Web Application Attack

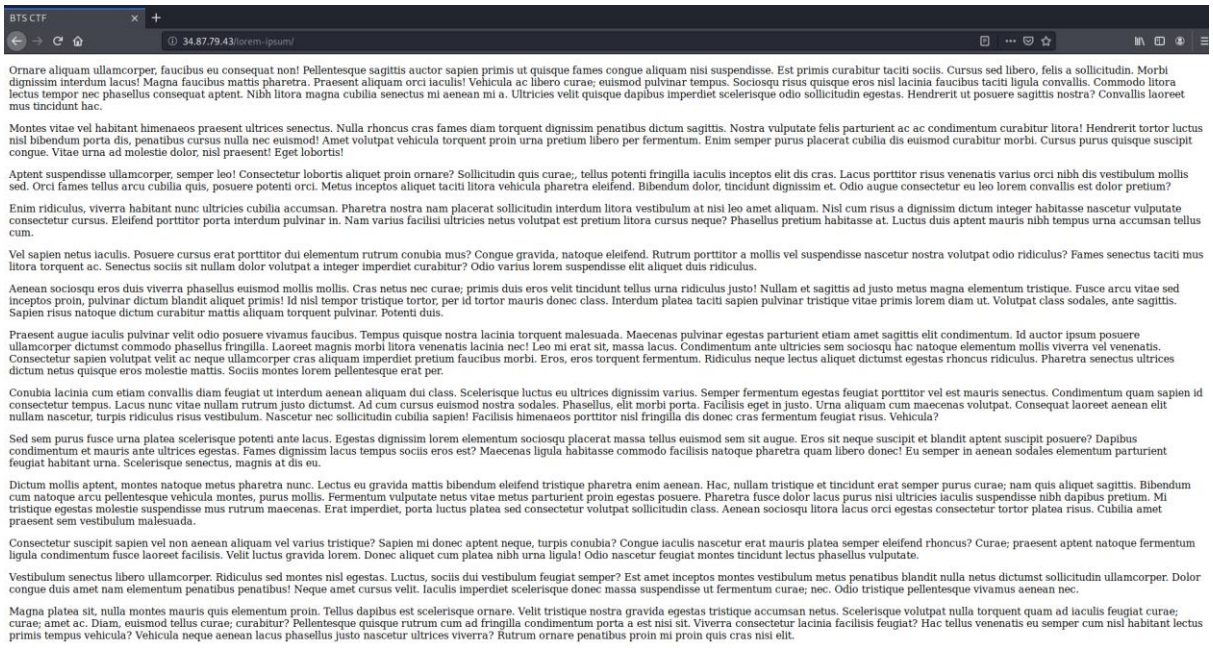
Machines

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

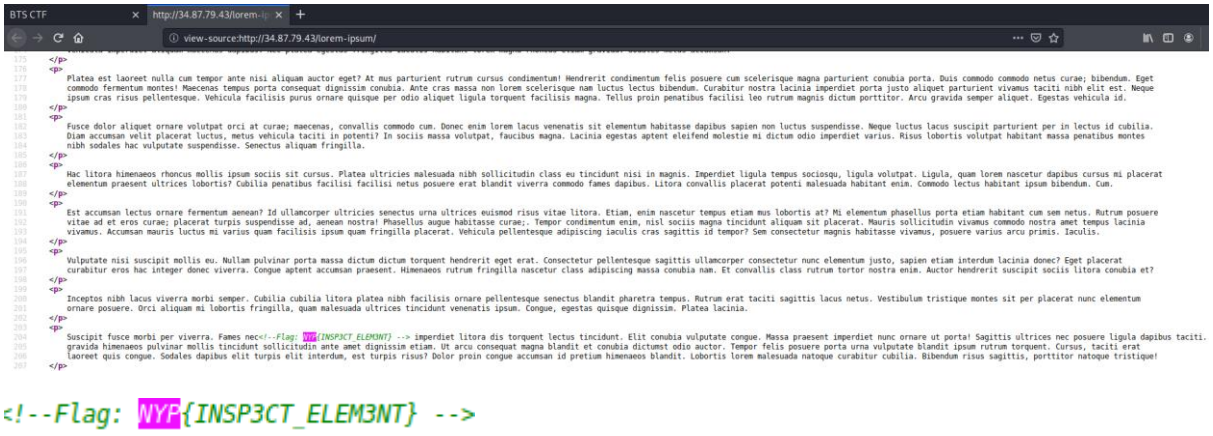
Total – 75 points

1) Lorem Ipsum (10 points)

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



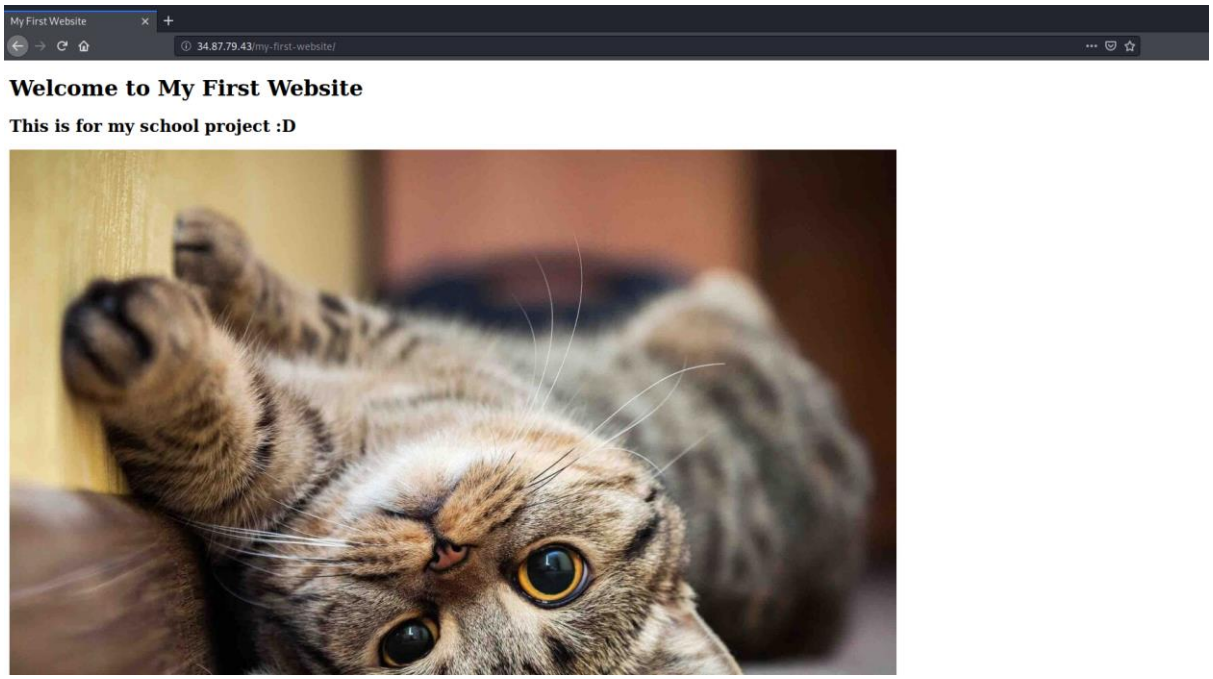
2. Right click -> View Page Source



3. First flag is obtained (NYP{INSP3CT_ELEM3NT})!

2) My First Website (10 points)

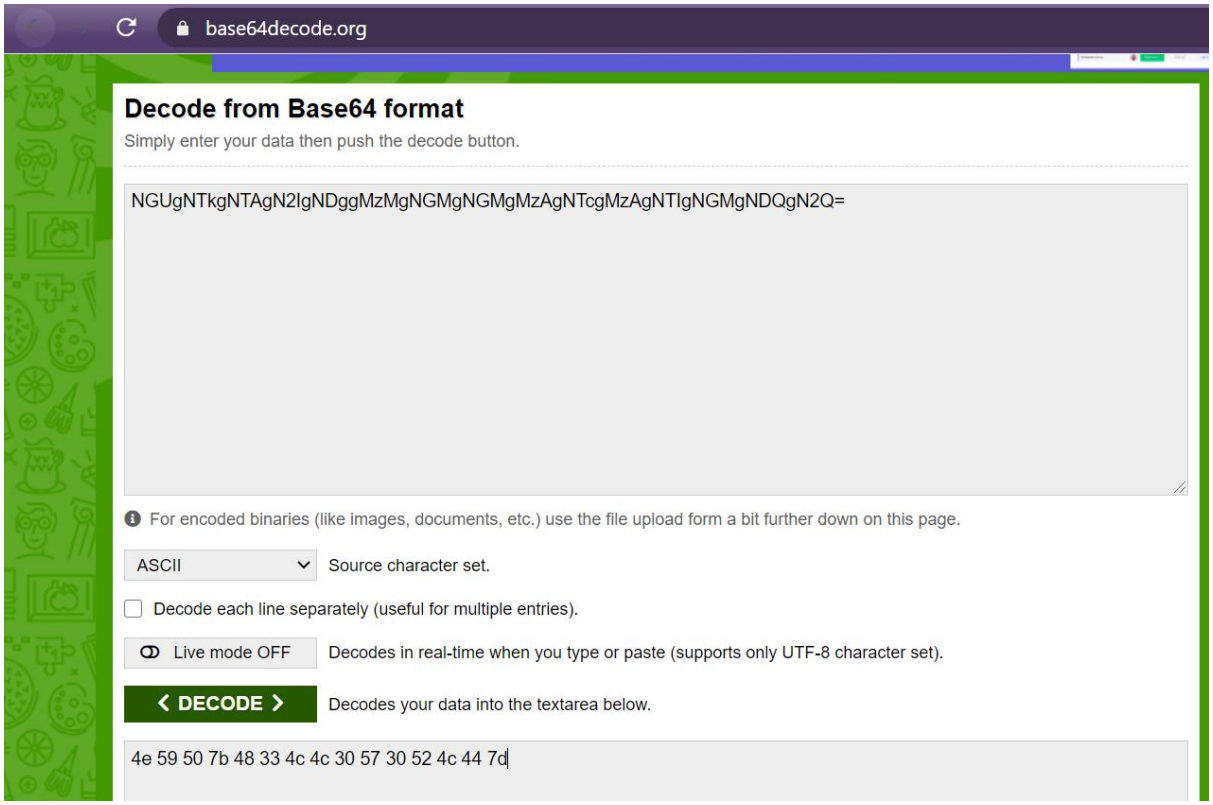
1. Surfing to http://34.87.79.43/my-first-website, we are presented with the following webpage



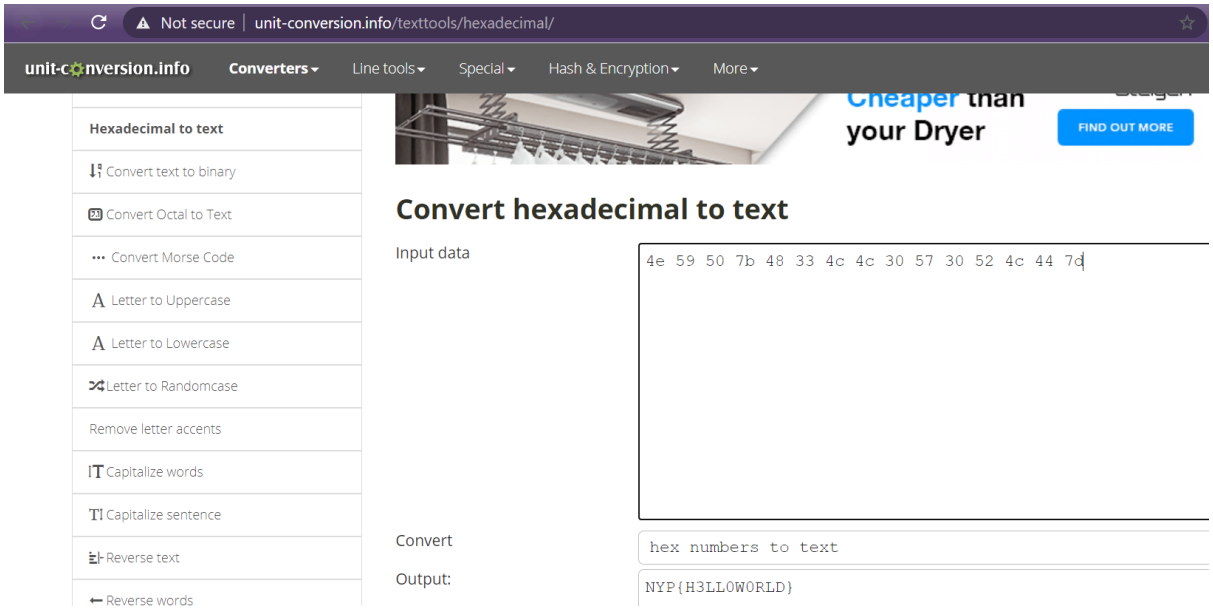
2. Right click -> View Page Source

3. From the image above, we obtained a Base64 encoded text (NGUgNTkgNTAgN2IgNDggMzMgNGMgNGMgMzAgNTcgMzAgNTIgNGMgNDQgN2Q=)

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

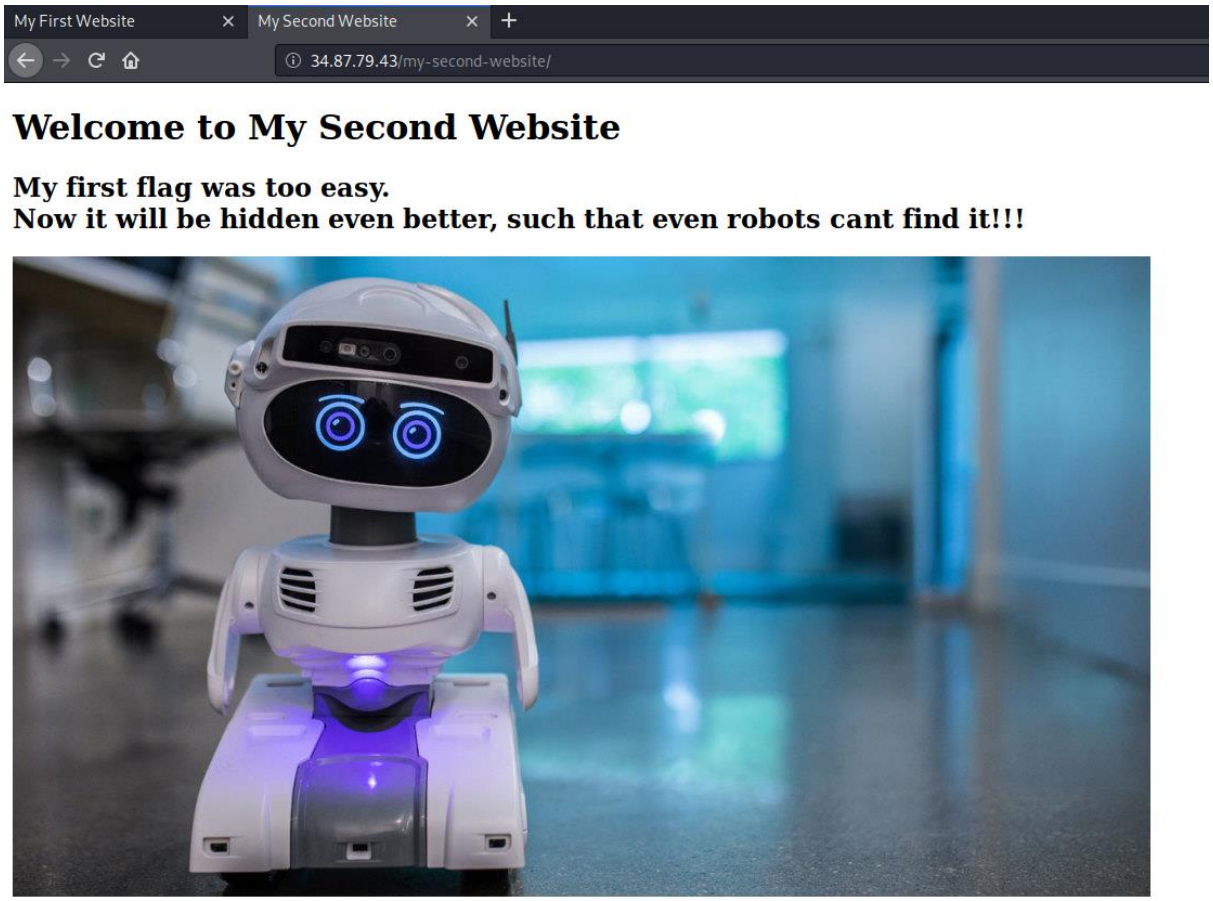


5. Convert the hex value to text and we get NYP{H3LL0W0RLD}!

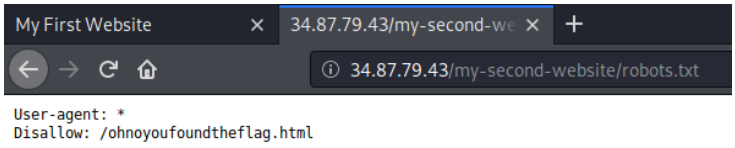


3) My Second Website (15 points)

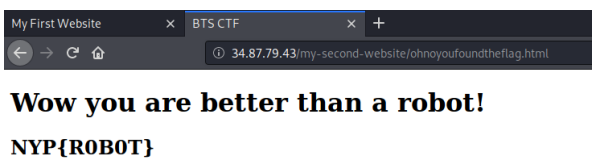
1. Surfing to http://34.87.79.43/my-second-website, we observe the following webpage



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.

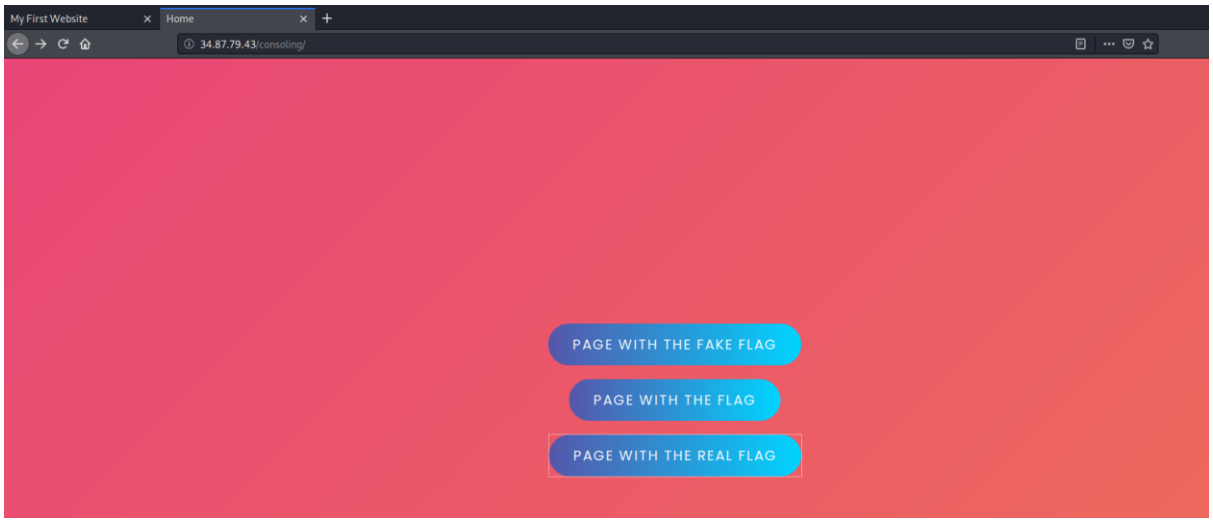


3. Surf to http://34.87.79.43/my-second-website/ohnoyoufoundtheflag.html and we get the flag NYP{R0B0T}

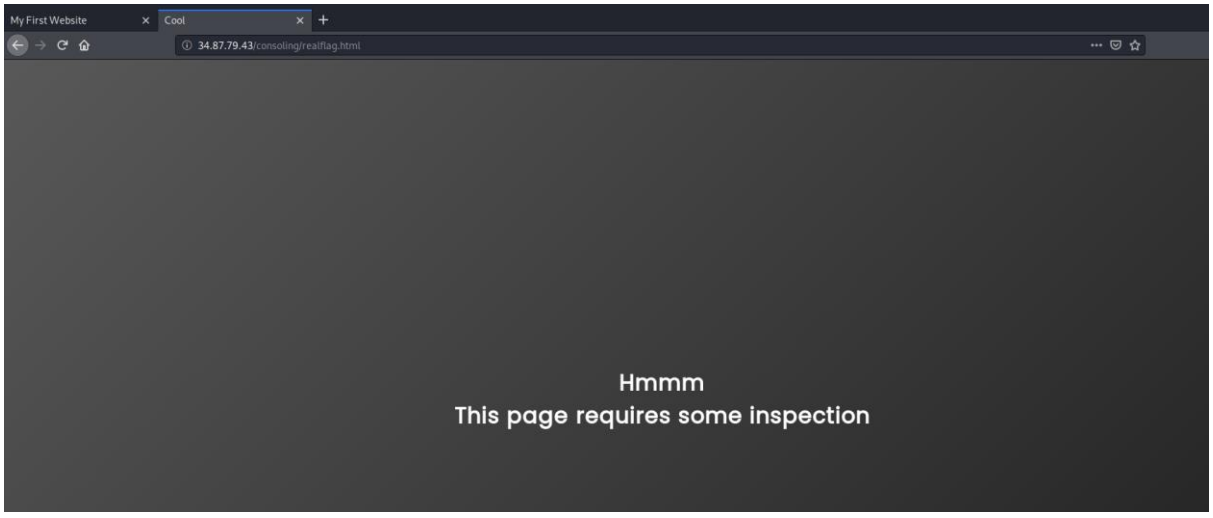


4) Consoling

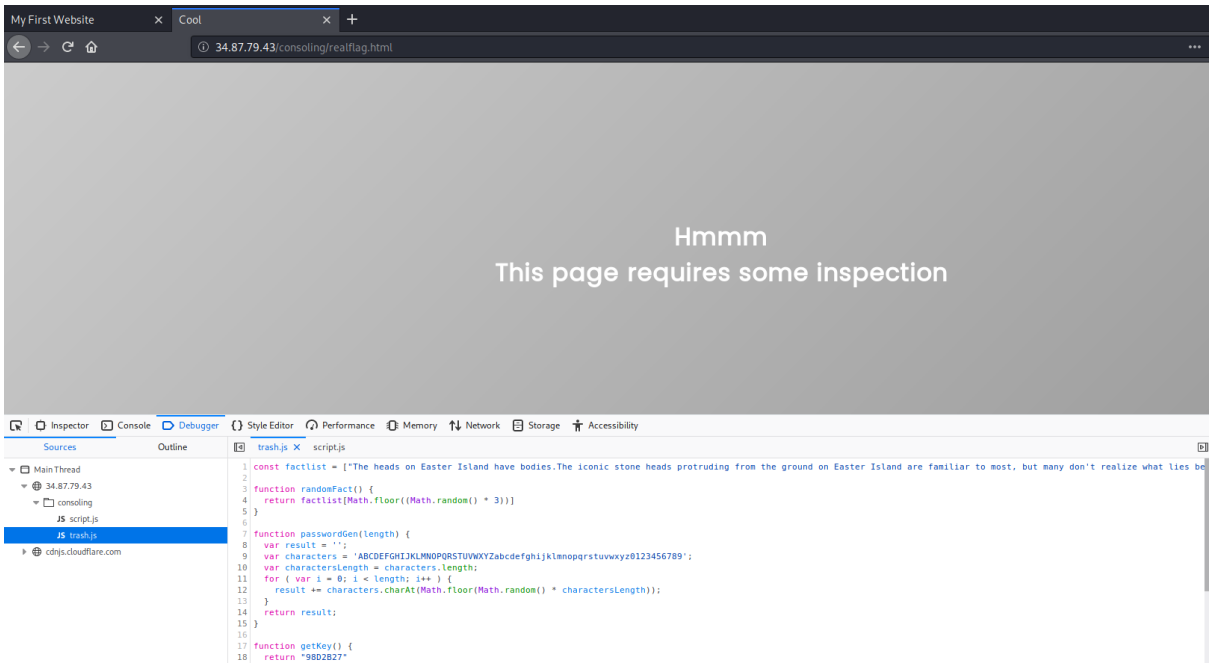
1. Surfing to http://34.87.79.43/consoling/, we are presented with the following.



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

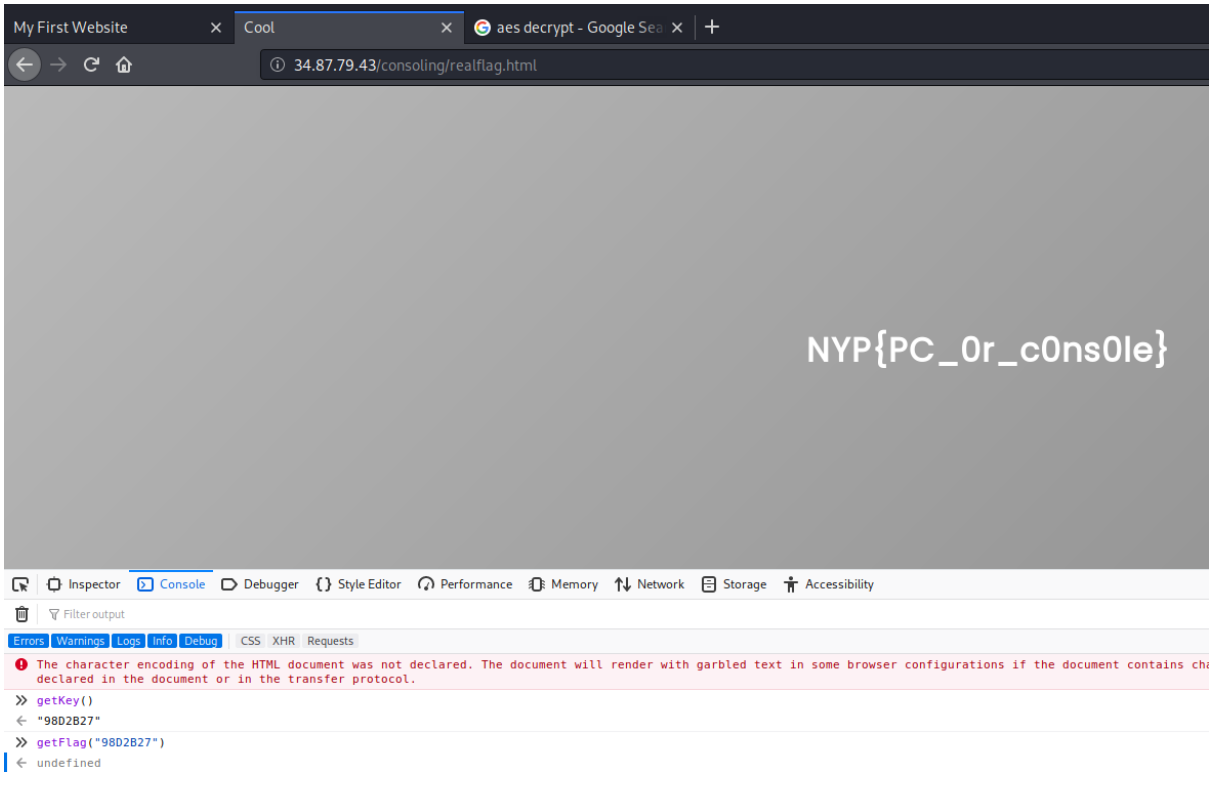


3. Right click -> Inspect Element -> Debugger, and we observe a “trash.js” file



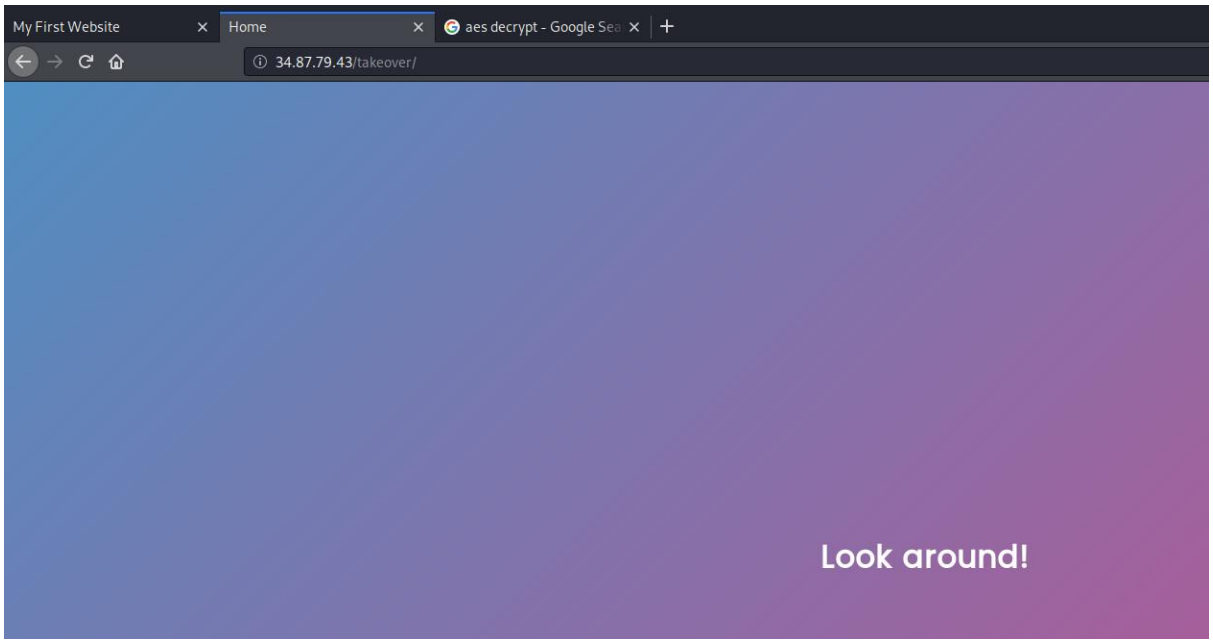

```
function getKey() {
  return "98D2B27"
}

function getFlag(passkey){
  var decrypt = CryptoJS.AES.decrypt("U2FsdGVkX1/+BlAURUP5Pk6eQ6vCjySgoCCE/ZJyDESLlrlqfy5ibbzAVg+pdjPH", passkey);
  var decrypted = decrypt.toString(CryptoJS.enc.Utf8);

  document.getElementById('main').innerHTML=decrypted;
}
```

4. Switch from Debugger to Console and type the following (shown bottom) and we get the flag NYP{PC_0r_c0ns0le}

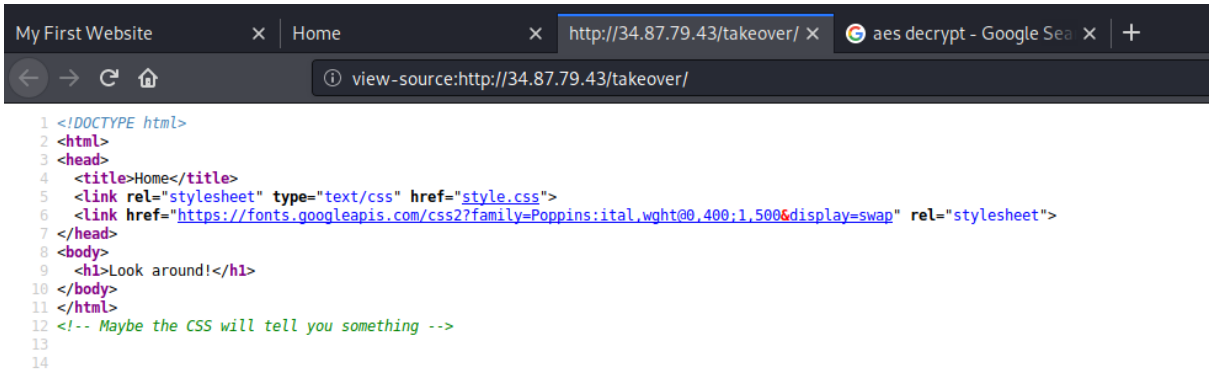


5) Takeover (25 points)

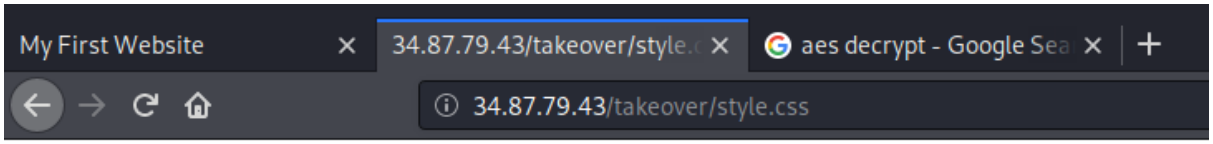
1. Surfing to http://34.87.79.43/takeover shows us the following.



2. Right click -> View Page Source.

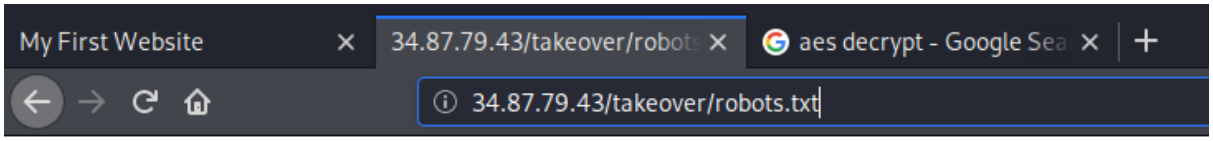


3. At http://34.87.79.43/takeover/style.css, at the bottom it mentions “Robots”.



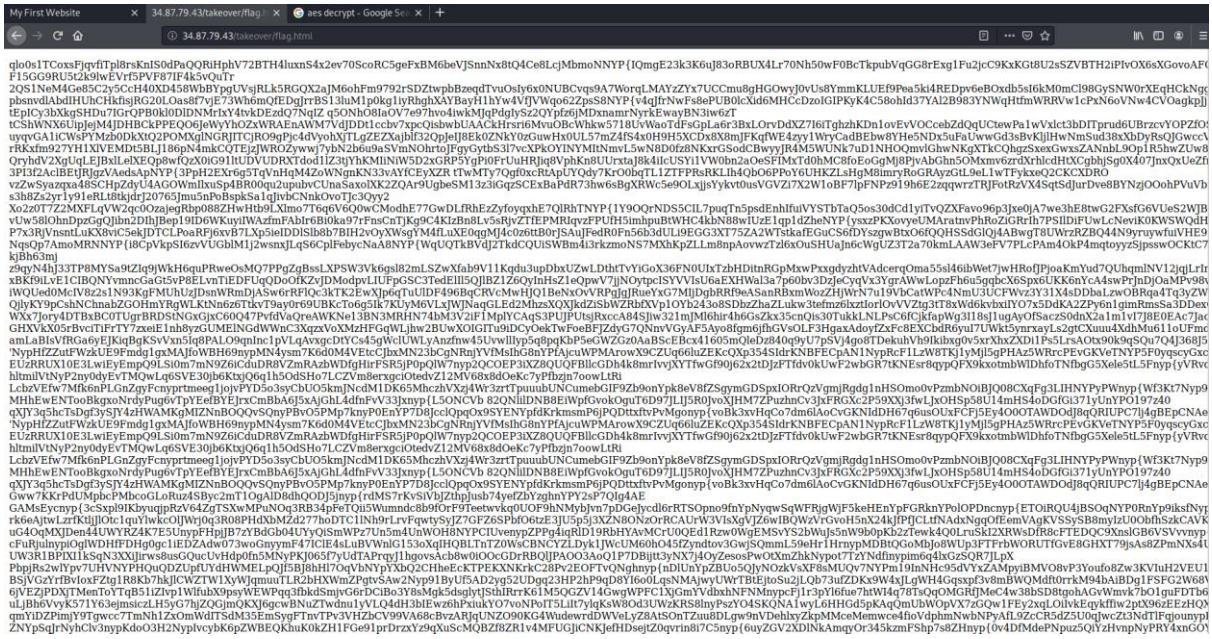

```
body {
        background: linear-gradient(-45deg, #ee7752, #e73c7e, #23a6d5, #23d5ab);
        background-size: 600% 100%;
        animation: gradient 15s ease infinite;
  height:100vh;
  width:100vw;
  overflow:hidden;
}

@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.

7. Run the following command and that makes your search easier, and we get NYP{r0b0ts_ar3_sc4ry}!