

WRITE - UP



IT NUMBER: IT22345332

NAME: G.P DINUJAYA THAMARA

WEEKEND BATCH

MALABE CAMPUS

1. where are the robots

where are the robots 

 | 100 points 

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ZARATEC/DANNY



Hints 

Description

1

Can you find the robots? <https://jupiter.challenges.picoctf.org/problem/60915/>
(link) or <http://jupiter.challenges.picoctf.org:60915>

55,779 solves / 59,505 users attempted (94%)

 84% Liked 

 picoCTF{FLAG}

Submit Flag

this is where link directs to

Welcome

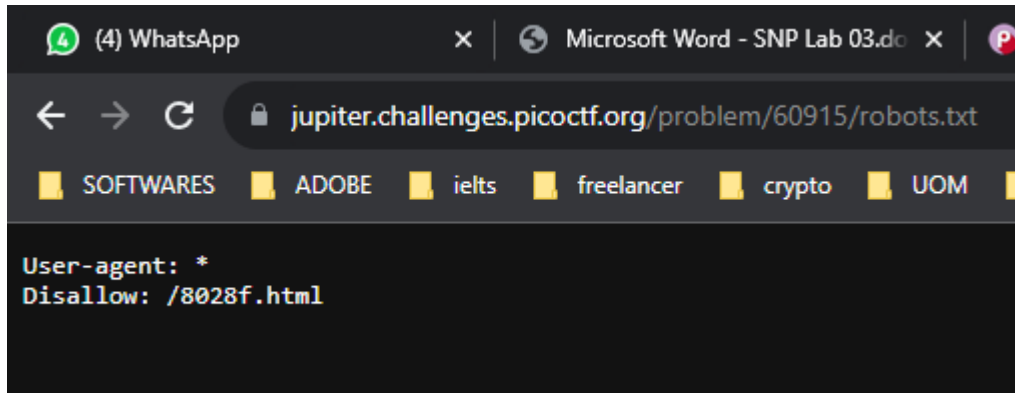
Where are the robots?

What part of the website could tell you where the creator doesn't want you to look? Is the hint given by them which makes sense to move to **robots.txt** file?

/robots.txt file is a standard used to provide instructions to web crawlers or "robots" about which parts of a website should or should not be crawled, indexed, or accessed. It is commonly used to control how search engines and other automated agents interact with a website

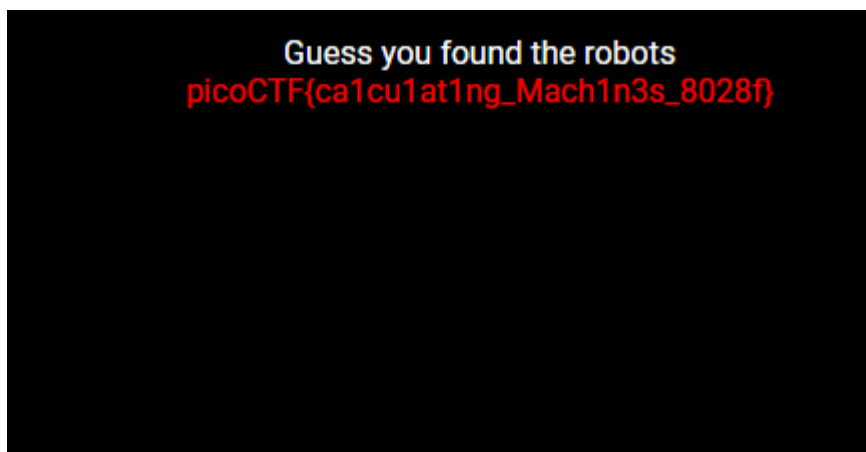
<https://jupiter.challenges.picoctf.org/problem/60915/robots.txt>

After I moved to robots.txt file it gives me the hint where to go next




could be a URL pointing to a specific web page that contains information relevant to the challenge. So visit that page by changing the last part of the URL as follows.

<https://jupiter.challenges.picoctf.org/problem/60915/8028f.html> after I change the URL I got the flag.



2. Scavenger Hunt

Scavenger Hunt | 50 points Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS


Hints 

Description

There is some interesting information hidden around this site
<http://mercury.picoctf.net:39698/>. Can you find it?

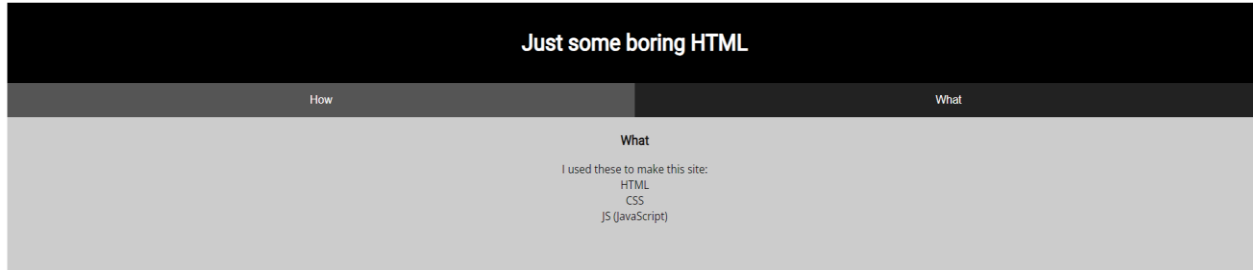
1

36,471 solves / 42,556 users attempted (86%)

 63% Liked  picoCTF{FLAG}

Submit Flag

When the following link is clicked it directs to a below webpage



So, when I visited the website as for the first step, I checked with the inspect element.

There were no clues to be found in that, so after that I moved to page source which gives the first part of the flag.

```
<!doctype html>
<html>
  <head>
    <title>Scavenger Hunt</title>
    <link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="mycss.css">
    <script type="application/javascript" src="myjs.js"></script>
  </head>

  <body>
    <div class="container">
      <header>
        <h1>Just some boring HTML</h1>
      </header>

      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen">How</button>
      <button class="tablink" onclick="openTab('tababout', this, '#222')">What</button>

      <div id="tabintro" class="tabcontent">
        <h3>How</h3>
        <p>How do you like my website?</p>
      </div>

      <div id="tababout" class="tabcontent">
        <h3>What</h3>
        <p>I used these to make this site: <br/>
          HTML <br/>
          CSS <br/>
          JS (JavaScript)
        </p>
        <!-- Here's the first part of the flag: picoCTF{t -->
      </div>

    </div>

  </body>
</html>
```

After I click mycss.css file I got the second part of the flag

```
}  
  
h1 {  
    color: white;  
}  
  
p {  
    font-family: "Open Sans";  
}  
  
.tablink {  
    background-color: #555;  
    color: white;  
    float: left;  
    border: none;  
    outline: none;  
    cursor: pointer;  
    padding: 14px 16px;  
    font-size: 17px;  
    width: 50%;  
}  
  
.tablink:hover {  
    background-color: #777;  
}  
  
.tabcontent {  
    color: #111;  
    display: none;  
    padding: 50px;  
    text-align: center;  
}  
  
#tabintro { background-color: #ccc; }  
#tababout { background-color: #ccc; }  
  
/* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_10 */
```

After that I clicked the myjs.js file to get some more clues in that there was a comment which gives a certain hint to move to robots.txt file

```
function openTab(tabName,elmnt,color) {
  var i, tabcontent, tablinks;
  tabcontent = document.getElementsByClassName("tabcontent");
  for (i = 0; i < tabcontent.length; i++) {
    tabcontent[i].style.display = "none";
  }
  tablinks = document.getElementsByClassName("tablink");
  for (i = 0; i < tablinks.length; i++) {
    tablinks[i].style.backgroundColor = "";
  }
  document.getElementById(tabName).style.display = "block";
  if(elmnt.style != null) {
    elmnt.style.backgroundColor = color;
  }
}

window.onload = function() {
  openTab('tabintro', this, '#222');
}

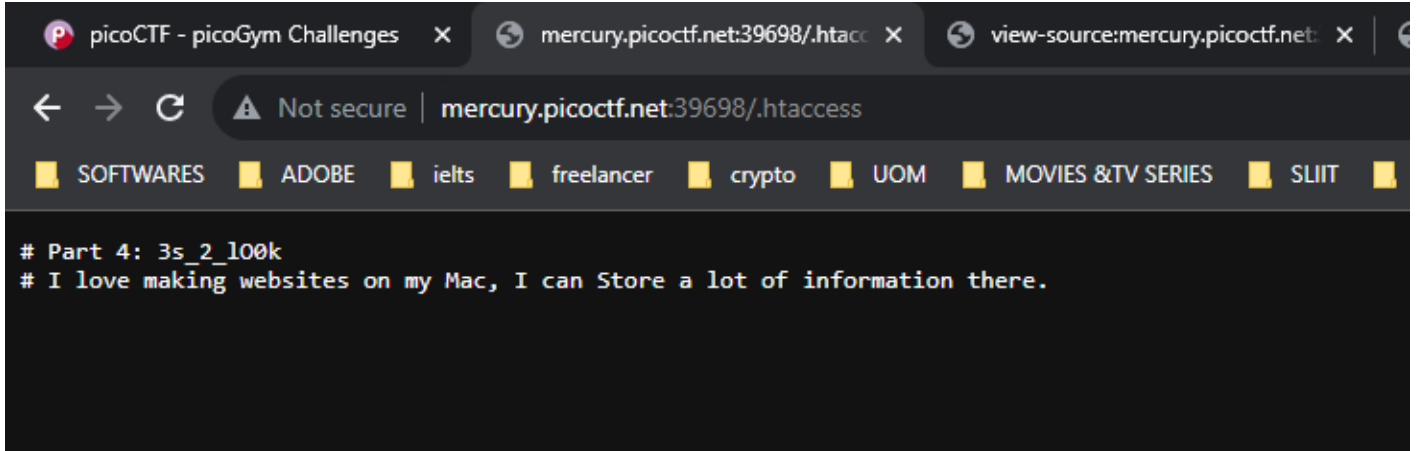
/* How can I keep Google from indexing my website? */
```

<http://mercury.picocft.net:39698/robots.txt> so when I moved to the robots file it gives me third part of the flag with some additional hints.

```
User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

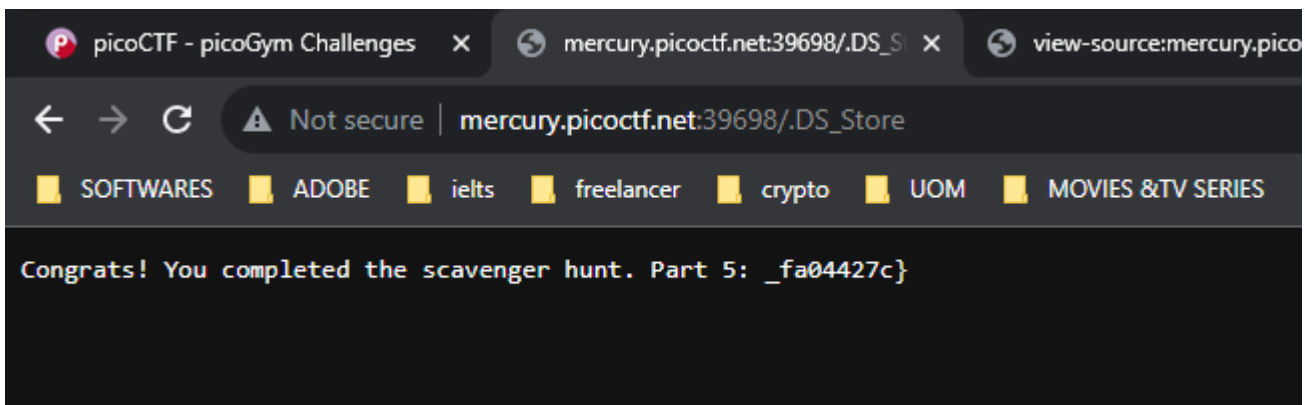
Since it has given a hint, **you have to access the Apache server.**

Through this file configuration (**/.htaccess**) we can access Apache web servers, The **.htaccess** (hypertext access) file is a configuration file used by Apache web servers to control various aspects of how a directory and its subdirectories behave. It can be used to set up authentication, URL rewriting, access control, and more.



In that I found the fourth part of the flag and another hint which says that he likes to store information on a mac. Which is probably a reference for the **.DS_Store**

.DS_Store is a file created by macOS operating systems to store custom attributes of a folder, such as the position of icons or background images. **These files are usually hidden and contain metadata about the folder's appearance and arrangement.**



3. login

login



 | 100 points 

Tags: picoMini by redpwn Web Exploitation

AUTHOR: BROWNIEINMOTION

Description



My dog-sitter's brother made this website but I can't get in; can you help?

login.mars.picoctf.net

Hints 

(None)

27,169 solves / 28,760 users attempted (94%)

 88% Liked 

 picoCTF{FLAG}

Submit Flag

When the link is clicked, it directs to the following page

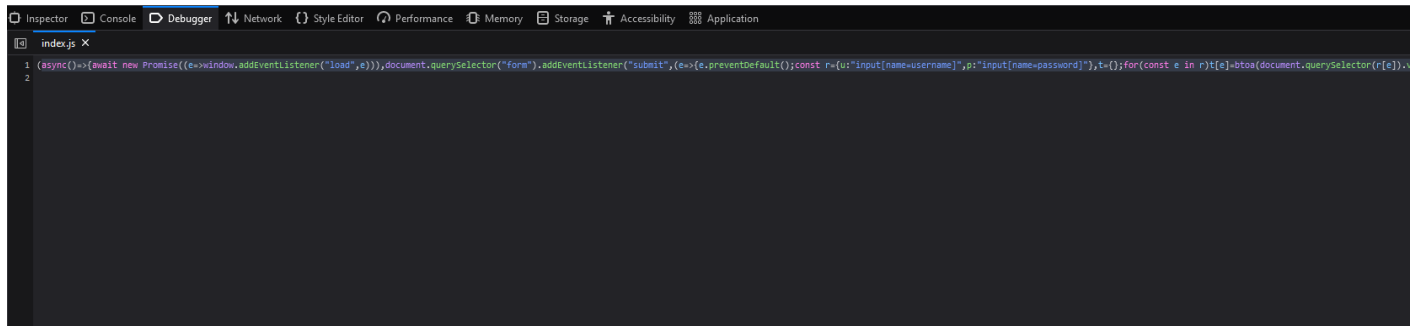
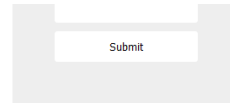
Login

Username

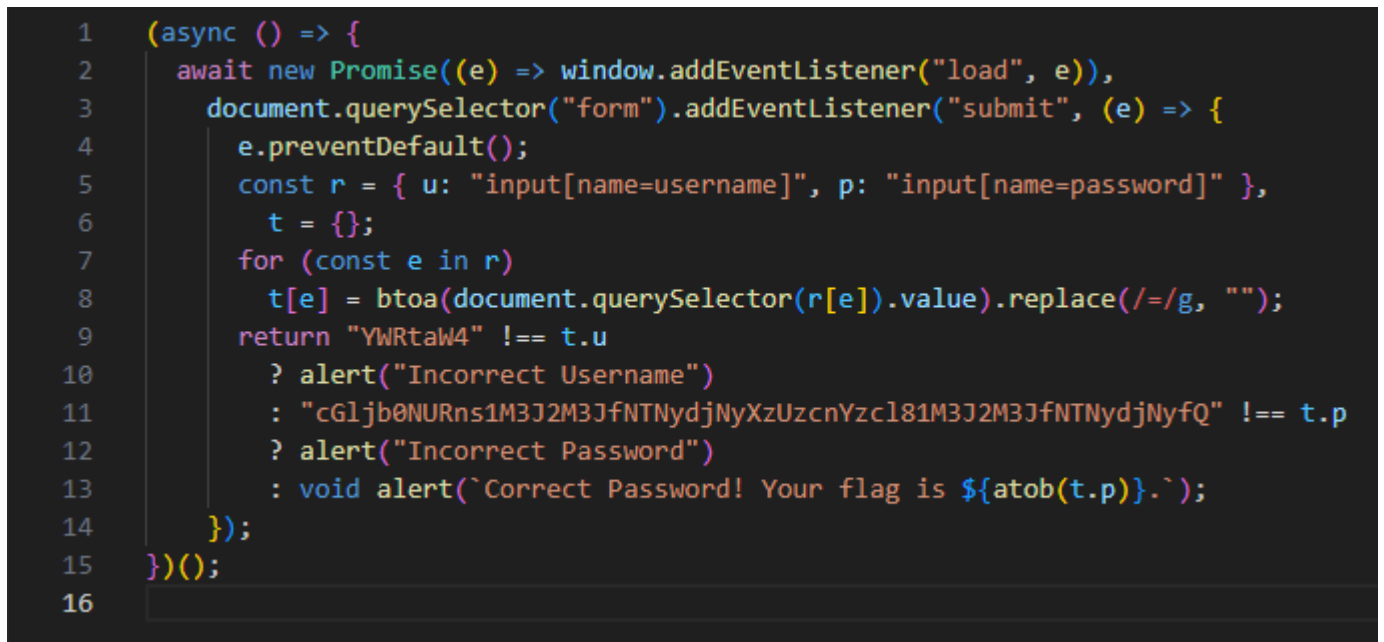
Password

Submit

As the first step check the inspect element to find clues in there were no clues in the html and css page and then lastly I check the js file



Since all the codes are in one line, its bit hard to identify so I copied in the vs and click format document which looks more clearer which is like this



In here **btoa** means encoding a string in base-64

for example `btoa("abc")` gives the output as "YWJj" where "abc" is encoded in base-64

`t[e] = btoa(document.querySelector(r[e]).value).replace(/=/g, "");` This code seems to be designed to encode values from HTML input elements and remove any equal signs (=) from the encoded output.

YWRtaW4 this in **base 64** when it is converted to **ASCII text** it gives **admin**

☐ 0x/0b prefix

ASCII text

admin

Hex (bytes)

61 64 6D 69 6E

Binary (bytes)

01100001 01100100 01101101 01101001 01101110

Decimal (bytes)

97 100 109 105 110

Base64

YWRtaW4=

Length (bytes)

`Correct Password! Your flag is \${atob(t.p)}.` from this string we can identify that we should convert the base 64 password to ASCII text to get the flag

Number delimiter

Space

☐ 0x/0b prefix

ASCII text

picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}

Hex (bytes)

70 69 63 6F 43 54 46 7B 35 33 72 76 33 72 5F 35 33 72 76 33
72 5F 35 33 72 76 33 72 5F 35 33 72 76 33 72 5F 35 33 72 76

Binary (bytes)

01110000 01101001 01100011 01101111 01000011 01010100
01000110 01111011 00110101 00110011 01110010 01110110

Decimal (bytes)

112 105 99 111 67 84 70 123 53 51 114 118 51 114 95 53 51 114
118 51 114 95 53 51 114 118 51 114 95 53 51 114 118 51 114 95

Base64

cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ==

Length (bytes)

43

Checksum

8-bit

Sum

C5

13

4. GET aHEAD

GET aHEAD 

 | 20 points 

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Description

Find the flag being held on this server to get ahead of the competition

<http://mercury.picoctf.net:34561/>

Hints 

1 2

Check out tools like Burpsuite to modify your requests and look at the responses

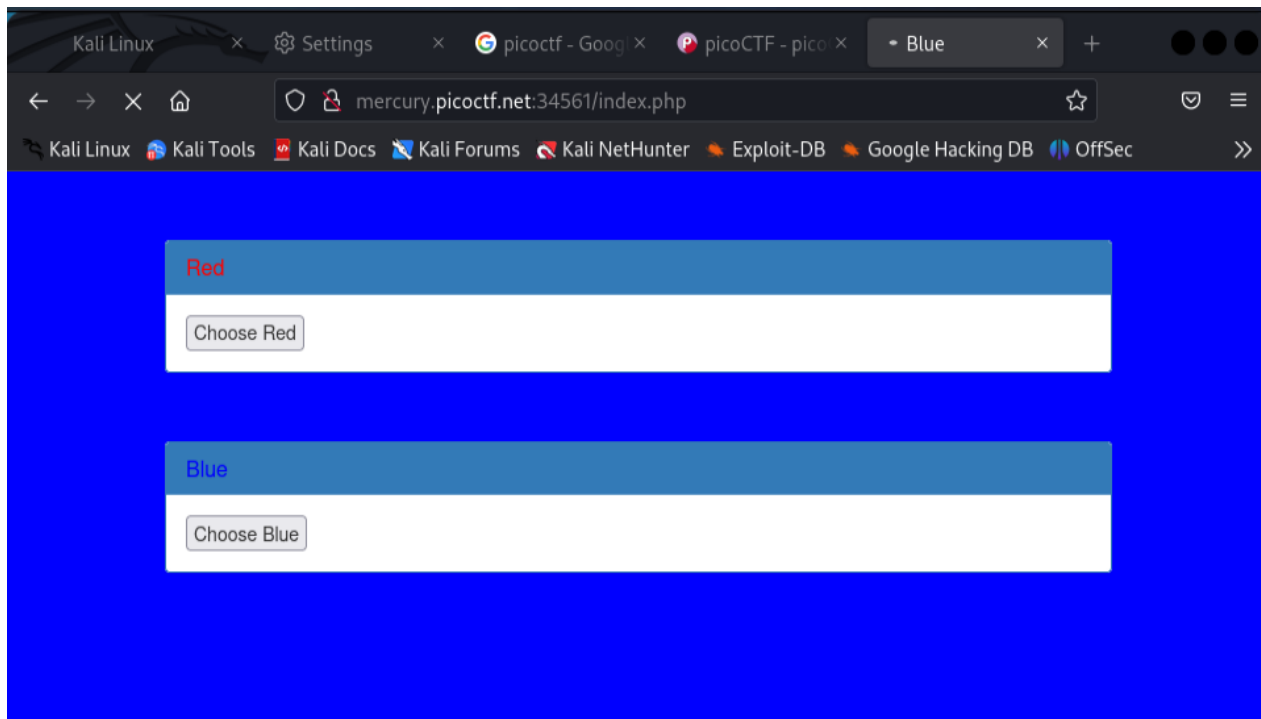
59,445 solves / 64,327 users attempted (92%)

 82% Liked 

 picoCTF{FLAG}

Submit Flag

Once I clicked the above link it redirected me to the following page



As usual, I moved to the inspect element and page sources there was a clue, these two colors use two different request methods.

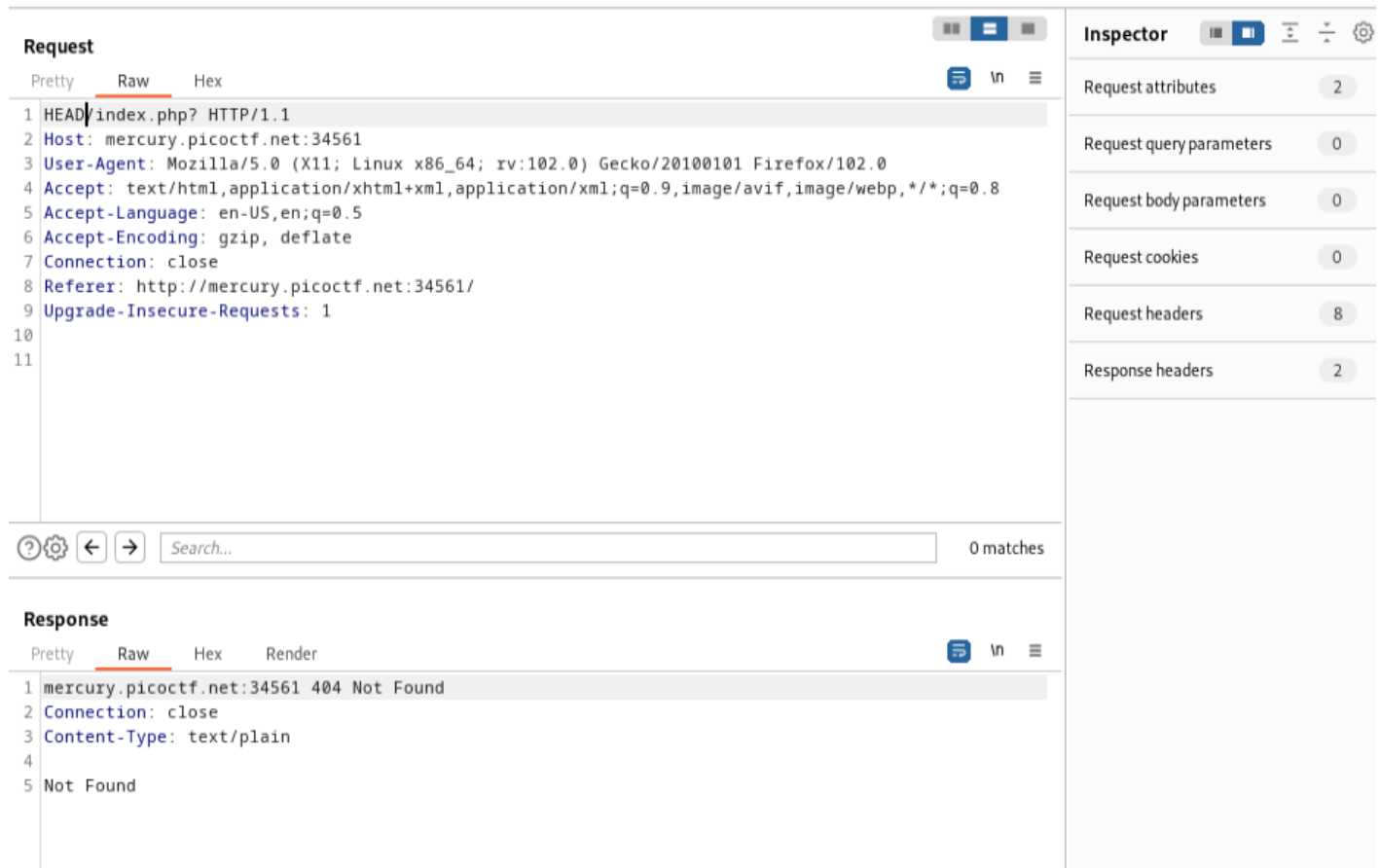
Red uses GET method.

Blue use POST method.

When we look at Request and respond headers inspectors they look perfectly normally

Since the challenge name also GET aHEAD I thought of changing the request method from GET to HEAD for that I **click send to repeater** then we can change any request. And click Send button

It gives me nothing.



The screenshot shows the Chrome DevTools interface. The 'Request' tab is active, displaying a HEAD request to `mercury.picocftf.net:34561/index.php? HTTP/1.1`. The request headers include `Host`, `User-Agent`, `Accept`, `Accept-Language`, `Accept-Encoding`, `Connection`, `Referer`, and `Upgrade-Insecure-Requests`. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, headers (8), and response headers (2). Below the request, the 'Response' tab is active, showing a 404 Not Found response from `mercury.picocftf.net:34561`. The response headers include `Connection` and `Content-Type`.

After that I change the request blue too from POST to HEAD, it gives me the flag.

1 x 2 x 3 x 4 x +

Send

Cancel

< ▾

> ▾

Target: http://

Request

Pretty Raw Hex

ln

1 HEAD /index.php HTTP/1.1

2 Host: mercury.picoctf.net:34561

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 0

9 Origin: http://mercury.picoctf.net:34561

10 Connection: close

11 Referer: http://mercury.picoctf.net:34561/

12 Upgrade-Insecure-Requests: 1

13

Search...

0 matches

Response

Pretty Raw Hex Render

ln

1 HTTP/1.1 200 OK

2 flag: picoCTF{r3j3ct_th3_du4llty_8f878508}

3 Content-type: text/html; charset=UTF-8

4

5. Mind your Ps and Qs

Mind your Ps and Qs  | 20 points Tags: picoCTF 2021 Cryptography

AUTHOR: SARA

Description

In RSA, a small **e** value can be problematic, but what about **n**? Can you decrypt this? [values](#)

Hints 

1

Bits are expensive, I used only a little bit over 100 to save money

27,729 solves / 32,396 users attempted (86%)



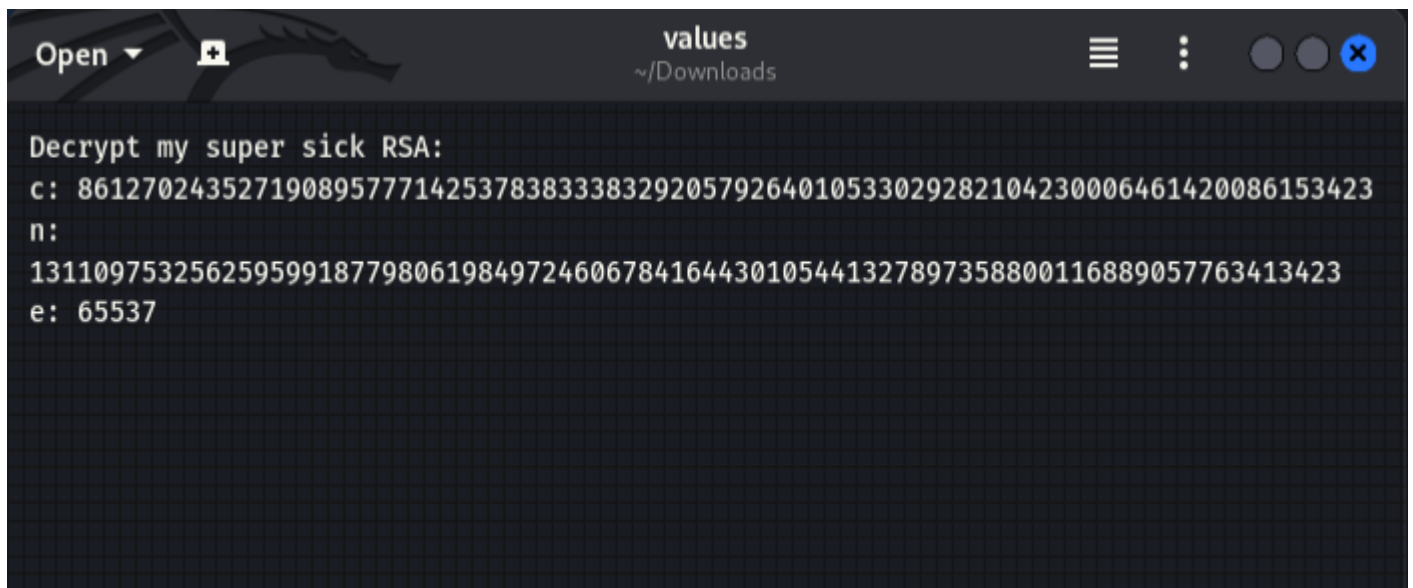
73% Liked










picoCTF{FLAG}

Submit Flag

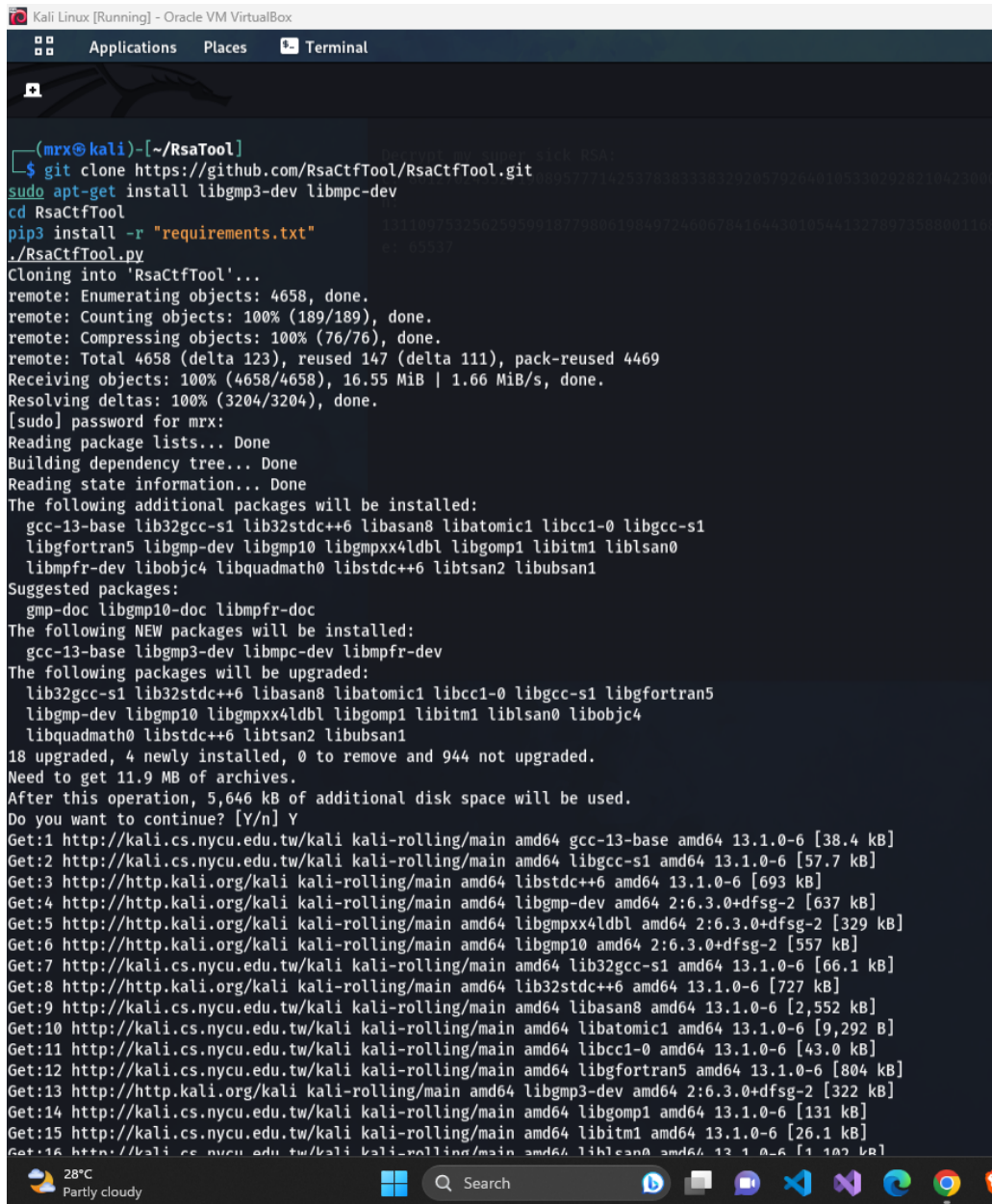
When I click the link values it downloaded this file



```
Open ▾  values ~/Downloads        
Decrypt my super sick RSA:  
c: 861270243527190895777142537838333832920579264010533029282104230006461420086153423  
n:  
1311097532562595991877980619849724606784164430105441327897358800116889057763413423  
e: 65537
```

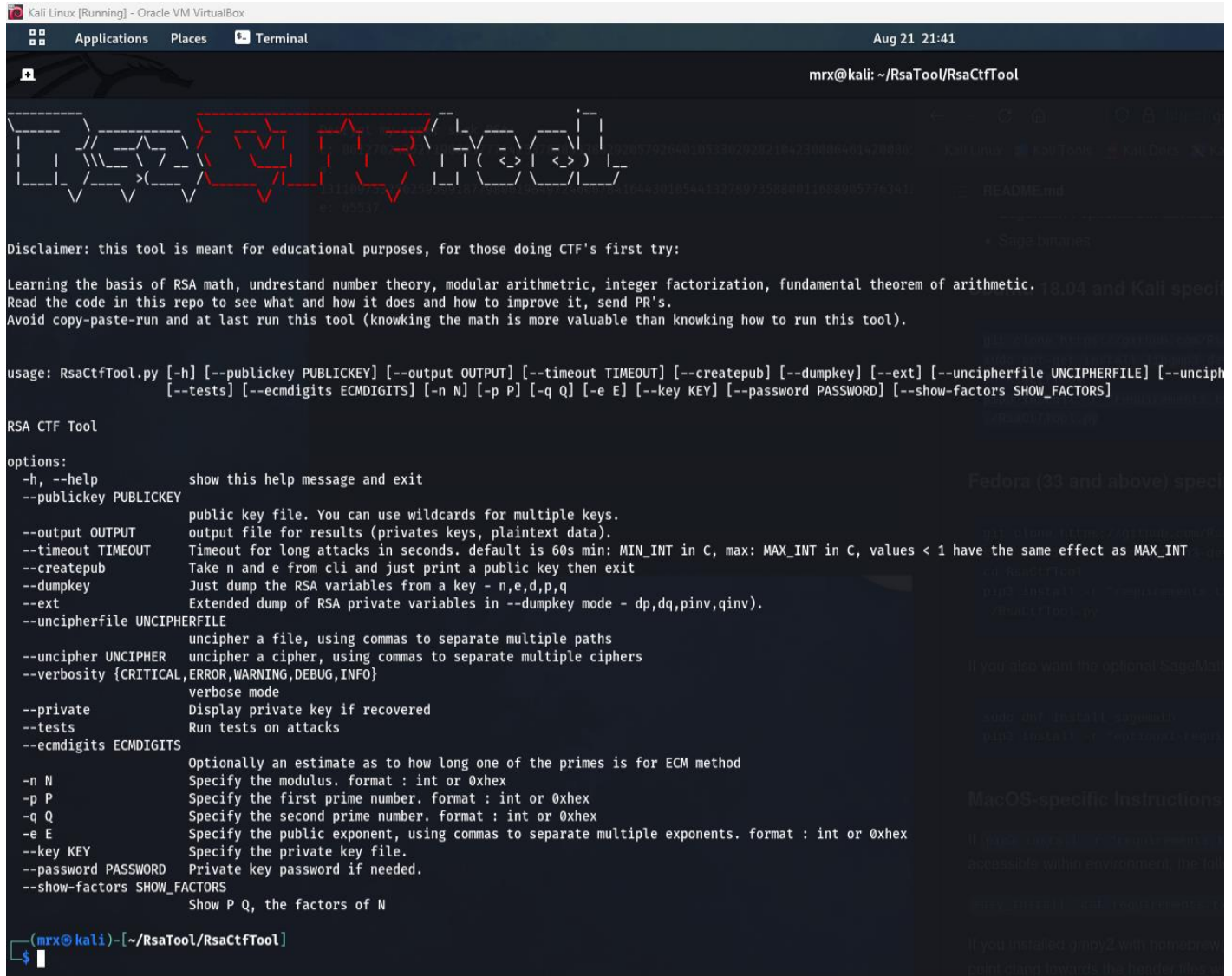
In here they have used RSA Algorithm where **RSA algorithm** is an asymmetric cryptography algorithm. Asymmetric means that it works on two different keys i.e., **Public Key** and **Private Key**. As the name describes, the Public Key is given to everyone, and the Private key is kept private. The RSA algorithm involves four steps: [key](#) generation, key distribution, encryption, and decryption

To solve this challenge, I found an online tool. I installed it in my kali machine.



```

(mrx@kali)~[~/RsaTool]
$ git clone https://github.com/RsaCtfTool/RsaCtfTool.git
$ sudo apt-get install libgmp3-dev libmpc-dev
$ cd RsaCtfTool
$ pip3 install -r "requirements.txt"
$ ./RsaCtfTool.py
Cloning into 'RsaCtfTool'...
remote: Enumerating objects: 4658, done.
remote: Counting objects: 100% (189/189), done.
remote: Compressing objects: 100% (76/76), done.
remote: Total 4658 (delta 123), reused 147 (delta 111), pack-reused 4469
Receiving objects: 100% (4658/4658), 16.55 MiB | 1.66 MiB/s, done.
Resolving deltas: 100% (3204/3204), done.
[sudo] password for mrx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gcc-13-base lib32gcc-s1 lib32stdc++6 libasan8 libatomic1 libbcc1-0 libgcc-s1
  libgfortran5 libgmp-dev libgmp10 libgmpxx4ldbl libgomp1 libitm1 liblsan0
  libmpfr-dev libobjc4 libquadmath0 libstdc++6 libtsan2 libubsan1
Suggested packages:
  gmp-doc libgmp10-doc libmpfr-doc
The following NEW packages will be installed:
  gcc-13-base libgmp3-dev libmpc-dev libmpfr-dev
The following packages will be upgraded:
  lib32gcc-s1 lib32stdc++6 libasan8 libatomic1 libbcc1-0 libgcc-s1 libgfortran5
  libgmp-dev libgmp10 libgmpxx4ldbl libgomp1 libitm1 liblsan0 libobjc4
  libquadmath0 libstdc++6 libtsan2 libubsan1
18 upgraded, 4 newly installed, 0 to remove and 944 not upgraded.
Need to get 11.9 MB of archives.
After this operation, 5,646 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 gcc-13-base amd64 13.1.0-6 [38.4 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libgcc-s1 amd64 13.1.0-6 [57.7 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libstdc++6 amd64 13.1.0-6 [693 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libgmp-dev amd64 2:6.3.0+dfsg-2 [637 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libgmpxx4ldbl amd64 2:6.3.0+dfsg-2 [329 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libgmp10 amd64 2:6.3.0+dfsg-2 [557 kB]
Get:7 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 lib32gcc-s1 amd64 13.1.0-6 [66.1 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 lib32stdc++6 amd64 13.1.0-6 [727 kB]
Get:9 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libasan8 amd64 13.1.0-6 [2,552 kB]
Get:10 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libatomic1 amd64 13.1.0-6 [9,292 B]
Get:11 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libbcc1-0 amd64 13.1.0-6 [43.0 kB]
Get:12 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libgfortran5 amd64 13.1.0-6 [804 kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 libgmp3-dev amd64 2:6.3.0+dfsg-2 [322 kB]
Get:14 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libgomp1 amd64 13.1.0-6 [131 kB]
Get:15 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libitm1 amd64 13.1.0-6 [26.1 kB]
Get:16 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 liblsan0 amd64 13.1.0-6 [110.7 kB]
  
```



```

Kali Linux [Running] - Oracle VM VirtualBox
Applications Places Terminal
Aug 21 21:41
mrx@kali: ~/RsaTool/RsaCtfTool

Disclaimer: this tool is meant for educational purposes, for those doing CTF's first try:
Learning the basis of RSA math, undrestand number theory, modular arithmetic, integer factorization, fundamental theorem of arithmetic.
Read the code in this repo to see what and how it does and how to improve it, send PR's.
Avoid copy-paste-run and at last run this tool (knowking the math is more valuable than knowking how to run this tool).

usage: RsaCtfTool.py [-h] [--publickey PUBLICKEY] [--output OUTPUT] [--timeout TIMEOUT] [--createpub] [--dumpkey] [--ext] [--uncipherfile UNCIPHERFILE] [--unciph
[--tests] [--ecmdigits ECMDIGITS] [-n N] [-p P] [-q Q] [-e E] [--key KEY] [--password PASSWORD] [--show-factors SHOW_FACTORS]

RSA CTF Tool

options:
  -h, --help                show this help message and exit
  --publickey PUBLICKEY     public key file. You can use wildcards for multiple keys.
  --output OUTPUT           output file for results (privates keys, plaintext data).
  --timeout TIMEOUT         Timeout for long attacks in seconds. default is 60s min: MIN_INT in C, max: MAX_INT in C, values < 1 have the same effect as MAX_INT
  --createpub               Take n and e from cli and just print a public key then exit
  --dumpkey                 Just dump the RSA variables from a key - n,e,d,p,q
  --ext                     Extended dump of RSA private variables in --dumpkey mode - dp,dq,pinv,qinv).
  --uncipherfile UNCIPHERFILE
                           uncipher a file, using commas to separate multiple paths
  --uncipher UNCIPHER      uncipher a cipher, using commas to separate multiple ciphers
  --verbosity {CRITICAL,ERROR,WARNING,DEBUG,INFO}
                           verbose mode
  --private                 Display private key if recovered
  --tests                  Run tests on attacks
  --ecmdigits ECMDIGITS     Optionally an estimate as to how long one of the primes is for ECM method
  -n N                     Specify the modulus. format : int or 0xhex
  -p P                     Specify the first prime number. format : int or 0xhex
  -q Q                     Specify the second prime number. format : int or 0xhex
  -e E                     Specify the public exponent, using commas to separate multiple exponents. format : int or 0xhex
  --key KEY                 Specify the private key file.
  --password PASSWORD      Private key password if needed.
  --show-factors SHOW_FACTORS
                           Show P Q, the factors of N

(mrx@kali)~-[~/RsaTool/RsaCtfTool]
$
  
```

After that using it requirement.txt file I found the different options enter the required values and got the flag

```
options:
-h, --help            Show this help message and exit
--publickey PUBLICKEY public key file. You can use wildcards for multiple
                        keys.
--output OUTPUT       output file for results (privates keys, plaintext
                        data).
--timeout TIMEOUT     Timeout for long attacks in seconds. default is 60s
                        min: MIN_INT in C, max: MAX_INT in C, values < 1 have
                        the same effect as MAX_INT
--createpub           Take n and e from cli and just print a public key then
                        exit
--dumpkey             Just dump the RSA variables from a key - n,e,d,p,q
--ext                Extended dump of RSA private variables in --dumpkey
                        mode - dp,dq,pinv,qinv).
--uncipherfile UNCIPHERFILE uncipher a file, using commas to separate multiple
                        paths
--uncipher UNCIPHER  uncipher a cipher, using commas to separate multiple
                        ciphers
--verbosity {CRITICAL,ERROR,WARNING,DEBUG,INFO} verbose mode
--private            Display private key if recovered
--tests              Run tests on attacks
--ecmdigits ECDIGITS  Optionally an estimate as to how long one of the
                        primes is for ECM method
-n N                Specify the modulus. format : int or 0xhex
-p P                Specify the first prime number. format : int or 0xhex
-q Q                Specify the second prime number. format : int or 0xhex
-e E                Specify the public exponent, using commas to separate
                        multiple exponents. format : int or 0xhex
--key KEY            Specify the private key file.
--password PASSWORD Private key password if needed.
(mrx@kali)~/RsaTool/RsaCtfTool
$ python3 RsaCtfTool.py -n 1311097532562595991877980619849724606784164430105441327897358800116889057763413423 -e 65537 --uncipher 86127024352719089577714253783833832920579264010533029282104230006461420086153423
```

```
[+] loading prime list file data/ti_rsa_signing_keys.txt...
100%|
[+] Time elapsed: 0.0021 sec.
[*] Performing mersenne_primes attack on /tmp/tmpvn9jyjl.
24%|
[+] Time elapsed: 0.0003 sec.
[*] Performing smallq attack on /tmp/tmpvn9jyjl.
[+] Time elapsed: 0.1545 sec.
[*] Performing lucas_gcd attack on /tmp/tmpvn9jyjl.
100%|
[+] Time elapsed: 0.0272 sec.
[*] Performing factordb attack on /tmp/tmpvn9jyjl.
[*] Attack success with factordb method !
[+] Total time elapsed min,max,avg: 0.0003/0.1545/0.0351 sec.

Results for /tmp/tmpvn9jyjl:

Unciphered data :
HEX : 0x007069636f4354467b736d6131315f4e5f6e305f67306f645f31333638363637397d
INT (big endian) : 13016382529449106065927291425342535437996222135352905256639573959002849415739773
INT (little endian) : 3711971977671268622040852236510036125495501942684770673221105381148513202625671168
utf-8 : picoCTF{sma11_N_n0_g0od_13686679}
utf-16 : 濃振掖樞懣愁丿也渥弼で掣ヾ些莖嫻紹
STR : b'\x00picoCTF{sma11_N_n0_g0od_13686679}'

(mrx@kali)~/RsaTool/RsaCtfTool
$
```

6.Insp3ct0r

Insp3ct0r 

👤 | 50 points ✕

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ZARATEC/DANNY

Hints 

Description

1 2

Kishor Balan tipped us off that the following code may need inspection:

<https://jupiter.challenges.picoctf.org/problem/44924/> ([link](#)) or

<http://jupiter.challenges.picoctf.org:44924>

83,228 solves / 87,729 users attempted (95%)



87% Liked



picoCTF{FLAG}

Submit Flag

In this challenge from the name even we can guess where to look and the hints are given as how you would inspect a web code on browser for that we must simply go to the inspect element or must view the page source, so in a webpage there are basically three parts which is html part, css part and the js part since the second given as there are three parts I thought of first looking those three files so as I thought the three parts of the flag were in these three separate files


```

</head>
<body>
  <div class="container">
    <header>
      <h1>Inspect Me</h1>
    </header>
    <button id="defaultOpen" class="tablink" onclick="openTab('tabintro', this, '#222')">What</button>
    <button class="tablink" onclick="openTab('tababout', this, '#222')">How</button>
    <div id="tabintro" class="tabcontent" style="display: block;">
      <h3>What</h3>
      <p>I made a website</p>
    </div>
    <div id="tababout" class="tabcontent" style="display: none;">
      <h3>How</h3>
      <p><img alt="picoCTF logo" data-bbox="145 310 165 325"/></p>
      <!--Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3-->
    </div>
  </div>

```

```

    cursor: pointer;
    padding: 14px 16px;
    font-size: 17px;
    width: 50%;
  }

```

```

.tablink:hover {
  background-color: #777;
}

```

```

.tabcontent {
  color: #111;
  display: none;
  padding: 50px;
  text-align: center;
}

```

```

#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }

```

```

/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ctive_0r_ju5t */

```

```

document.getElementById(tabName).style.display = "block";
if(elmnt.style != null) {
  elmnt.style.backgroundColor = color;
}
}

```

```

window.onload = function() {
  openTab('tabintro', this, '#222');
}

```

```

/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399) */

```

7.Cookies

Cookies 

 | 40 points 

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Hints 

Description

(None)

Who doesn't love cookies? Try to figure out the best one.

<http://mercury.picoctf.net:29649/>

44,699 solves / 48,484 users attempted (92%)

 61% Liked 

 picoCTF{FLAG}

Submit Flag

Once I click this link it gives me this page

Cookies

[Home](#)

Welcome to my cookie search page. See how much I
like different kinds of cookies!

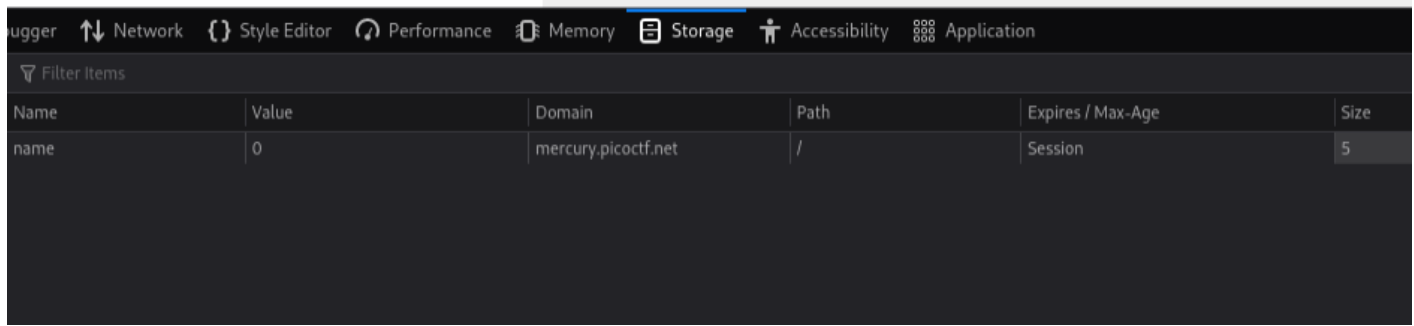
snickerdoodle

Search

Cookie is a way to have users store information about what they are doing and present it back to you.

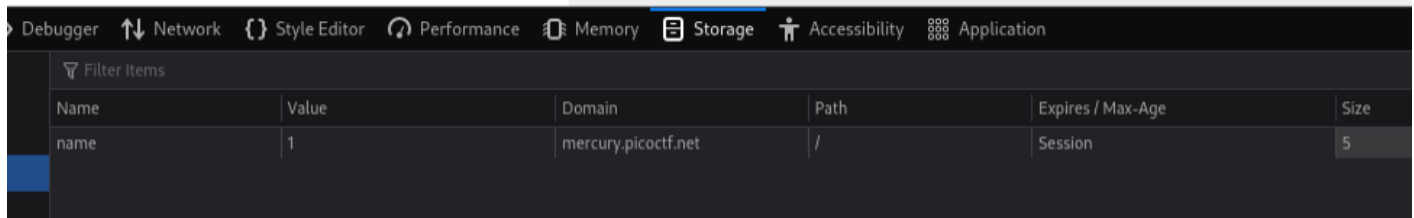
In here when you type different type of cookies the value changes that it has a array of cookies we cannot go through one by one so need to use Burpsuite to automate this function

I love snickerdoodle cookies!



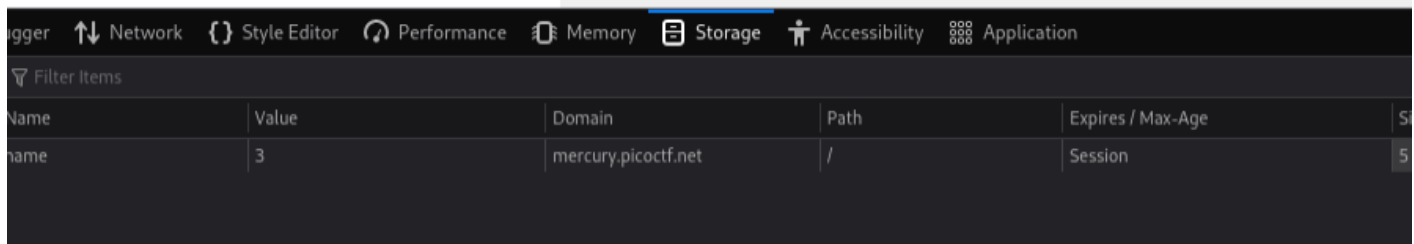
Name	Value	Domain	Path	Expires / Max-Age	Size
name	0	mercury.picoctf.net	/	Session	5

I love chocolate chip cookies!



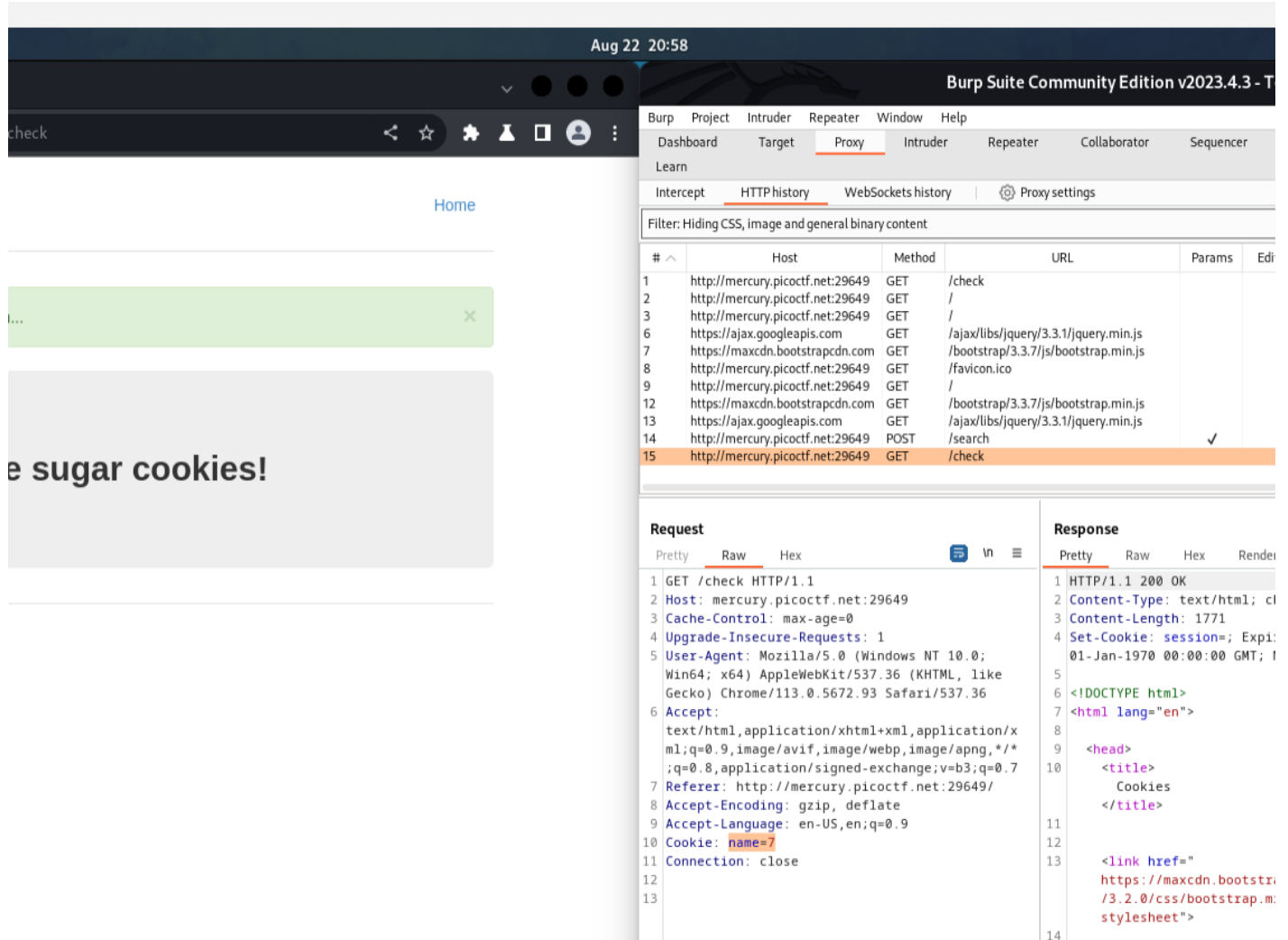
Name	Value	Domain	Path	Expires / Max-Age	Size
name	1	mercury.picoctf.net	/	Session	5

I love gingersnap cookies!



Name	Value	Domain	Path	Expires / Max-Age	Size
name	3	mercury.picoctf.net	/	Session	5

So I opened burpsuite moved proxy tab click intercept is off to on the intercept and click open browser and paste the link



Aug 22 20:58

Burp Suite Community Edition v2023.4.3 - T

check

Home

e sugar cookies!

Filter: Hiding CSS, image and general binary content

#	^	Host	Method	URL	Params	Edi
1		http://mercury.picoctf.net:29649	GET	/check		
2		http://mercury.picoctf.net:29649	GET	/		
3		http://mercury.picoctf.net:29649	GET	/		
6		https://ajax.googleapis.com	GET	/ajax/libs/jquery/3.3.1/jquery.min.js		
7		https://maxcdn.bootstrapcdn.com	GET	/bootstrap/3.3.7/js/bootstrap.min.js		
8		http://mercury.picoctf.net:29649	GET	/favicon.ico		
9		http://mercury.picoctf.net:29649	GET	/		
12		https://maxcdn.bootstrapcdn.com	GET	/bootstrap/3.3.7/js/bootstrap.min.js		
13		https://ajax.googleapis.com	GET	/ajax/libs/jquery/3.3.1/jquery.min.js		
14		http://mercury.picoctf.net:29649	POST	/search		✓
15		http://mercury.picoctf.net:29649	GET	/check		

Request

Pretty Raw Hex

```

1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:29649
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://mercury.picoctf.net:29649/
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: name=7
11 Connection: close
12
13

```

Response

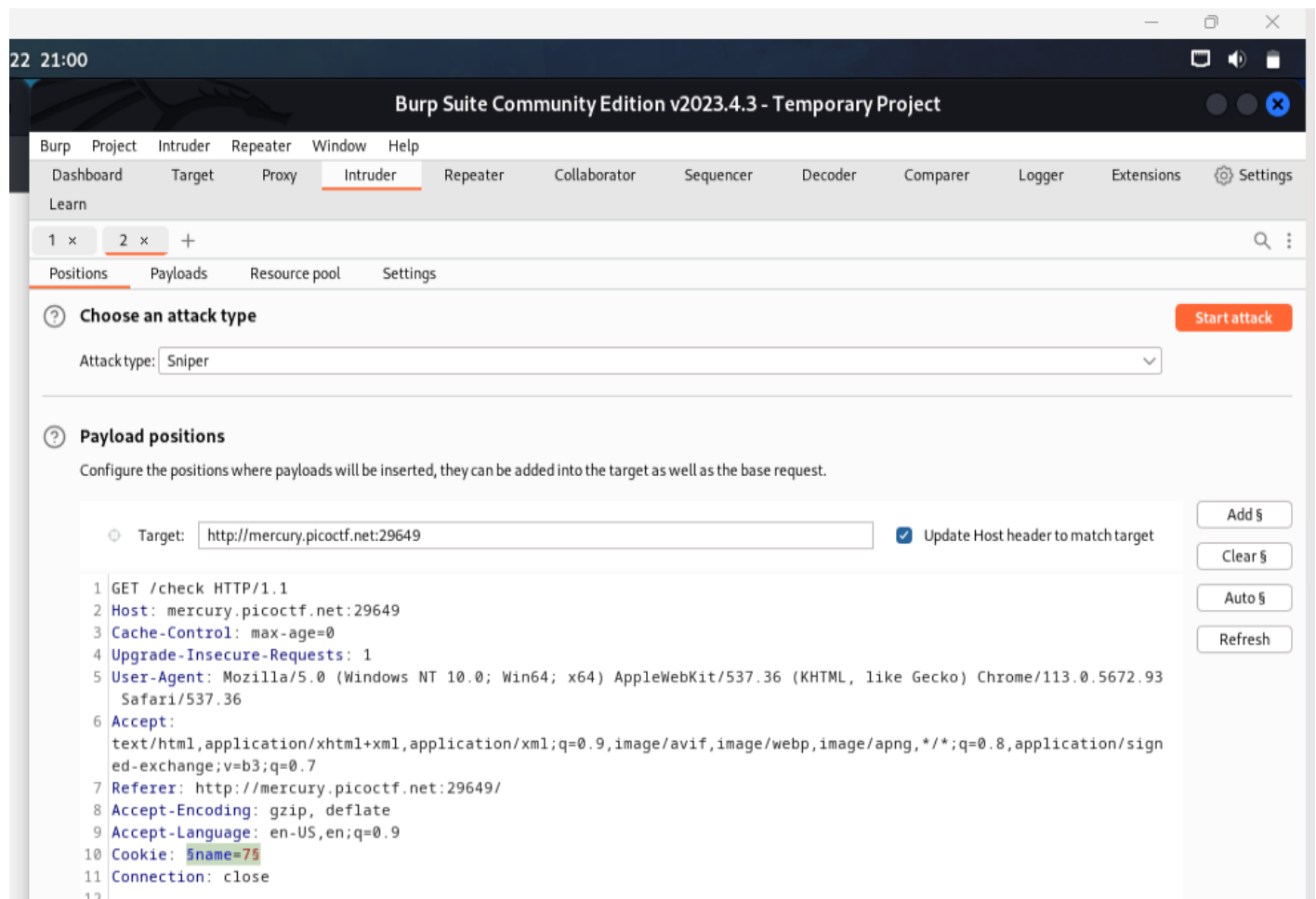
Pretty Raw Hex Render

```

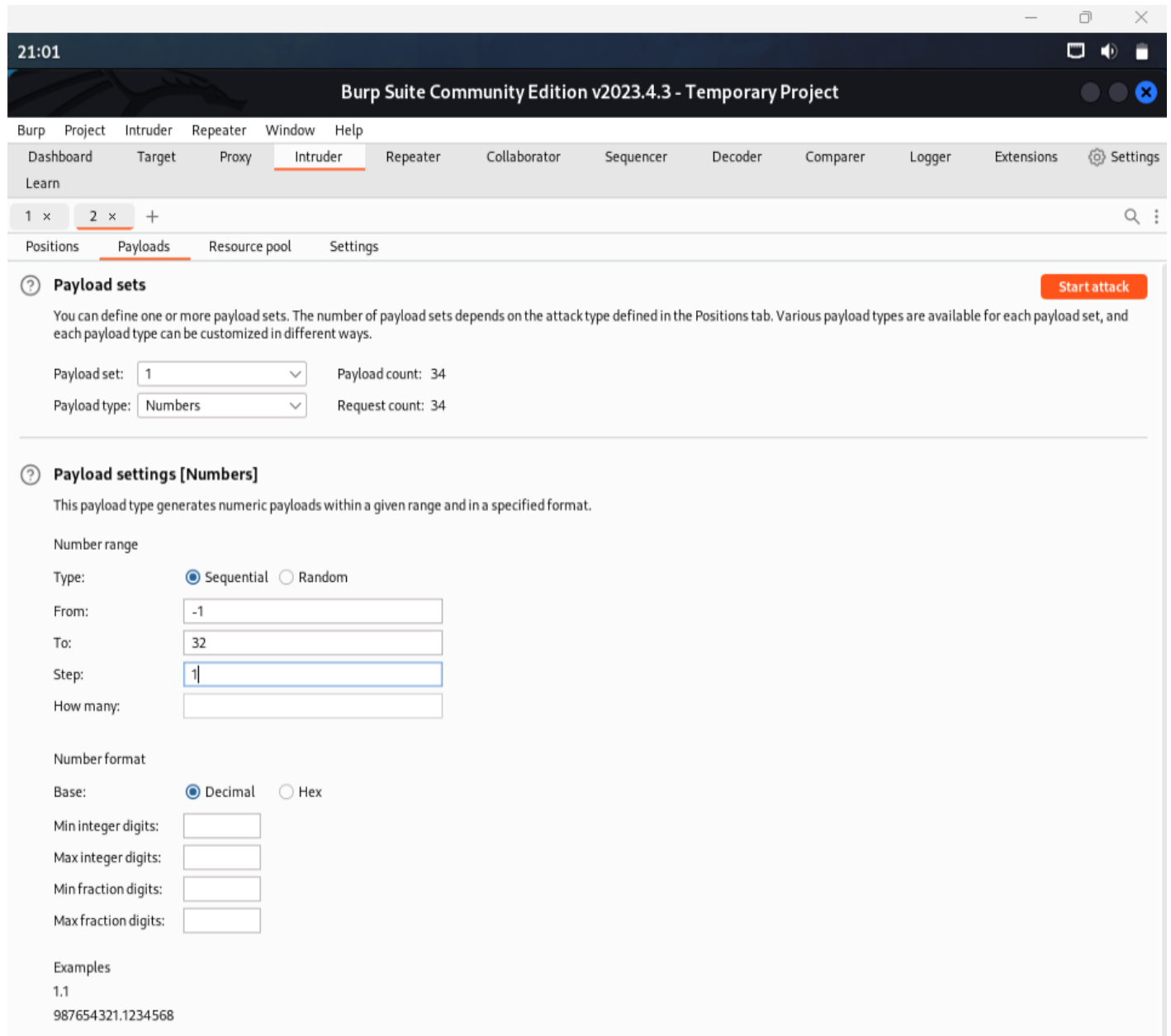
1 HTTP/1.1 200 OK
2 Content-Type: text/html; cl
3 Content-Length: 1771
4 Set-Cookie: session=; Expi: 01-Jan-1970 00:00:00 GMT; I
5
6 <!DOCTYPE html>
7 <html lang="en">
8
9 <head>
10 <title>
11 Cookies
12 </title>
13
14 <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">

```

So since we need to send different values we need to send it to intruder



Then move to payloads tab do the following changes to it and click start attack.



21:01

Burp Suite Community Edition v2023.4.3 - Temporary Project

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Settings

Learn

1 x 2 x +

Positions **Payloads** Resource pool Settings

Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 34
 Payload type: Numbers Request count: 34

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: -1

To: 32

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

1.1

987654321.1234568

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1932
1	-1	302	<input type="checkbox"/>	<input type="checkbox"/>	557
2	0	200	<input type="checkbox"/>	<input type="checkbox"/>	1940
3	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1941
4	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1941
5	3	200	<input type="checkbox"/>	<input type="checkbox"/>	1937
6	4	200	<input type="checkbox"/>	<input type="checkbox"/>	1937
7	5	200	<input type="checkbox"/>	<input type="checkbox"/>	1940
8	6	200	<input type="checkbox"/>	<input type="checkbox"/>	1938
9	7	200	<input type="checkbox"/>	<input type="checkbox"/>	1932
10	8	200	<input type="checkbox"/>	<input type="checkbox"/>	1935
11	9	200	<input type="checkbox"/>	<input type="checkbox"/>	1931
12	10	200	<input type="checkbox"/>	<input type="checkbox"/>	1935
13	11	200	<input type="checkbox"/>	<input type="checkbox"/>	1933
14	12	200	<input type="checkbox"/>	<input type="checkbox"/>	1932

From this we must select the one with unusual length then it will give the flag.

8.Power Cookie

Power Cookie 

 | 200 points 

Tags: picoCTF 2022 Web Exploitation cookie

AUTHOR: LT 'SYREAL' JONES

Hints 

Description

1

Can you get the flag?

Go to this [website](#) and see what you can discover.

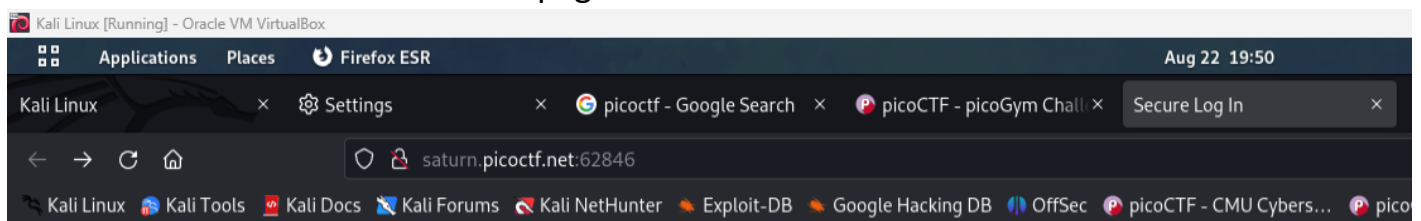
16,627 solves / 16,960 users attempted (98%)

 93% Liked 

 picoCTF{FLAG}

Submit Flag

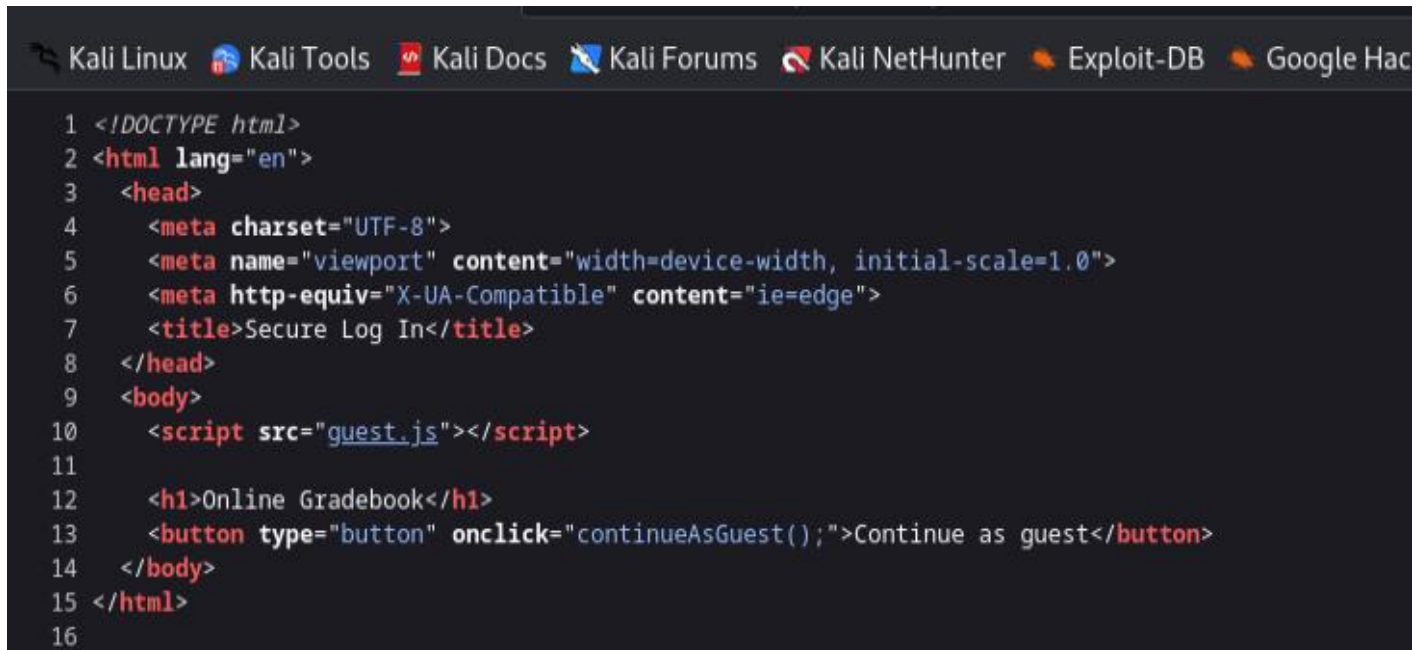
The above link redirects me to this page



Online Gradebook

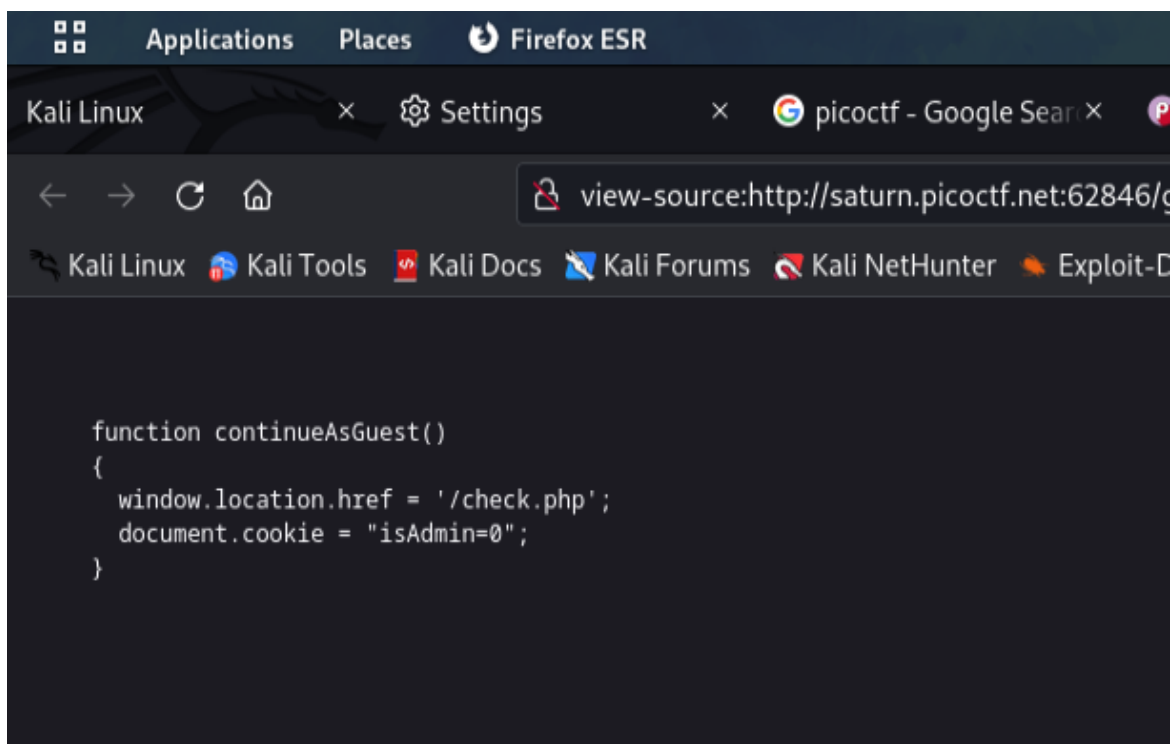
Continue as guest

As the page is plain and as usually for the first I went to the source page which some hint about an js file.



```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <meta http-equiv="X-UA-Compatible" content="ie=edge">
7     <title>Secure Log In</title>
8   </head>
9   <body>
10    <script src="guest.js"></script>
11
12    <h1>Online Gradebook</h1>
13    <button type="button" onclick="continueAsGuest();">Continue as guest</button>
14  </body>
15 </html>
16
```

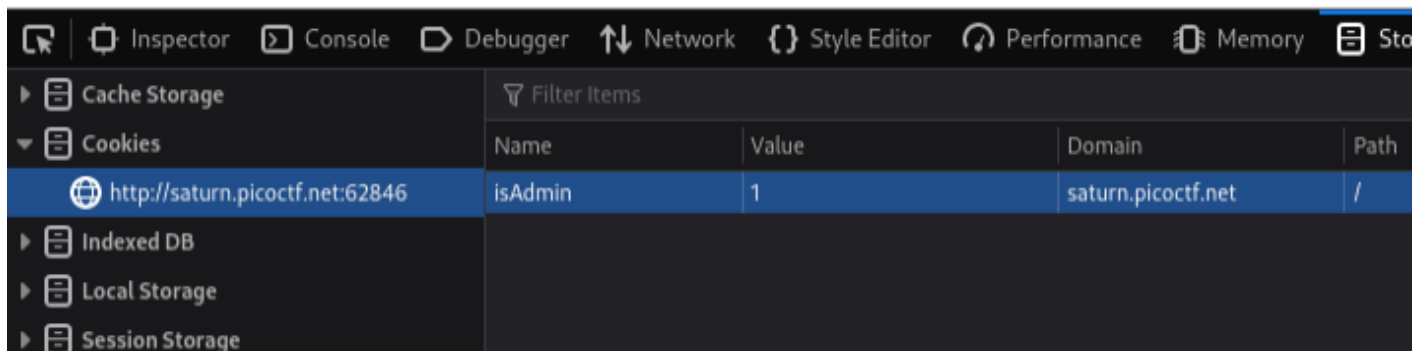
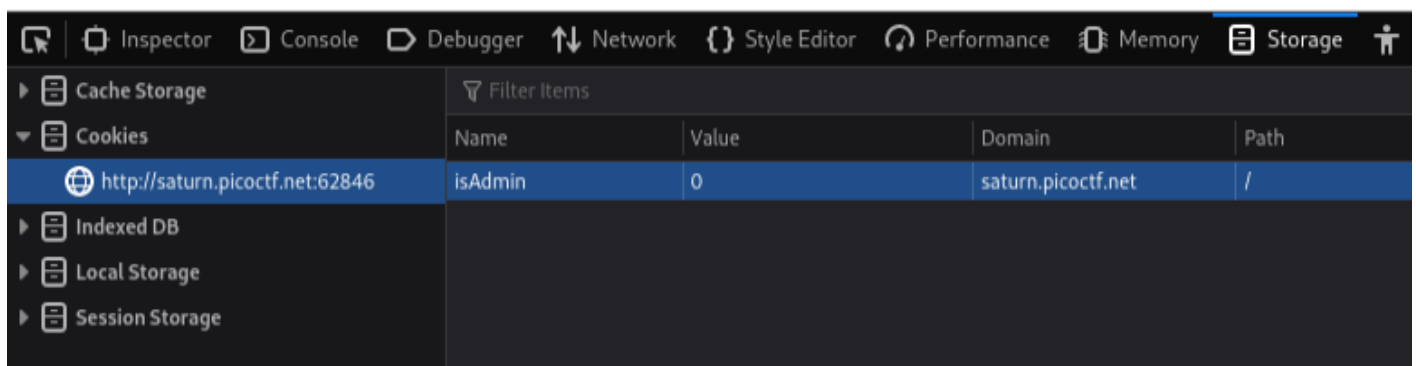
In the guest.js file it gives me a hint about cookies



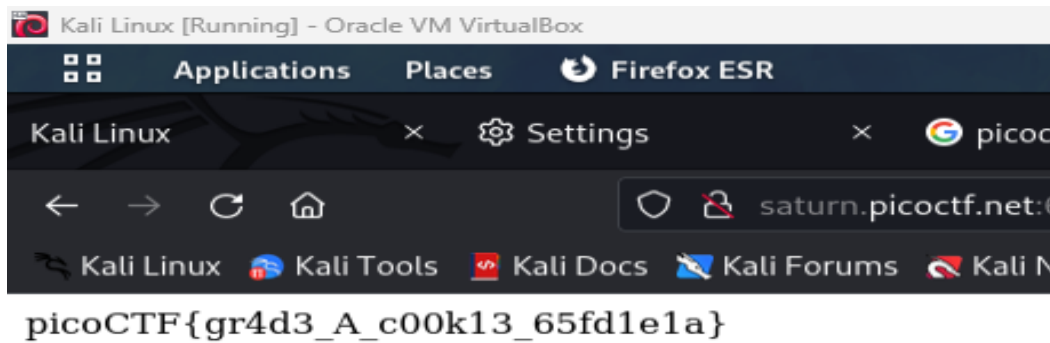
```
function continueAsGuest()
{
  window.location.href = '/check.php';
  document.cookie = "isAdmin=0";
}
```

In document.cookie = "isAdmin = 0" it's a Boolean value where it is whether it is an Admin or not so if we change this value to 1 (modified this cookie) in developer option. we can get closer to the flag. And also, from the code segment './check.php' we can clearly identify that it is running php. It is server-side language it looking for the cookie that user carries

So I opened the inspector element and moved to the storage tab there in Cookies sections I change the value from zero to one which like making "isAdmin" true by making "isAdmin = 1"





After this reloaded the page using CTRL+SHIFT+R which is hard refresh reasking the webserver to give the required page



9. logon

logon 

 | 100 points 

Tags: picoCTF 2019 Web Exploitation

AUTHOR: BOBSON

Description

The factory is hiding things from all of its users. Can you login as Joe and find what they've been looking at? <https://jupiter.challenges.picoctf.org/problem/15796/> (link) or <http://jupiter.challenges.picoctf.org:15796>

Hints

1

Hmm it doesn't seem to check anyone's password, except for Joe's?

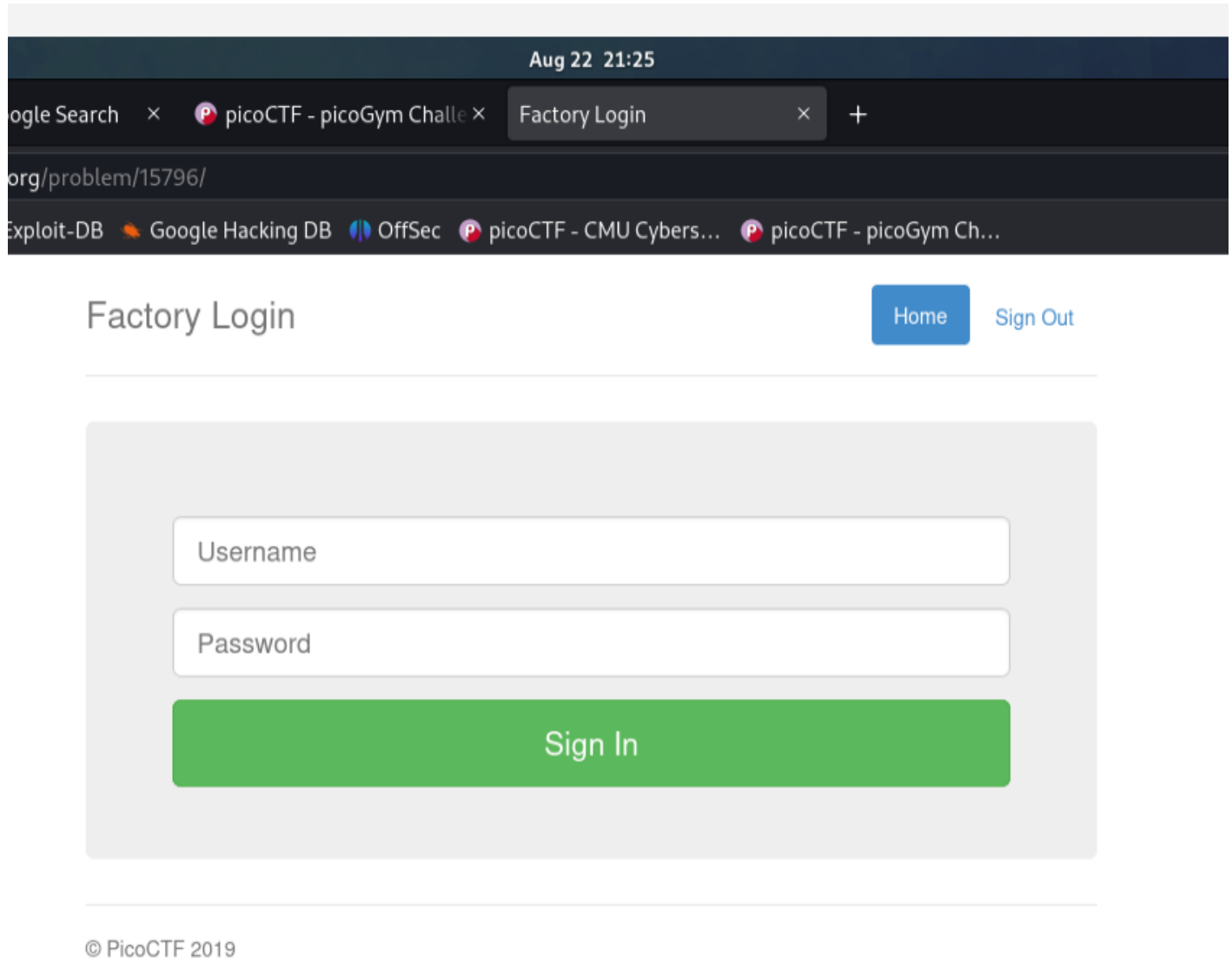
41,599 solves / 44,017 users attempted (95%)

 88% Liked 

 picoCTF{FLAG}

Submit Flag

Once I click the above, I was redirected to the below page



Aug 22 21:25

Google Search × picoCTF - picoGym Challenge × Factory Login × +

org/problem/15796/

Exploit-DB Google Hacking DB OffSec picoCTF - CMU Cybers... picoCTF - picoGym Ch...

Factory Login

Home Sign Out

Username

Password

Sign In

© PicoCTF 2019

It gives a hint that it doesn't seem to check anyone's password, except for Joe's?

So I entered username as admin and password also as admin page directed to this page

Factory Login

Home

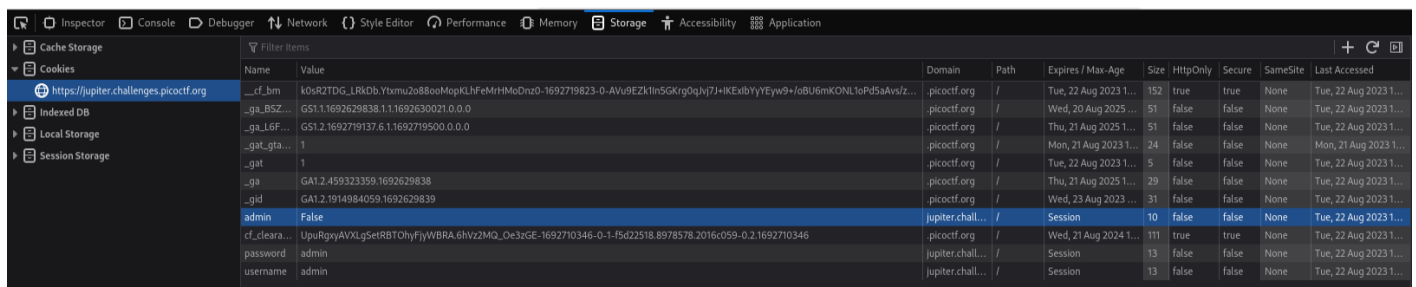
Sign Out

Success: You logged in! Not sure you'll be able to see the flag though.

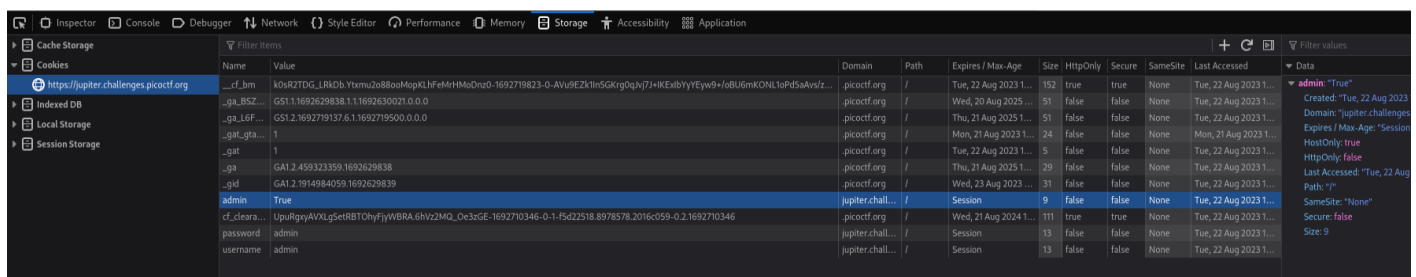
No flag for you

© PicoCTF 2019

Then moved I to the inspect element then in the storage tab I changed the cookie settings as follows and got the flag.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__cf_bm	k0sR2TDG_LRkDb_Yomu2o88ooMopKLHfMhMoDn0-1692719823-0-AVu9EZkln5GKrg0qj7J+KExibYyEYw9+oBU6mKONLtoPd5aAvs/z...	picoctf.org	/	Tue, 22 Aug 2023 1...	152	true	true	None	Tue, 22 Aug 2023 1...
_ga_BS2...	GS1.1.1692629838.1.1.1692630021.0.0.0	picoctf.org	/	Wed, 20 Aug 2025 ...	51	false	false	None	Tue, 22 Aug 2023 1...
_ga_L6F...	GS1.2.1692719137.6.1.1692719500.0.0.0	picoctf.org	/	Thu, 21 Aug 2023 1...	51	false	false	None	Tue, 22 Aug 2023 1...
_gat_gta...	1	picoctf.org	/	Mon, 21 Aug 2023 1...	24	false	false	None	Mon, 21 Aug 2023 1...
_gat	1	picoctf.org	/	Tue, 22 Aug 2023 1...	5	false	false	None	Tue, 22 Aug 2023 1...
_ga	GA1.2.459323359.1692629838	picoctf.org	/	Thu, 21 Aug 2025 1...	29	false	false	None	Tue, 22 Aug 2023 1...
_gid	GA1.2.1914984059.1692629839	picoctf.org	/	Wed, 23 Aug 2023 ...	31	false	false	None	Tue, 22 Aug 2023 1...
admin	False	jupiter.chall...	/	Session	10	false	false	None	Tue, 22 Aug 2023 1...
cf_cleara...	UpuRgyAVXlgSetRBT0hFyWBRa.6hV22MQ_Oe3zGE-1692710346-0-1-Fs022518.8978578.2016c059-0.2.1692710346	picoctf.org	/	Wed, 21 Aug 2024 1...	111	true	true	None	Tue, 22 Aug 2023 1...
password	admin	jupiter.chall...	/	Session	13	false	false	None	Tue, 22 Aug 2023 1...
username	admin	jupiter.chall...	/	Session	13	false	false	None	Tue, 22 Aug 2023 1...



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__cf_bm	k0sR2TDG_LRkDb_Yomu2o88ooMopKLHfMhMoDn0-1692719823-0-AVu9EZkln5GKrg0qj7J+KExibYyEYw9+oBU6mKONLtoPd5aAvs/z...	picoctf.org	/	Tue, 22 Aug 2023 1...	152	true	true	None	Tue, 22 Aug 2023 1...
_ga_BS2...	GS1.1.1692629838.1.1.1692630021.0.0.0	picoctf.org	/	Wed, 20 Aug 2025 ...	51	false	false	None	Tue, 22 Aug 2023 1...
_ga_L6F...	GS1.2.1692719137.6.1.1692719500.0.0.0	picoctf.org	/	Thu, 21 Aug 2023 1...	51	false	false	None	Tue, 22 Aug 2023 1...
_gat_gta...	1	picoctf.org	/	Mon, 21 Aug 2023 1...	24	false	false	None	Mon, 21 Aug 2023 1...
_gat	1	picoctf.org	/	Tue, 22 Aug 2023 1...	5	false	false	None	Tue, 22 Aug 2023 1...
_ga	GA1.2.459323359.1692629838	picoctf.org	/	Thu, 21 Aug 2025 1...	29	false	false	None	Tue, 22 Aug 2023 1...
_gid	GA1.2.1914984059.1692629839	picoctf.org	/	Wed, 23 Aug 2023 ...	31	false	false	None	Tue, 22 Aug 2023 1...
admin	True	jupiter.chall...	/	Session	9	false	false	None	Tue, 22 Aug 2023 1...
cf_cleara...	UpuRgyAVXlgSetRBT0hFyWBRa.6hV22MQ_Oe3zGE-1692710346-0-1-Fs022518.8978578.2016c059-0.2.1692710346	picoctf.org	/	Wed, 21 Aug 2024 1...	111	true	true	None	Tue, 22 Aug 2023 1...
password	admin	jupiter.chall...	/	Session	13	false	false	None	Tue, 22 Aug 2023 1...
username	admin	jupiter.chall...	/	Session	13	false	false	None	Tue, 22 Aug 2023 1...

Factory Login

Home

Sign Out



Flag:

picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}

© PicoCTF 2019

10. Some Assembly Required 1

Some Assembly Required 1 

 | 70 points 

Tags: picoCTF 2021 Web Exploitation

AUTHOR: SEARS SCHULZ

Description

<http://mercury.picoctf.net:36152/index.html>

Hints 

(None)

20,752 solves / 22,016 users attempted (94%)



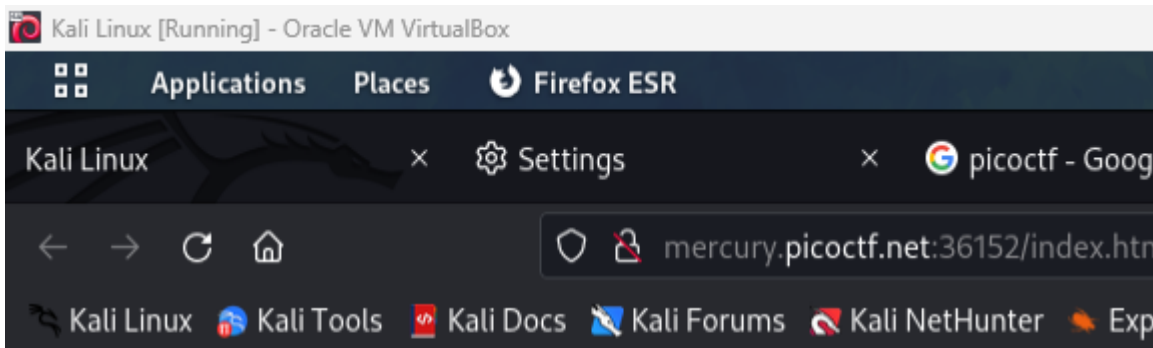
62% Liked



picoCTF{FLAG}

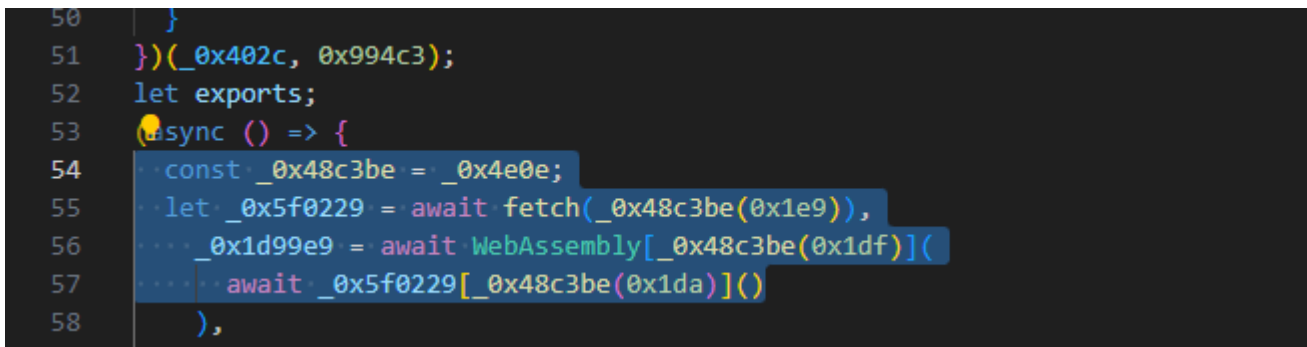
Submit Flag

Once I click the link it directed to this page



Enter flag:

I moved to the inspect element and found a js file.



We must consider this also because title of the challenge also some assembly required

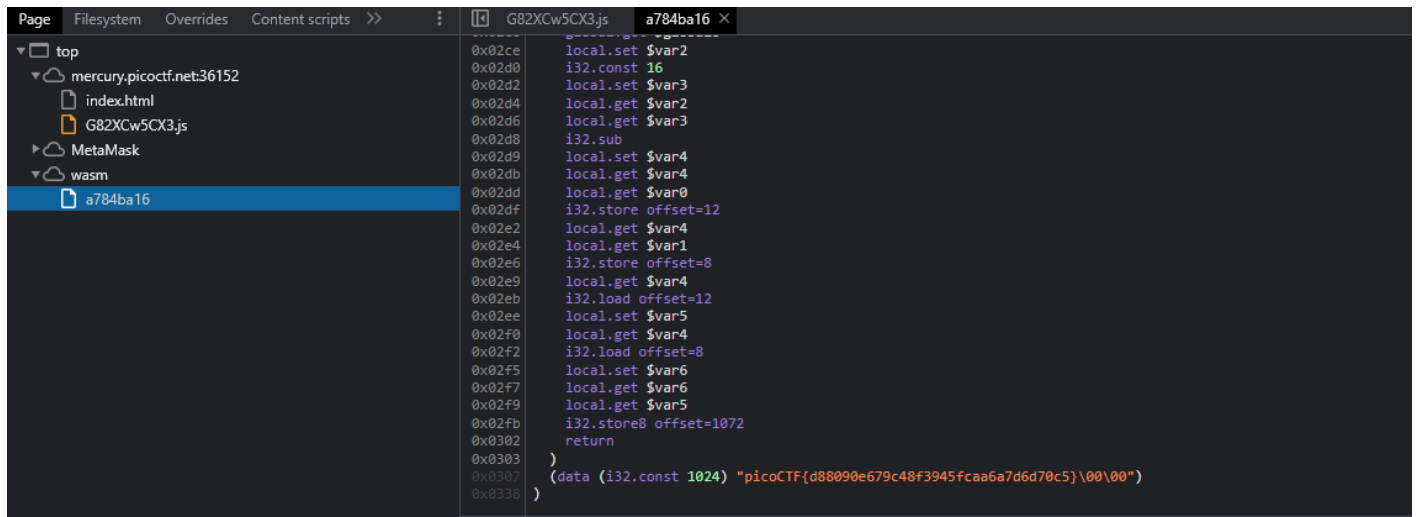
WebAssembly means that we are fetching something from some address that defined by this code.

`await fetch(_0x48c3be(0x1e9))`

and in sources there is a wasm file too.

wasm = WebAssembly is a binary instruction format for a stack-based virtual machine. Wasm is designed as a portable compilation target for programming languages, enabling deployment on the web for client and server applications.

In the wasm file I was able to get the flag



```

0x02ce    local.set $var2
0x02d0    i32.const 16
0x02d2    local.set $var3
0x02d4    local.get $var2
0x02d6    local.get $var3
0x02d8    i32.sub
0x02d9    local.set $var4
0x02db    local.get $var4
0x02dd    local.get $var0
0x02df    i32.store offset=12
0x02e2    local.get $var4
0x02e4    local.get $var1
0x02e6    i32.store offset=8
0x02e9    local.get $var4
0x02eb    i32.load offset=12
0x02ee    local.set $var5
0x02f0    local.get $var4
0x02f2    i32.load offset=8
0x02f5    local.set $var6
0x02f7    local.get $var6
0x02f9    local.get $var5
0x02fb    i32.store8 offset=1072
0x0302    return
0x0303    )
0x0307    (data (i32.const 1024) "picoCTF{d88090e679c48f3945fcaa6a7d6d70c5}\\00\\00")
0x0338    )
  
```

```
Terminal  Help  assembly.js - CTF - Visual Studi

login.js  JS assembly.js X

$ assembly.js > [?] _0x402c
1  const _0x402c = [
2      "value",
3      "2wfTpTR",
4      "instantiate",
5      "275341bEPcme",
6      "innerHTML",
7      "1195047NznhZg",
8      "1qfevql",
9      "input",
10     "1699808QuoWhA",
11     "Correct!",
12     "check_flag",
13     "Incorrect!",
14     "./JIFxzHyW8W",
15     "23SMpAuA",
16     "802698XOMSrr",
17     "charCodeAt",
18     "474547vVoGD0",
19     "getElementById",
20     "instance",
21     "copy_char",
22     "43591XxcwU1",
23     "5044541lVtzW",
24     "arrayBuffer",
25     "2NIQmVj",
26     "result",
27 ];
28 const _0x4e0e = function (_0x553839, _0x53c021) {
29     _0x553839 = _0x553839 - 0x1d6;
30     let _0x402c6f = _0x402c[_0x553839];
31     return _0x402c6f;
32 };
33 (function (_0x76dd13, _0x3dfcae) {
34     const _0x371ac6 = _0x4e0e;
35     while (!![]) {
36         try {
37             const _0x478583 =
38                 -parseInt(_0x371ac6(0x1eb)) +
39                 parseInt(_0x371ac6(0x1ed)) +
40                 -parseInt(_0x371ac6(0x1db)) * -parseInt(_0x371ac6(0x1d9)) +
41                 -parseInt(_0x371ac6(0x1e2)) * -parseInt(_0x371ac6(0x1e3)) +
42                 -parseInt(_0x371ac6(0x1de)) * parseInt(_0x371ac6(0x1e0)) +
43                 parseInt(_0x371ac6(0x1d8)) * parseInt(_0x371ac6(0x1ea)) +
44                 -parseInt(_0x371ac6(0x1e5));
45             if (_0x478583 === _0x3dfcae) break;
46             else _0x76dd13["push"](_0x76dd13["shift"]());
```