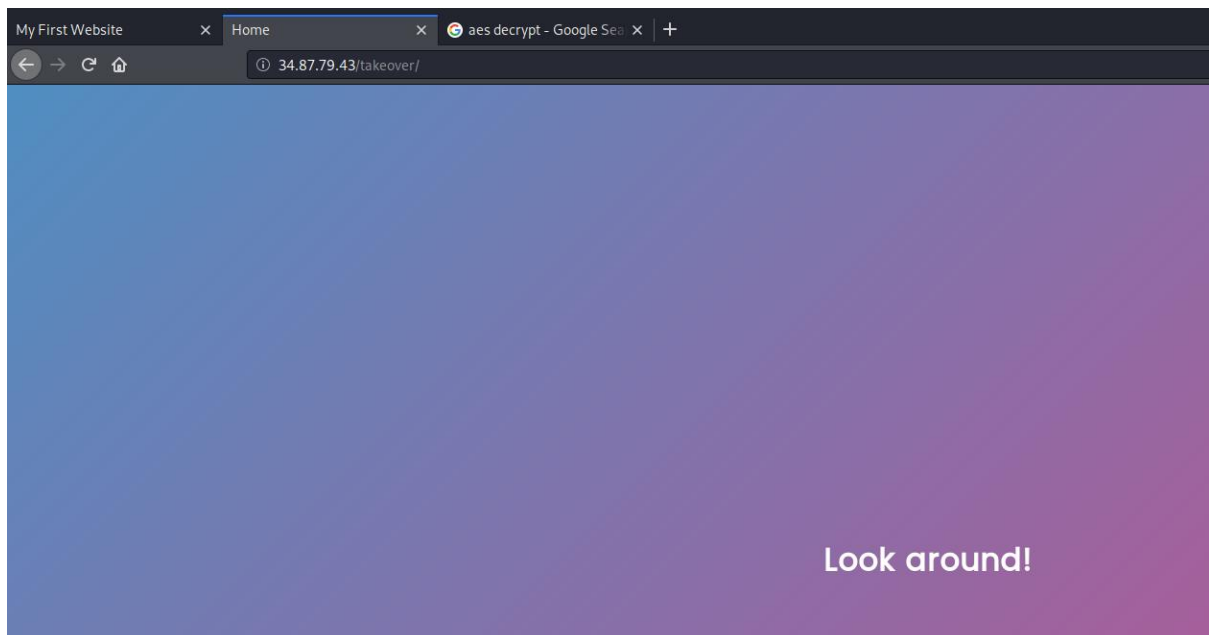


4. Switch from Debugger to Console and type the following (shown bottom) and we get the flag NYP{PC\_Or\_c0ns0le}

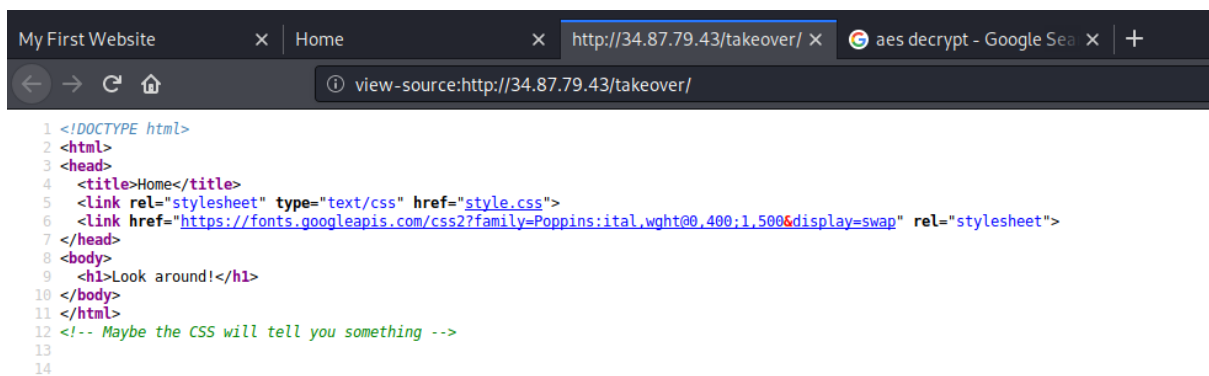


## 5) Takeover (25 points)

1. Surfing to <http://34.87.79.43/takeover> shows us the following.

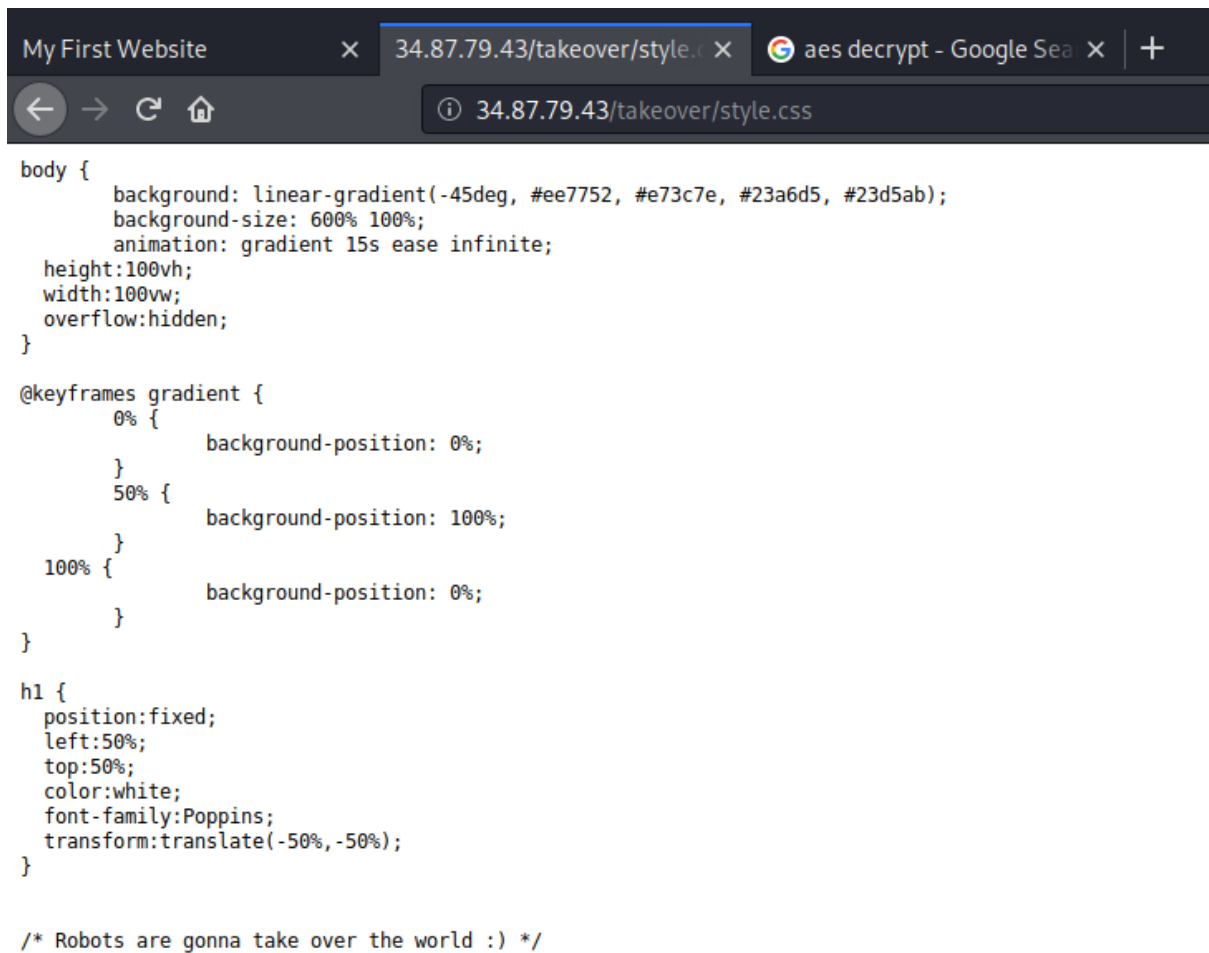


2. Right click -> View Page Source.





3. At <http://34.87.79.43/takeover/style.css>, at the bottom it mentions "Robots".



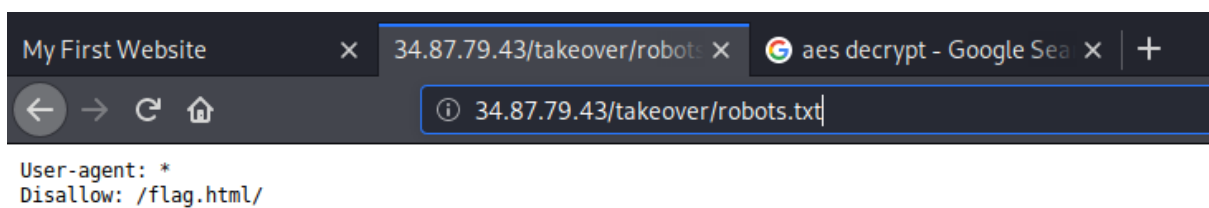
```
body {
  background: linear-gradient(-45deg, #ee7752, #e73c7e, #23a6d5, #23d5ab);
  background-size: 600% 100%;
  animation: gradient 15s ease infinite;
  height:100vh;
  width:100vw;
  overflow:hidden;
}

@keyframes gradient {
  0% {
    background-position: 0%;
  }
  50% {
    background-position: 100%;
  }
  100% {
    background-position: 0%;
  }
}

h1 {
  position:fixed;
  left:50%;
  top:50%;
  color:white;
  font-family:Poppins;
  transform:translate(-50%,-50%);
}

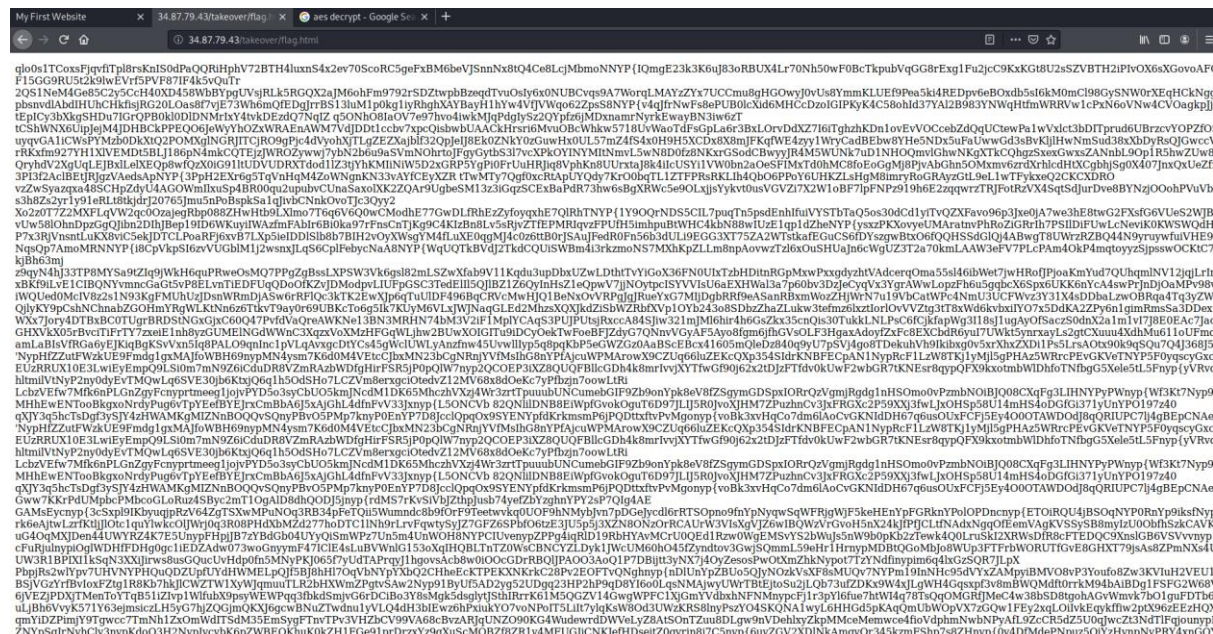
/* Robots are gonna take over the world :) */
```

4. Goto to <http://34.87.79.43/takeover/robots.txt> and notice /flag.html/



```
User-agent: *
Disallow: /flag.html/
```

5. At <http://34.87.79.43/takeover/flag.html>, there's just too many NYP flags!



6. Open terminal and type the following command.

```
root@kali:~/ctf# wget http://34.87.79.43/takeover/flag.html
--2020-10-17 06:37:29-- http://34.87.79.43/takeover/flag.html
Connecting to 34.87.79.43:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 248683 (243K) [text/html]
Saving to: 'flag.html'

flag.html                                100%[=====]
2020-10-17 06:37:29 (7.91 MB/s) - 'flag.html' saved [248683/248683]
```

7. Run the following command and that makes your search easier, and we get NYP{r0b0ts\_ar3\_sc4ry}!

```
root@kali:~/ctf# grep "NYP{" --color flag.html
yHWAAnyP7jYTxrYdEUqcWhkU03jmdjB05yPASjYIYJrvpEPjLj MwbeiLL80D6hnMkUSNJrJz
DW10GozZ5IwGADh1SIoeUX9MYtnrvFSMcnlJkoDcoeP1Wcr4Snp{pUpoGsYOSgN5N07Uzt
sc9Aj4nypbo1eU4CwiekYpEWTjLXV7E6I16rWiBrThsix6SlPlKXo13jN06jt080Ip3gC5e
NAEr139X3lRbTNfDp84KiPNQt0hHGwxNYP{r0b0ts_ar3_sc4ry}8BwFD9nqb0L98MqZdnR
kMFVkwqyLl0oYL4tq0zdzq8clZqWxfmWH8rtiqXW96kmrqyOk8d2ExMeNypNYP0zxA990WSM
DiojRX9veA8HzdvG4xP8Y1R4LA8hx3gP1I2fQkvWJCe7LGrFS6tdNYg9JHMrpQPNyPnHTyt
rQgdnYZKNsMstmvnfs3ENyPSCCLeVJl0RpY0oif2dqoeEgiC0u0feSg8HM5NLZhsXNA9ZiE
us6DetdDWoHgzW2McBgGNZtgQkfVbuZw1KtisgeN42LX4EPAWwX5Hg85EAefJsp1pAdtCo4
w1cXwq5i8BjpgxKFAf1sDsbTG7Y2gKcQfv2Ey5MplB7siZSiMKUEMXBcf5qwJWnFJ6TXgdU
3J0xCIQeXQYXkCP1rp0Jz180ZobcPVCW0poltCN2iKXPPXPZB2EwpzwqfyttLnyp{VYsUu
+G04d4ufb137x0bNTN40k0rNYP{r0b0ts_ar3_sc4ry}8BwFD9nqb0L98MqZdnR
+G04d4ufb137x0bNTN40k0rNYP{r0b0ts_ar3_sc4ry}8BwFD9nqb0L98MqZdnR
```