Assignment 3

Phase 1-

This phase's name is cookies.So, from the name itself I figure it out that flag is hidden inside the cookie so i clicked on the provided link and inspected that page . In inspect, go to application and cookies . Inside the cookie there is one link when i click on that i got one table with value, name and other data. According to the values of cookies, the page content is changed.

There is some range for the cookies so i tried brute force and got 28 is the highest last valid value for cookies so, i tried all the values, and on value 18 I got my flag value.

Flag is :-picoCTF{3v3ry1_l0v3s_c00k135_bb3b3535}

Phase 2-

When I open the website it says inspect me so when I click on view source code at the bottom, it gives me 1/3rd part of the flag, which is’ picoCTF{tru3_d3’ after this, the exploit can hidden inside the CSS or javascript file so from the source code itself when I open the css code in the bottom I got 2/3rd part of the flag which is ‘ t3ct1ve_0r_ju5t’ after this I checked the javascript file inside that I got the 3rd part ‘_lucky?f10be399}’

Flag is -picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?f10be399}

Phase 3-

When i click on the site and check the source code of that it gives me something like this

```
if (checkpass.substring(0, split) == 'pico') {
if (checkpass.substring(split*6, split*7) == '723c') {
if (checkpass.substring(split, split*2) =='CTF{') {
if (checkpass.substring(split*4, split*5)== 'ts_p') {
if (checkpass.substring(split*3, split*4) == 'lien') {
if (checkpass.substring(split*5, split*6)== 'lz_7') {
if (checkpass.substring(split*2, split*3)== 'no_c') {
if (checkpass.substring(split*7, split*8)== 'e}') {
alert("Password Verified")
```

From the above, I understand that I got a flag but it is not arranged in the correct form like

0,split is ‘pico’so after this split,split*2 should come whose value is ‘CTF{’ so like this i arranged in ascending / serial order and got a flag

Flag is – ‘picoCTF{no_clients_plz_7723ce}’

Phase 4–

For this phase initially it is hard to figure it out that where is flag after read from the hint i got that flag is hidden inside the source code but when i open the source code it says “Only User who use pico Browser are allowed” So to perform this i used Burp Suit tool using this we can modify our html request page and also see our response html page parallelly.

In Burp suit using his own browser first i open the link which is given in problem after that i click on Repeater which show me both request and response html page .

Now to Convey the msg that yes i m using PicoBrowser i change the user-agent part of the html request page to PicoBrowser and send the request.

After this the response page says that “I dont users visiting from another sites ”

So, in request html page referer : http://mercury.picoctf.net:1270 referer tells from where it request coming from. So again send request and got response that “this site is worked only in 2018” so for this in request page i add Date:2018

After this in response it said “i dont want to be tracked” so i add DNT:dntand after this it is for sweden people so, i add sweden ip x-forwarded-for : Sweden ip(102.177.146.0) then it says for people who speaks sweden so in header i add Accept-language :sv After this i got the response with my flag value.

Flag is : picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_f56f58a5}

Phase 5: -

When I click on the link and see the source code there are two files where flag may be hidden first in CSS and another javascript file. In CSS file nothing is strange but when i opened the javascript file i found this” Your flag is ${atob(t.p)}” which means flag value is this , I only we need to decode the flag so in that code only i found btoa() function which decode string to base64 so to get the correct value i used command echo value | base64 -d gives me the correct value and as i know that password is my flag so i put password in place of value that is “cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ”

And i got the flag

Flag is picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}.