

picoCTF_WebExploration

Skills Learned:

Burp Suite (Request Header Manipulation, Cookies, METHODS)
 web enumeration (dirsearch)
 html, css, .js
 /robots.txt, ./DS_Store
 md5 collisions
 cookie encryption

Skills Needed:

Web Assembly/Debugging
 How to break cookie encryption

GET aHEAD

20 points

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:21939/>

17,766 solves / 30,527 attempts (58%)

81%
Liked

picoCTF{FLAG} **Submit Flag**

Hints

1 2

Exploitation

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Ext
65	http://mercury.picoctf.net:21939	GET	/index.php?			200	1123	HTML	php
66	http://mercury.picoctf.net:21939	POST	/index.php			200	1125	HTML	php

Request **Raw** **Hex**

```

1 POST /index.php HTTP/1.1
2 Host: mercury.picoctf.net:21939
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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:21939

```

Response

```

1 HTTP/1.1 200 OK
2 Content-type: text/html; charset=UTF-8
3
4
5 <!doctype html>
6 <html>
7   <head>
8     <title>
9       Blue
10      </title>
11      <link rel="stylesheet" type="text/css" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bo
12          
```

1/24/22, 3:39 PM

```
10 Connection: close
11 Referer: http://mercury.picoctf.net:21939/index.php?
12 Upgrade-Insecure-Requests: 1
13
14
```

```
picoCTF - Evernote
otstrap.min.css">
<style>
  body{
    background-color:blue;
  }
</style>
</head>
<body>
<div class="container">
  <div class="row">
    <div class="col-md-6">
      <div class="panel panel-primary" style="margin-top:50px">
        <div class="panel-heading">
```

0 matches 0 matches

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options Us

1 x ...

Send Cancel < > Target: http://mercury.picoctf.net:21939

Request changed "post" to "head" **Response**

Pretty Raw Hex \n \n \n

1 HEAD /index.php HTTP/1.1
2 Host: mercury.picoctf.net:21939
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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:21939
10 Connection: close
11 Referer: http://mercury.picoctf.net:21939/index.php?
12 Upgrade-Insecure-Requests: 1
13
14

Pretty Raw Hex \n \n \n

1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4lity_6ef27873}
3 Content-type: text/html; charset=UTF-8
4
5

Changing POST request to HEAD in the Repeter

Cookies 

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

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

<http://mercury.picoctf.net:17781/>

Hints

(None)

13,311 solves / 22,356 attempts (60%)

58% Liked

 picoCTF{FLAG}

Submit Flag

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

snickerdoodle

Search

© PicoCTF

# ^	Host	Method	URL
68	http://mercury.picoctf.net:17781	GET	/
69	https://ajax.googleapis.com	GET	/ajax/libs/jquery/3.3.1/jquery.n
70	https://maxcdn.bootstrapcdn.com	GET	/bootstrap/3.3.7/js/bootstrap.r
71	http://mercury.picoctf.net:17781	POST	/search
72	http://mercury.picoctf.net:17781	GET	/check

tried "chocolate chip"

Request

Pretty Raw Hex ⌂ \n ⌂

```

1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:17781
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
   Gecko/20100101 Firefox/91.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://mercury.picoctf.net:17781/
8 Connection: close
9 Cookie: name=1
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty Raw Hex ⌂ \n ⌂

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

```

Send Cancel < >

Request

Pretty Raw Hex ⌂ \n ⌂

```

1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:17781
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://mercury.picoctf.net:17781/
8 Connection: close
9 Cookie: name=18
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty Raw Hex Render ⌂ \n ⌂

Cookies

Home

Flag:

changing the value until

https://www.evernote.com/client/web#?b=8b3ce6a2-dccf-d150-4129-0492cf938796&n=54b47ddb-dc19-f746-3806-c189af711b10&

the flag pops

பிசுட்டி வார்யூ லெவ்ஸ் கூகிள் மார்க்கெ

Insp3ct0r 

50 points

Tags: Category: Web Exploitation

AUTHOR: ZARATEC/DANNY

Hints

1 2

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

<https://jupiter.challenges.picoctf.org/problem/41511/> ([link](#)) or

<http://jupiter.challenges.picoctf.org:41511>

40,924 solves / 109,152 attempts (37%)

 86% Liked 

flag picoCTF{FLAG}

[Submit Flag](#)

Inspect Me

What

How

How

I used these to make this site:

HTML

css

JS (JavaScript)

```
DOCTYPE html>
tml> event
<head>
<title>My First Website :)</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>...</header>
      <button id="defaultOpen" class="tablink" onclick="openTab('tabintro', this, '#222')" style="background-color: #222; color: white; border: none; padding: 5px; width: 150px; height: 30px; border-radius: 5px; font-size: 14px; font-weight: bold; margin-bottom: 10px;">Intro</button>
      <button class="tablink" onclick="openTab('tababout', this, '#222')" style="background-color: #222; color: white; border: none; padding: 5px; width: 150px; height: 30px; border-radius: 5px; font-size: 14px; font-weight: bold; margin-bottom: 10px;">About</button>
    > <div id="tabintro" class="tabcontent" style="display: none; border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9; border-radius: 5px; min-height: 200px; margin-bottom: 10px;">...</div>
    > <div id="tababout" class="tabcontent" style="display: block; border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9; border-radius: 5px; min-height: 200px; margin-bottom: 10px;">
      <h3>How</h3>
      > <p>...</p>
        <!--Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3-->
      </div>
    </div>
  </div>
</body>
<html>
```

```
39 }
40 .tabcontent {
41   color: #111;
42   display: none;
43   padding: 50px;
44   text-align: center;
45 }
46
47 #tabintro { background-color: #ccc; }
48 #tababout { background-color: #ccc; }
49
50 /* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ctlive_0r_ju5t */
51 }
```



```
}
```

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

/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?832b0699} */
```



Three-part flag found in the html, css, javascript

Scavenger Hunt

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

Hints

There is some interesting information hidden around this site <http://mercury.picoctf.net:44070/>. Can you find it?

10,771 solves / 38,868 attempts (28%)

59%
Liked

picoCTF{FLAG}

In the html

```
</p>
<!--Here's the first part of the flag: picoCTF{t-->
/div>
<--
```

in the css

```
40
41 .tabcontent {
42   color: #111;
43   display: none;
44   padding: 50px;
```

```

45     text-align: center;
46 }
47
48 #tabintro { background-color: #ccc; }
49 #tababout { background-color: #ccc; }
50
51 /* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0 */

```

in the javascript

```

1 function openTab(tabName,elmnt,color) {
2     var i, tabcontent, tablinks;
3     tabcontent = document.getElementsByClassName("tabcontent");
4     for (i = 0; i < tabcontent.length; i++) {
5         tabcontent[i].style.display = "none";
6     }
7     tablinks = document.getElementsByClassName("tablink");
8     for (i = 0; i < tablinks.length; i++) {
9         tablinks[i].style.backgroundColor = "";
10    }
11    document.getElementById(tabName).style.display = "block";
12    if(elmnt.style != null) {
13        elmnt.style.backgroundColor = color;
14    }
15 }
16
17 window.onload = function() {
18     openTab('tabintro', this, '#222');
19 }
20
21 /* How can I keep Google from indexing my website? */
22

```

/robots.txt

```

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

```

At the point:

dirsearch -u <http://mercury.picocft.net:44070/>

```

Target: http://mercury.picocft.net:44070/
[19:12:16] Starting:
[19:12:23] 200 - 62B - ./DS_Store
[19:12:27] 200 - 95B - ./htaccess
[19:12:27] 200 - 95B - ./htaccess/
[#####] 57% 6249/10927 76/s job:1/1 errors:0

```

found part 5 before 4

./DS_Store

Congrats! You completed the scavenger hunt. Part 5: _7a46d25d}

./htaccess

```

<?> 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_l0 */

```

```
# Part 4: 3s_2_l00k
# I love making websites on my Mac, I can store a lot of information there.
```

Some Assembly Required 1 

Tags: Category: Web Exploitation

AUTHOR: SEARS SCHULZ

Description

<http://mercury.picoctf.net:55336/index.html>

Hints
(None)

6,449 solves / 8,878 attempts (73%)

 65% Liked 

 picoCTF{FLAG} 

It is my Birthday Who are you? Login

← → ⌛ ⌂ mercury.picoctf.net:55336/index.html

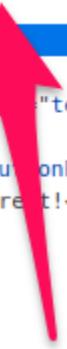
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DE

Enter flag:

Submit

Looking at html reveals .js

```
<html>
  <head>
    <meta charset="UTF-8">
    <script src="G82XCw5CX3.js"></script>
  </head>
  <body>
    <h4>Enter flag:</h4>
    <input id="input" type="text">
    <p id="result">Incorrect!</p>
  </body>
</html>
```



.js shows us a hidden directory brings us to a file

Network Style Editor Performance Memory Storage Accessibility Application

G82XCw5CX3.js X

```
1 rHTML', '1195047NzhZg', '1qfevql', 'input', '1699808QuoWhA', 'Correct!', 'check_flag', 'Incorrect!', './JIFxzHyW8W!', '23SMpAuA'
```

Which has the flag

```
[biddion㉿kali)-[~/Documents/GitHub/picoCTF/WebExplorationSkills]
└─$ cat JIFxzHyW8W
asmcesspA♦ triggers for kali-menu (2021.4.2) ...
Processing A♦iggers for man-db (2.9.4-4) ...
    A♦
--(biddion㉿kali)-[~]
└─$ dirsearch http://mercury.picoctf.net:44070/
!A♦L target is missing, try using -u <url>
A♦♦
--(biddion㉿kali)-[~]
└─$ Asearch -u http://mercury.picoctf.net:44070/
    ♦
    |   memory_wasm_call_ctorsstrcmp
check_flaginput copy_char
                                _dso_handle
__global_base[http, aspx, jsp, html, js] | HTTP method: GET | Threads: 30 | Wordl
__memory_base_heap_base
Output File: __table_base/.dirsearch/reports/mercury.picoctf.net-44070/-_22-
♦
?♦*#♦*♦*!A !bck!/b6! 6 (!i 6e(!cl 6logs/errors-22-01-23_19-12-15.log
                                @o (!A j!           6 -!
Target: http://mercury.picoctf.net:44070/
:
[19:12:16] Starting:
[19:12:23] 200 - 628 - /.DS_Store
[19:12:27] 200 - 958 - /htaccess
[19:12:27] 200 - 958 - /htaccess/
[19:13:49] 200 - 961B - /index.html
6[19:14:] j! 200 - 1248 - /robots.txt

Task Completed
-
-!A♦!dq!@kali)-[~]
!A♦!dq! - http://mercury.picoctf.net:55336/
!A♦!dq!etk! Using, try using -u <url>
--(biddion㉿kali)-[~]
└─$ dirsearch -t !A♦!dq! -y.picoctf.net:55336/
!A♦! dq! ! F!!A!" ! "q!# #
- [19:29:53] Starting: 2021.4.2
  !$A♦!% $ %q!& - ! !
!'A♦!( ' (q!) & )k!* *6
Extensions: php, aspx, js(!+ +mt, js | HTTP method: GET | Threads: 30 | Wordl
                                L
Output File: /home/biddion/.dirsearch/reports/mercury.picoctf.net-55336/-_22-
Error Log: /home/biddion/.dirsearch/logs/errors-22-01-23_19-29-51.log
?#♦*♦*!A! k! 6
Target: http://mercy.picoctf.net:55336/
    ! ! :♦*♦*
[19:29:53] Starting:
[19:31:25] 200 - 2358 - /im2A♦.html
                                +picoCTF{51e513c498950a515b1aab5e941b2615}
Task Completed
```



More Cookies

👤 | 90 points ✖

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

I forgot Cookies can Be modified

Hints

1 2

981 solves / 3.215 attempts (31%)

31% Liked

flag picoCTF{FLAG}

Submit Flag

Too Hard; can't do!

where are the robots 

Tags: Category: Web Exploitation

AUTHOR: ZARATEC/DANNY

Description

Can you find the robots? <https://jupiter.challenges.picoctf.org/problem/36474/> ([link](#)) or <http://jupiter.challenges.picoctf.org:36474>

Hints 1

27,643 solves / 60,050 attempts (46%)

 82% Liked 

 picoCTF{FLAG} Submit Flag

coGym x Welcome x More Cookies x more cookies picoctf - Go x +

<https://jupiter.challenges.picoctf.org/problem/36474/>

Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

Welcome

Where are the robots?

This is just following bread crumbs
</robots.txt>

     <https://jupiter.challenges.picoctf.org/problem/36474/robots.txt>

 Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

User-agent: *
Disallow: /477ce.html

</477ce.html>

<https://jupiter.challenges.picoctf.org/problem/36474/477ce.html>

 Exploit-DB  Google Hacking DB  OffSec

Guess you found the robots
picoCTF{ca1cu1at1ng_Mach1n3s_477ce}

logon 

Tags: Category: 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/13594/> ([link](#)) or <http://jupiter.challenges.picoctf.org:13594>

Hints  1

19,346 solves / 27,367 attempts (71%)

 87% Liked 

 picoCTF{FLAG} 

CTF - picoGym  Factory Login  jupiter.challenges.picoctf.org  More Cookies  more cookies picoctf - Go 

https://jupiter.challenges.picoctf.org/problem/13594/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Factory Login

Home Sign Out

Username

Password

Sign In

© PicoCTF 2019

I tired just changing the value from 'false' to 'true'

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

8  ...

 Cancel < >

Request

```

1 GET /problem/13594/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga=GA1.2.1160019831.1642929874; _gid=GA1.2.222856668.1642929874; password=dave;
4   username=joe; admin=False
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Referer: https://jupiter.challenges.picoctf.org/problem/13594/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Te: trailers
16 Connection: close
17

```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options Learn

8 ...

Send Cancel < > Target

Request

```

1 GET /problem/13594/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga=GA1.2.1160019831.1642929874; _gid=GA1.2.222856668.1642929874; password=dave;
4   username=joe; admin=True
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Referer: https://jupiter.challenges.picoctf.org/problem/13594/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Te: trailers
16 Connection: close
17

```

Response

```

1 Factory Login
2
3 Flag:
4 picoCTF{th3_c0nsp1r4cy_l1v3s_d1c24fef}
5
6 © PicoCTF 2019

```

Success!!!

dont-use-client-side 

Tags: Category: Web Exploitation

AUTHOR: ALEX FULTON/DANNY

Description

Can you break into this super secure portal?

<https://jupiter.challenges.picoctf.org/problem/37821/> ([link](#)) or
<http://jupiter.challenges.picoctf.org:37821>

Hints

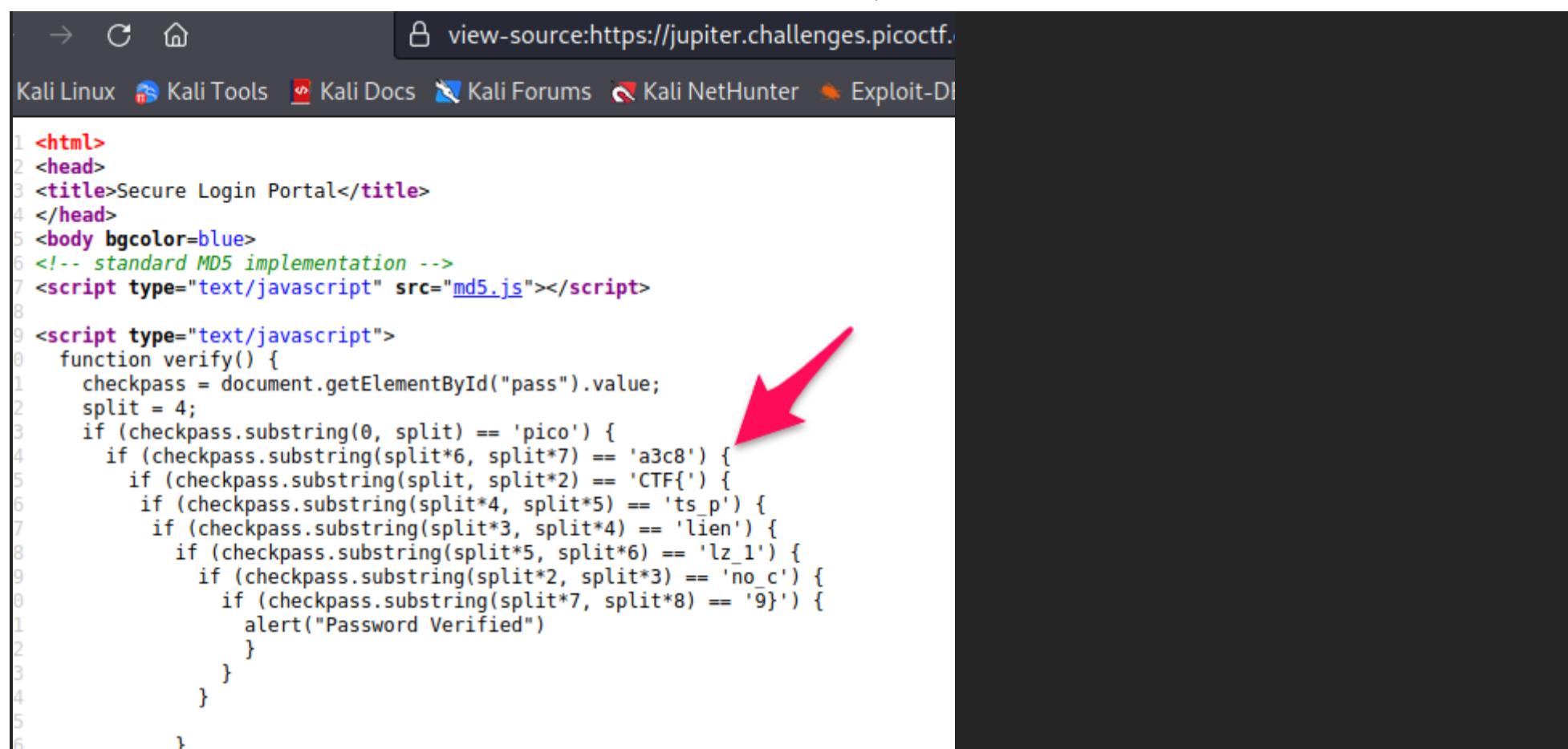
1

19,897 solves / 37,995 attempts (52%)

88% Liked

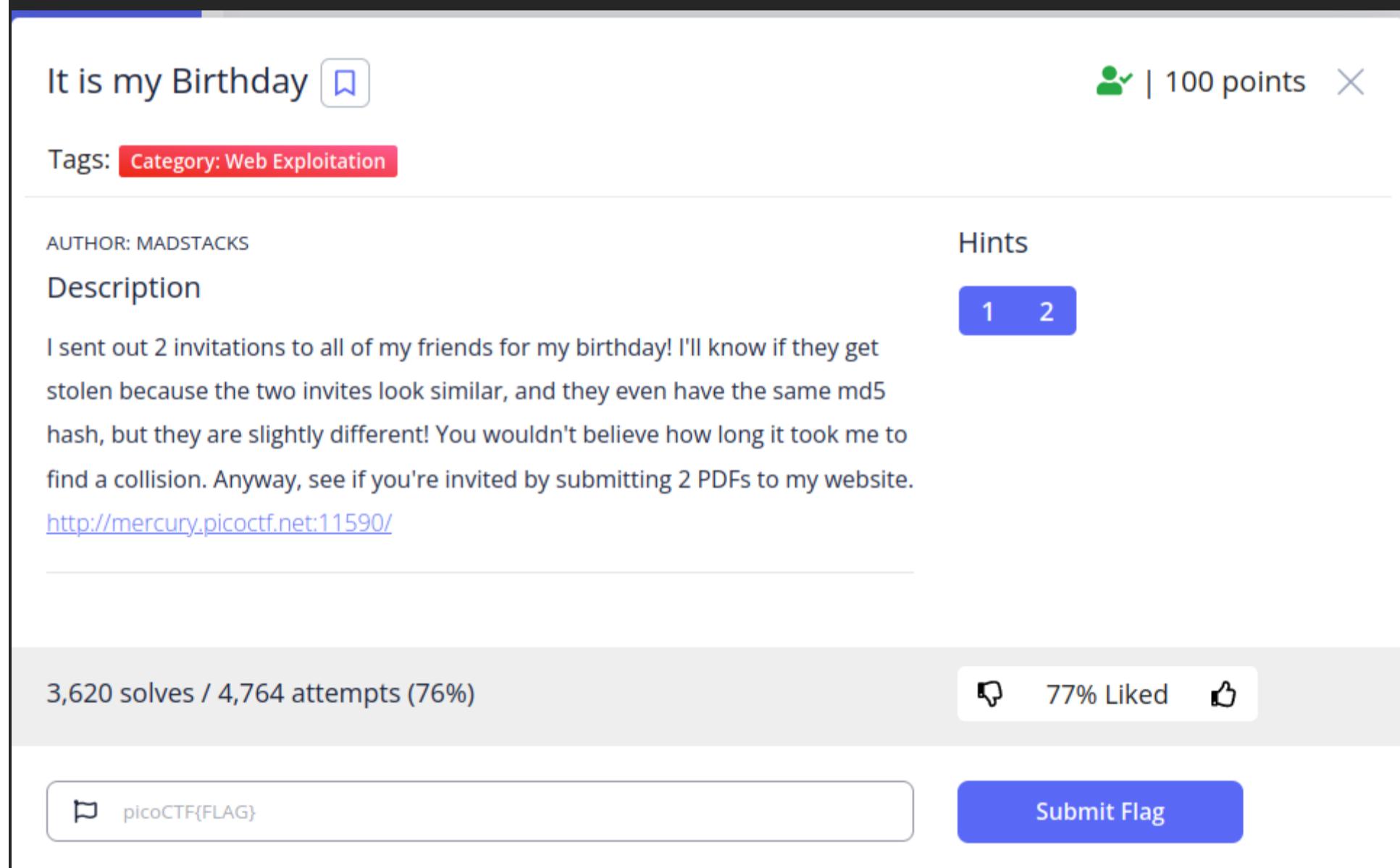
 picoCTF{FLAG}

Submit Flag



```
<html>
<head>
<title>Secure Login Portal</title>
</head>
<body bgcolor=blue>
<!-- standard MD5 implementation -->
<script type="text/javascript" src="md5.js"></script>
<br>
<script type="text/javascript">
function verify() {
    checkpass = document.getElementById("pass").value;
    split = 4;
    if (checkpass.substring(0, split) == 'pico') {
        if (checkpass.substring(split*6, split*7) == 'a3c8') {
            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_1') {
                            if (checkpass.substring(split*2, split*3) == 'no_c') {
                                if (checkpass.substring(split*7, split*8) == '9}') {
                                    alert("Password Verified")
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
</script>
```

Viewing the code, the flag is in javascript, broken in the clear. I don't know how to write a script that will piece it together but my two eyes do work.



It is my Birthday 

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website.
<http://mercury.picoctf.net:11590/>

Hints

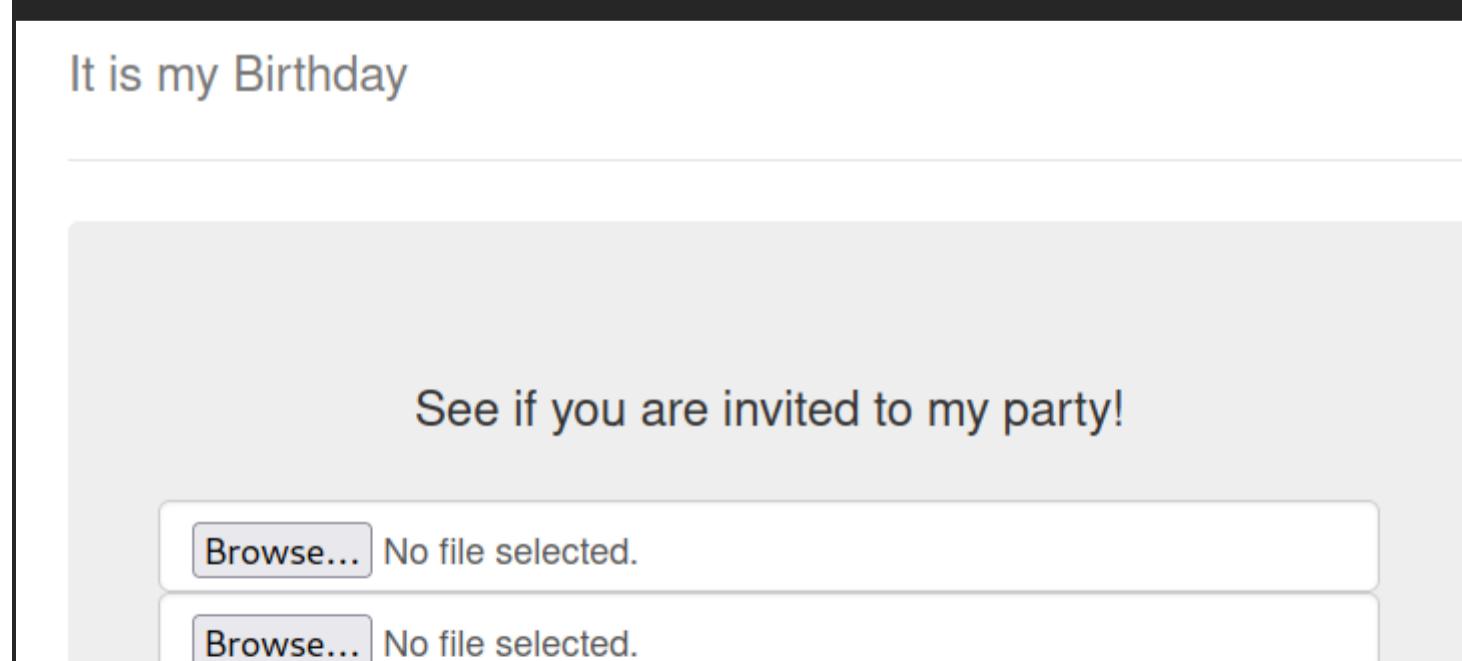
1 2

3,620 solves / 4,764 attempts (76%)

 77% Liked 

 picoCTF{FLAG} 

This task involves a collision of two md5 encoded files

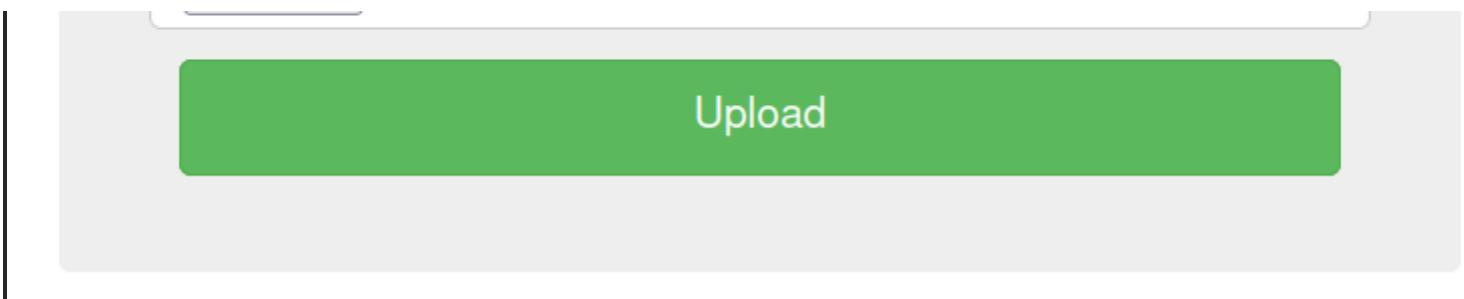


It is my Birthday

See if you are invited to my party!

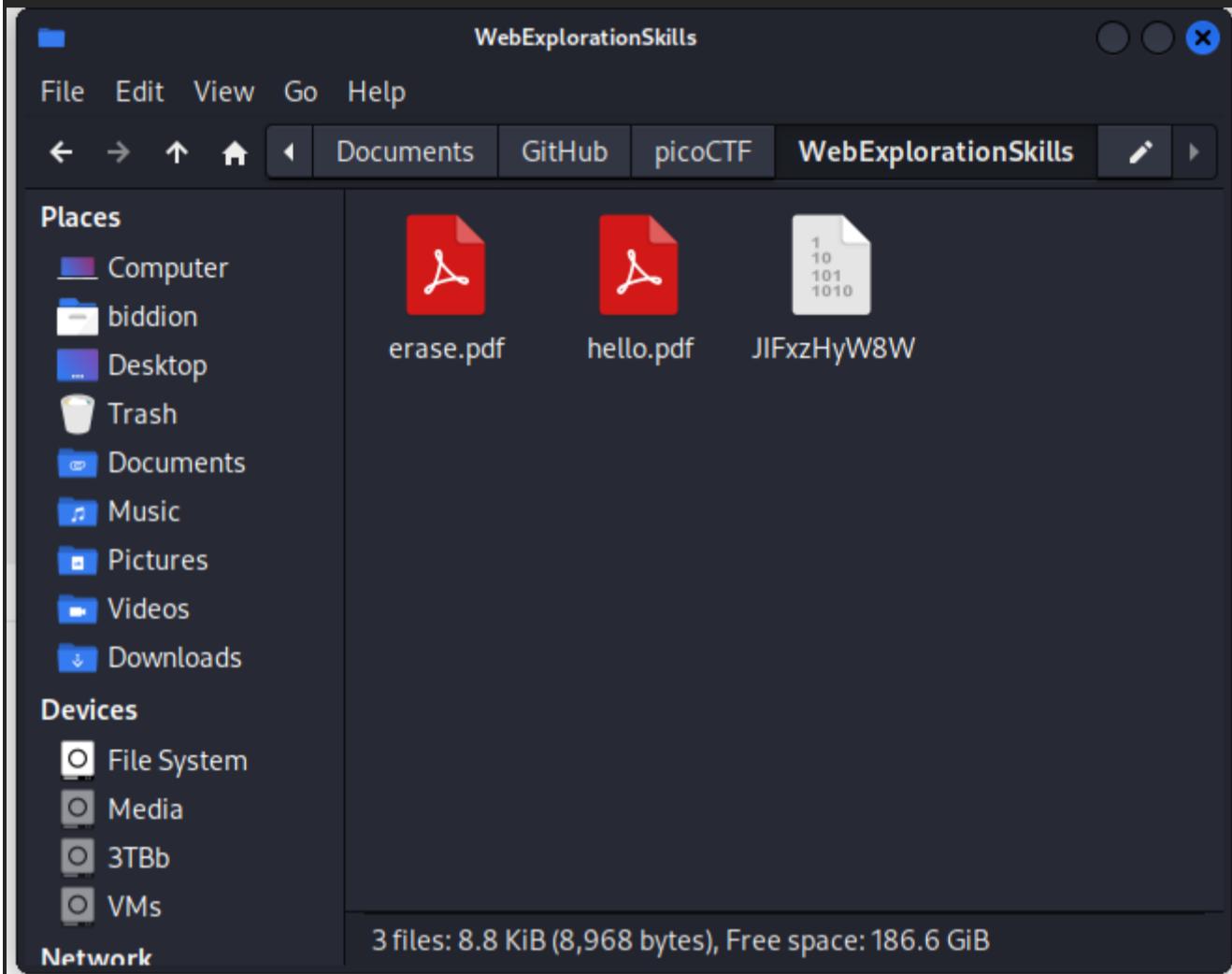
No file selected.

No file selected.

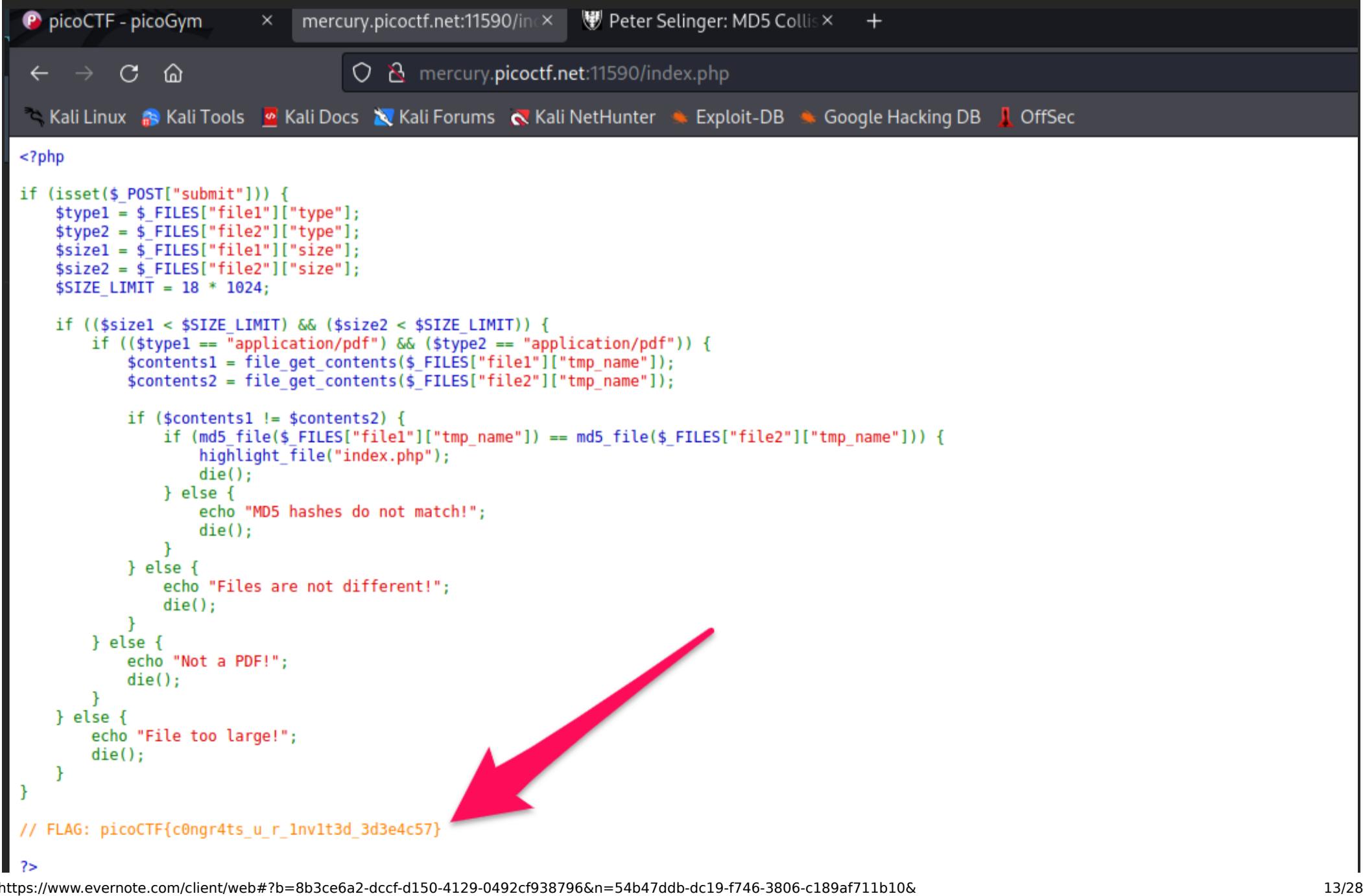


Found this: <https://www.msds.dal.ca/~selinger/md5collision/>

Downloaded two files with collisions



I had to rename the files with .pdf



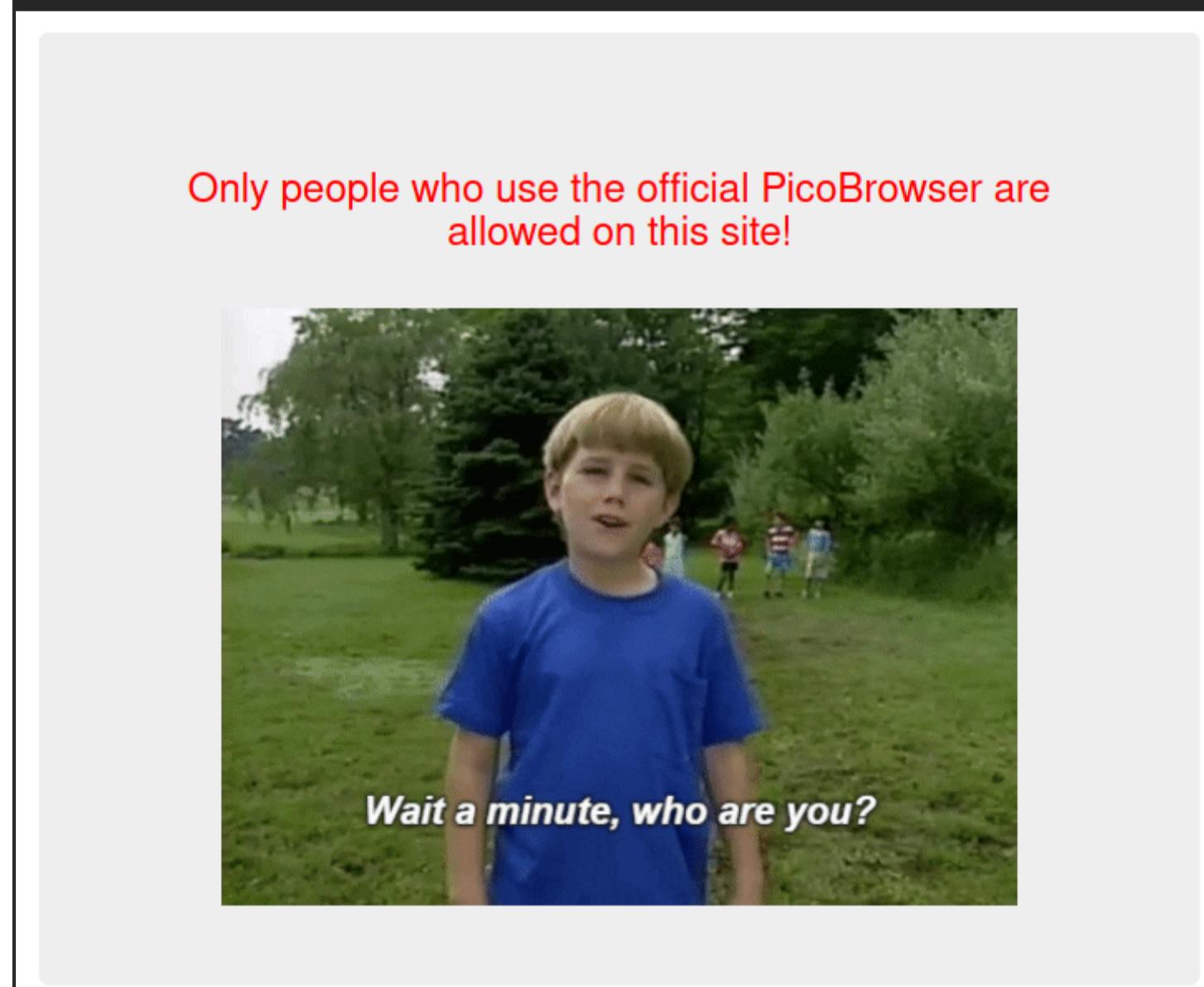
The screenshot shows a web browser window with the URL "mercury.picoctf.net:11590/index.php". The page content is a PHP script. A red arrow points to the line where MD5 hashes are compared:

```
<?php  
if (isset($_POST["submit"])) {  
    $type1 = $_FILES["file1"]["type"];  
    $type2 = $_FILES["file2"]["type"];  
    $size1 = $_FILES["file1"]["size"];  
    $size2 = $_FILES["file2"]["size"];  
    $SIZE_LIMIT = 18 * 1024;  
  
    if (($size1 < $SIZE_LIMIT) && ($size2 < $SIZE_LIMIT)) {  
        if (($type1 == "application/pdf") && ($type2 == "application/pdf")) {  
            $contents1 = file_get_contents($_FILES["file1"]["tmp_name"]);  
            $contents2 = file_get_contents($_FILES["file2"]["tmp_name"]);  
  
            if ($contents1 != $contents2) {  
                if (md5_file($_FILES["file1"]["tmp_name"]) == md5_file($_FILES["file2"]["tmp_name"])) {  
                    highlight_file("index.php");  
                    die();  
                } else {  
                    echo "MD5 hashes do not match!";  
                    die();  
                }  
            } else {  
                echo "Files are not different!";  
                die();  
            }  
        } else {  
            echo "Not a PDF!";  
            die();  
        }  
    } else {  
        echo "File too large!";  
        die();  
    }  
}  
  
// FLAG: picoCTF{c0ngr4ts_u_r_lnv1t3d_3d3e4c57}  
?>
```

```
<!DOCTYPE html>
<html lang="en">
```

Invitation received!

Is "iiiiiiinnnnnnnnnnnnnnnnnnnn" a clue?



Hmm. This looks like a job for Burp.

Request

Response

https://www.evernote.com/client/web#?b=8b3ce6a2-dccf-d150-4129-0492cf938796&n=54b47ddb-dc19-f746-3806-c189af711b10&

14/28

```

1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:1270
3 User-Agent: PicoBrowser
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11

```

I don't trust users visiting from another site.



This kid is already getting on my nerves!!!

I think I need a list of request header types

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers>

Even better

https://kapeli.com/cheat_sheets/HTTP_Header_Fields.docset/Contents/Resources/Documents/index

HTTP Header Fields Cheat Sheet - Kap... 230 kB

Request	Response
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:1270 3 Referer: http://mercury.picoctf.net:1270 4 User-Agent: PicoBrowser 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 Upgrade-Insecure-Requests: 1 11 Cache-Control: max-age=0 12 </pre>	<p>Sorry, this site only worked in 2018.</p>

Just "mercury.picoctf.net" didn't work so I had to actually complete the socket

Request	Response
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:1270 3 Referer: http://mercury.picoctf.net:1270 4 Date: Thu, 15 Dec 2018 00:00:00 GMT 5 User-Agent: PicoBrowser 6 Accept: 7 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 8 Accept-Language: en-US,en;q=0.5 9 Accept-Encoding: gzip, deflate 10 Connection: close 11 Upgrade-Insecure-Requests: 1 12 Cache-Control: max-age=0 13 </pre>	<p>I don't trust users who can be tracked.</p>



Do not track

<https://www.geeksforgeeks.org/http-headers-dnt/>

Syntax:

DNT:0

DNT:1

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < > ↻ ↺

Request

Pretty Raw Hex ⌂ ⌂ ⌂

```

1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:1270
3 Referer: http://mercury.picoctf.net:1270
4 Date: Thu, 15 Dec 2018 00:00:00 GMT
5 User-Agent: PicoBrowser
6 DNT: 0 do not track
7 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14

```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂

This website is only for people from Sweden.

I tried "location" and "origin"; finally, I googled "request header change senders ipaddress"

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-For>

Burp Project Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < > ↻ ↺

Request

Pretty Raw Hex ⌂ ⌂ ⌂

```

1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:1270
3 Referer: http://mercury.picoctf.net:1270
4 Date: Thu, 15 Dec 2018 00:00:00 GMT
5 User-Agent: PicoBrowser
6 DNT: 0
7 X-Forwarded-For: 85.226.200.210 hardest one to figure out
8 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Cache-Control: max-age=0
14

```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂

You're in Sweden but you don't speak Swedish?



Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < > ↻ ↻

Request

Pretty Raw Hex ⌂ ln ⌂

```

1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:1270
3 Referer: http://mercury.picoctf.net:1270
4 Date: Thu, 15 Dec 2018 00:00:00 GMT
5 User-Agent: PicoBrowser
6 DNT: 0
7 X-Forwarded-For: 85.226.200.210
8 Accept-Language: sv
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
10 Accept-Language: en-US,en;q=0.5
11 Accept-Encoding: gzip, deflate
12 Connection: close
13 Upgrade-Insecure-Requests: 1
14 Cache-Control: max-age=0
15
16

```

Response

Pretty Raw Hex Render ⌂ ln ⌂

What can I say except, you are welcome

picoCTF{http_h34d3rs_v3ry_c00l_much_w0w_f56f58a5}

© PicoCTF

Apparently, not 'sw' but 'sv'

login ⌂

Tags: Category: 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)

6,312 solves / 9,809 attempts (64%)

86% Liked

picoCTF{FLAG} **Submit Flag**



I have Burp Suite open and tried random login but nothing was sent the burp.

```

1 <!doctype html>
2 <html>
3   <head>
4     <link rel="stylesheet" href="styles.css">
5     <script src="index.js"></script>
6   </head>
7   <body>
8     <div>
9       <h1>Login</h1>
10      <form method="POST">
11        <label for="username">Username</label>
12        <input name="username" type="text"/>
13        <label for="password">Password</label>
14        <input name="password" type="password"/>
15        <input type="submit" value="Submit"/>
16      </form>
17    </div>
18  </body>
19 </html>
20

```

looking at html i see a .js

clicking .js reveal the following

```

(async()=>{await new Promise((e=>window.addEventListener("load",e))),document.querySelector("form").addEventListener("submit",(e=>
{e.preventDefault();const r={u:"input[name=username]",p:"input[name=password]"},t={};for(const e in
r)t[e]=btoa(document.querySelector(r[e]).value).replace(/=/g,"");return"YWRtaW4"!==t.u?alert("Incorrect
Username"):"cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ"!==t.p?alert("Incorrect Password"):void alert(`Correct Password! Your
flag is ${atob(t.p)}.`)}))})();

```

cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ

CyberChef from Base 64 (The magic filter)

to load)	Result snippet	Properties
-Za-z0-9-_ ,true)	picoCTF{53rv3r_53rv3r_53rv3r_53rv3r}	Valid UTF8

	<code>_53rv3r}</code>	Entropy: 3.16	
-Za-z0-9_.',true)	picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}	Valid UTF8 Entropy: 3.16	
	cG1jb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ	Matching ops: Fr Valid UTF8 Entropy: 4.40	

Some Assembly Required 2 B

Tags: Category: Web Exploitation

AUTHOR: SEARS SCHULZ

Description

<http://mercury.picoctf.net:61778/index.html>

Hints
(None)

1,560 solves / 3,361 attempts (46%)

D picoCTF{FLAG} L 53% Liked U

Submit Flag

firefox - Mercury - Kali Linux - Kali Tools - Kali Docs - Kali Forums - Kali NetHunter - Exploit -

picoCTF - picoGym X mercury.picoctf.net:61778/index.html +

← → ⌂ ⌄ ⌁ D L mercury.picoctf.net:61778/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit

Enter flag:

Submit

firefox - Mercury - Kali Linux - Kali Tools - Kali Docs - Kali Forums - Kali NetHunter - Exploit -

Enter flag:

Submit

Incorrect!

Entering "flag" does not work. haha!

While dirsearch is running i look at html

```

1 <html>
2 <head>
3   <meta charset="UTF-8">
4   <script src="Y8splx37qY.js"></script>
5 </head>
6 <body>
7   <h4>Enter flag:</h4>
8   <input type="text" id="input"/>
9   <button onclick="onButtonPress()">Submit</button>
10  <p id="result"></p>
11 </body>
12 </html>
13

```

and find .js

```

const _0x6d8f=
['copy_char','value','207aLjBod','1301420SaUSqf','233ZRpipt','2224QffgXU','check_flag','408533hsoVYx','instance','278338GVFUUrH','Correct!',54
9933ZVjkwI','innerHTML','charCodeAt','./aD8SvhyVkb','result','977AzKzwq','Incorrect!','exports','length','getElementById','1jIrMBu','input','6
15361geljRK'];const _0x5c00=function(_0x58505a,_0x4d6e6c){_0x58505a=_0x58505a-0xc3;let _0x6d8fc4=_0x6d8f[_0x58505a];return _0x6d8fc4;};
(function(_0x12fd07,_0x4e9d05){const _0x4f7b75=_0x5c00;while(![]){try{const _0x1bb902=-parseInt(_0x4f7b75(0xc8))*-parseInt(_0x4f7b75(0xc9))+-
parseInt(_0x4f7b75(0xcd))+parseInt(_0x4f7b75(0xcf))+parseInt(_0x4f7b75(0xc3))+-
parseInt(_0x4f7b75(0xc6))*parseInt(_0x4f7b75(0xd4))+parseInt(_0x4f7b75(0xcb))+-
parseInt(_0x4f7b75(0xd9))*parseInt(_0x4f7b75(0xc7));if(_0x1bb902===_0x4e9d05)break;else _0x12fd07['push'](_0x12fd07['shift']
());}catch(_0x4f8a){_0x12fd07['push'](_0x12fd07['shift']());}}}{_0x6d8f,0x4bb06});let exports;(async()=>{const _0x835967=_0x5c00;let
_0x1adb5f=await fetch(_0x835967(0xd2)),_0x355961=await WebAssembly['instantiate'](await _0x1adb5f['arrayBuffer']
()),_0x5c0ffa=_0x355961[_0x835967(0xcc)];exports=_0x5c0ffa[_0x835967(0xd6)];});function onButtonPress(){const _0x50ea62=_0x5c00;let
_0x5f4170=document[_0x50ea62(0xd8)](_0x50ea62(0xda))[_0x50ea62(0xc5)];for(let _0x19d3ca=0x0;_0x19d3ca<_0x5f4170['length'];_0x19d3ca++)
{exports[_0x50ea62(0xc4)](_0x5f4170[_0x50ea62(0xd1)](_0x19d3ca),_0x19d3ca);}exports['copy_char']
(0x0,_0x5f4170[_0x50ea62(0xd7)]),exports[_0x50ea62(0xca)]()=0x1?document['getElementById'](_0x50ea62(0xd3))
[_0x50ea62(0xd0)]=_0x50ea62(0xce):document[_0x50ea62(0xd8)](_0x50ea62(0xd3))['innerHTML']=_0x50ea62(0xd5);}

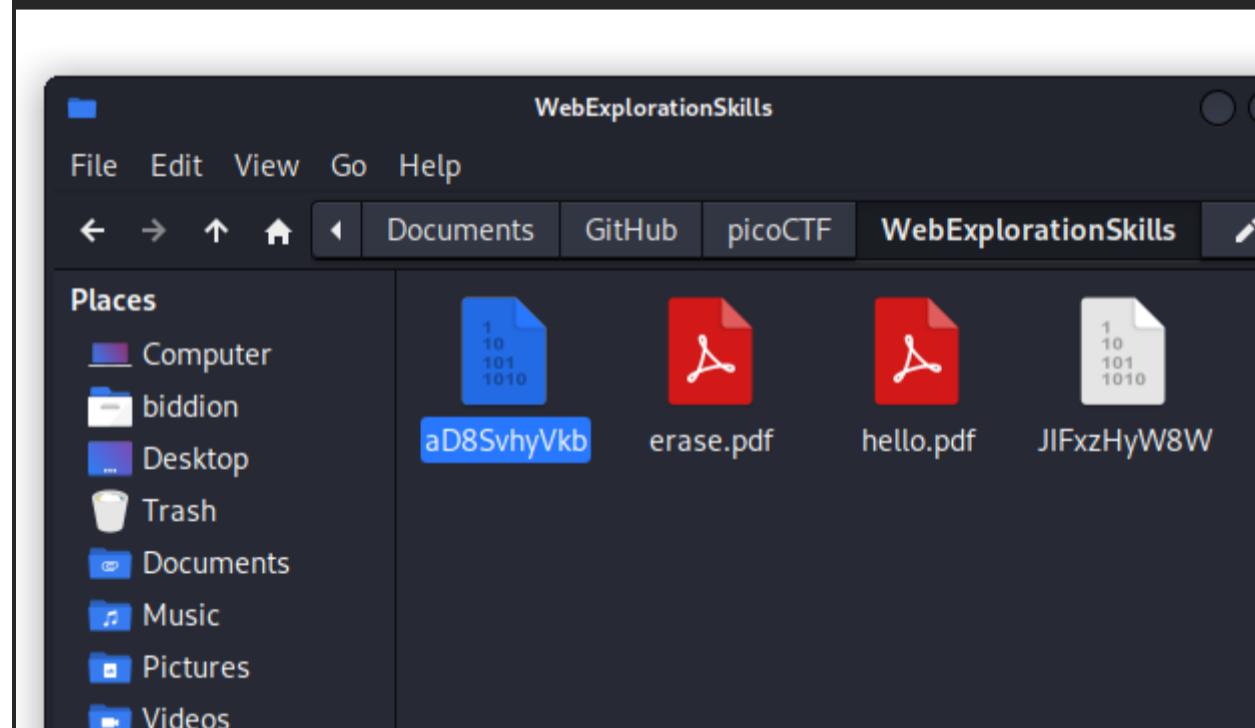
```

These two look interesting

'278338GVFUUrH','Correct!'

'./aD8SvhyVkb'

I download the file



└──(biddion㉿kali)-[~/Documents/GitHub/picoCTF/WebExplorationSkills]

└─\$ file aD8SvhyVkb

aD8SvhyVkb: WebAssembly (wasm) binary module version 0x1 (MVP)

both running this and cat'ing it doesn't bear fruit nor flag.

copy 278338GVFUUrH into the box doesn't work nor does aD8SvhyVkb

Enter flag:

Incorrect!

Being stumped, I looked up a writeup and found I need to know about webassembly/debugging



Super Serial

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

Try to recover the flag stored on this website <http://mercury.picoctf.net:5428/>

Hints

1,178 solves / 1,842 attempts (64%)

71% Liked

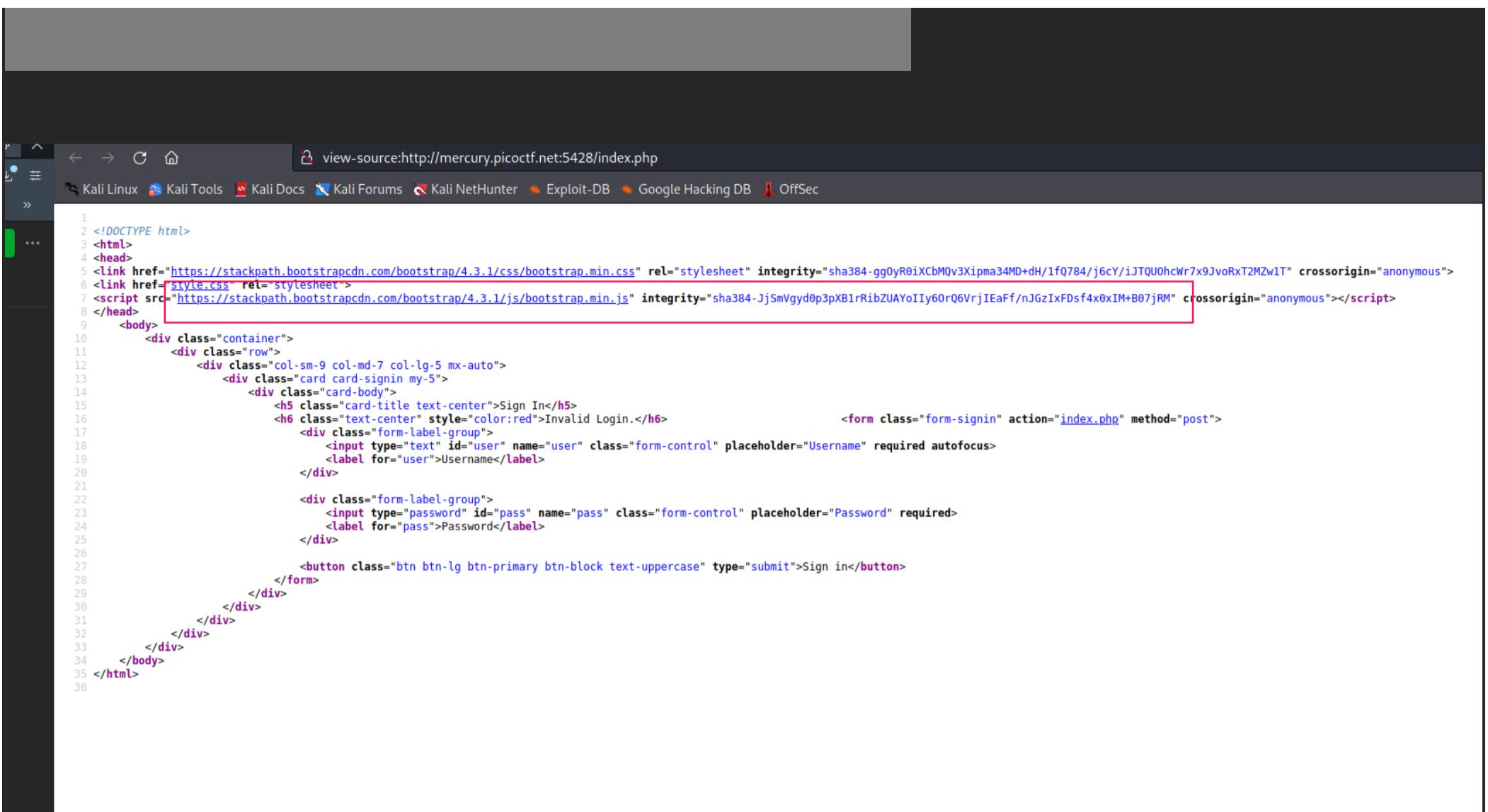
picoCTF{FLAG}

Sign In

Invalid Login.

Username

Password



```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <head>
5 <link href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-gg0yR0iXcbM0v3Xipma34MD+dH/1fQ784/j6cYi3TQU0hcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
6 <link href="style.css" rel="stylesheet">
7 <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy60r06VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>
8 </head>
9 <body>
10 <div class="container">
11 <div class="row">
12 <div class="col-sm-9 col-md-7 col-lg-5 mx-auto">
13 <div class="card card-signin my-5">
14 <div class="card-body">
15 <h5 class="card-title text-center">Sign In</h5>
16 <h6 class="text-center" style="color:red">Invalid Login.</h6>
17 <div class="form-label-group">
18 <input type="text" id="user" name="user" class="form-control" placeholder="Username" required autofocus>
19 <label for="user">Username</label>
20 </div>
21 <div class="form-label-group">
22 <input type="password" id="pass" name="pass" class="form-control" placeholder="Password" required>
23 <label for="pass">Password</label>
24 </div>
25 <div class="form-label-group">
26 <button class="btn btn-lg btn-primary btn-block text-uppercase" type="submit">Sign in</button>
27 </div>
28 </div>
29 </div>
30 </div>
31 </div>
32 </div>
33 </div>
34 </body>
35 </html>

```

The .js which is too massive to be of any use to me.

Hints

1

The flag is at ..//flag

DirSearch (7.0.1.2) v0.4.2

Extensions: php, aspx, jsp, html, js | **HTTP method**

Output File: /home/biddion/.dirsearch/reports/merc

Error Log: /home/biddion/.dirsearch/logs/errors-22

Target: http://mercury.picoctf.net:5428/

[14:35:30] Starting:

```

[14:36:08] 200 - 0B - /access.log
[14:36:34] 200 - 1KB - /authentication.php
[14:36:46] 200 - 0B - /cookie.php
[14:37:03] 200 - 1KB - /index.php
[14:37:03] 200 - 1KB - /index.php/login/
[14:37:32] 200 - 36B - /robots.txt

```

Task Completed

I'll try each of the above

/access.log is just as it says; but it's empty

/authentication.php

Welcome guest

GO BACK TO LOGIN

/cookie.php

The screenshot shows the NetworkMiner interface with the 'Cookies' tab selected. A single cookie entry is visible:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
PHPSESSID	3h0hmenmhkifpg04f09hbcn99h	mercury.picocft.net	/	Session	35	false	false	None

Hmmmm "3h0hmenmhkifpg04f09hbcn99h"?

/robots.txt

The screenshot shows a browser window with the URL `mercury.picocft.net:5428/robots.txt`. The content of the robots.txt file is displayed:

```
User-agent: *
Disallow: /admin.php*
```

/admin.php*_ not found nor is .php an option

Let's try SQLi via Burp's Intruder.--Doesn't look fruitful

I looked up more about what is .phps

<https://filext.com/file-extension/PHPS>

The text in BG is a bit weird

The screenshot shows a browser window with the URL `mercury.picocft.net:5428/index.php*`. The page content is:

```
is_guest() || $perm_res->is_admin() { setcookie("login", urlencode(base64_encode(serialize($perm_res))), time() + (86400 * 30), "/"); header("Location: authentication.php"); die(); } else { $msg = 'Invalid Login.' }
'; } } ?>
```

The screenshot shows a sign-in form with the following fields:

- Sign In
- Username
- Password
- SIGN IN

I'm not sure what to do here. I don't know much about how websites work.___I have to quit here.

The screenshot shows a challenge card for 'Most Cookies'. At the top, it says 'Web Exploitation' and '110 points'. Below that, the challenge title is 'Most Cookies' with a bookmark icon. It has 'Tags: Category: Web Exploitation' and 'AUTHOR: MADSTACKS'. The 'Description' section contains the text: 'Alright, enough of using my own encryption. Flask session cookies should be plenty secure! [server.py](#) <http://mercury.picoctf.net:65344/>'. To the right, there's a 'Hints' section with a blue box containing the number '1' and the text 'How secure is a flask cookie?'. Below the description, it shows '1,368 solves / 2,676 attempts (51%)' with '86% Liked' and like/dislike buttons. At the bottom, there's a text input field with 'picoCTF{FLAG}' and a 'Submit Flag' button.

First I need to learn what is a flask 'session' cookie

People also ask :

What is Flask session cookie?

The session data is **stored on the top of cookies** and signed by the server cryptographically. ... In the flask, a session object is used to track the session data which is a dictionary object that contains a key-value pair of the session variables and their associated values.

Setting a Cookie

In Flask, we use `set_cookie()` method of the response object to set cookies. The syntax of `set_cookie()` method is as follows:

```
set_cookie(key, value="", max_age=None)
```

The `key` is a required argument and refers to the name of the cookie. The `value` is data you want to store in the cookie and it defaults to empty string. The `max_age` refers to the expiration time of the cookie in seconds, if not set the cookie will cease to exist when the user closes the browser.

Open `main2.py` and add the following code just after the `contact()` view function:

`flask_app/main2.py`

```
1 from flask import Flask, render_template, request, redirect, url_for, flash, make_response
2 ...
3 @app.route('/cookie/')
4 def cookie():
5     res = make_response("Setting a cookie")
6     res.set_cookie('foo', 'bar', max_age=60*60*24*365*2)
7     return res
8 ...
```

Here we are creating a cookie named `foo` with the value `bar` that will last for 2 years.

Start the server and visit <http://localhost:5000/cookie/>. You should see a page with "Settings".

Looking at the .py that was supplied

```
        return resp
    else:
        message = "That doesn't appear to be a valid cookie."
        category = "danger"
        flash(message, category)
        resp = make_response(redirect("/"))
        session["very_auth"] = "blank"
        return resp

@app.route("/reset")
def reset():
    resp = make_response(redirect("/"))
    session.pop("very_auth", None)
    return resp

@app.route("/display", methods=["GET"])
def flag():
    if session.get("very_auth"):
        check = session["very_auth"]
        if check == "admin":
            resp = make_response(render_template("flag.html", value=flag_value, title=title))
            return resp
        flash("That is a cookie! Not very special though...", "success")
        return render_template("not-flag.html", title=title, cookie_name=session["very_auth"])
    else:
        resp = make_response(redirect("/"))
        session["very_auth"] = "blank"
        return resp

if __name__ == "__main__":
    app.run()
```

Does this mean I need to have 'admin' cookie?



I learned about cookie encryption

<https://jwt.io>

picobrowser 

Tags: Category: Web Exploitation

AUTHOR: ARCHIT

Description

This website can be rendered only by **picobrowser**, go and catch the flag!

<https://jupiter.challenges.picoctf.org/problem/26704/> ([link](#)) or
<http://jupiter.challenges.picoctf.org:26704>

Hints

1

You don't need to download a new web browser

12,808 solves / 17,542 attempts (73%)

89% Liked



This was easy with Burp

Request

```

1 GET /problem/26704/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga=GA1.2.1160019831.1642929874; _gid=GA1.2.222856668.1642929874
4 User-Agent: picobrowser
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://jupiter.challenges.picoctf.org/problem/26704/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17

```

Response

My New Website

picobrowser!

Flag:

picoCTF{p1c0_s3cr3t_ag3nt_e9b160d0}

© PicoCTF 2019

Client-side-again

Tags: Category: Web Exploitation

AUTHOR: DANNY

Description

Can you break into this super secure portal?

<https://jupiter.challenges.picoctf.org/problem/56816/> ([link](#)) or
<http://jupiter.challenges.picoctf.org:56816>

Hints

1

8,746 solves / 19,748 attempts (44%)

74% Liked

picoCTF(FLAG)

Hints

1

What is obfuscation?

<https://www.quora.com/Is-code-obfuscation-a-common-practice-to-protect-the-client-side-code-in-web-applications>

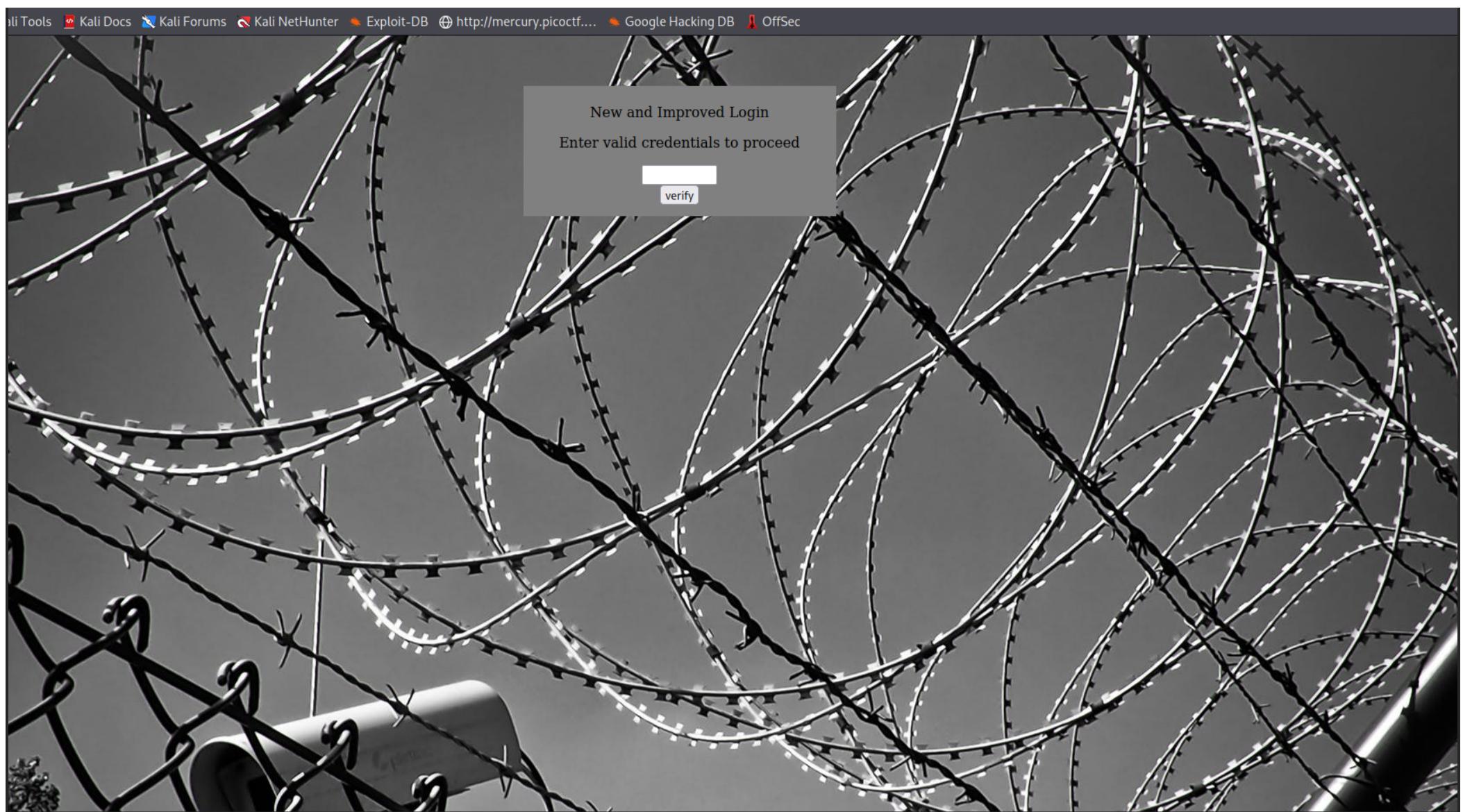
Various build tools are available to developers to perform obfuscation, with a few of the most prominent being the JavaScript Obfuscator, Google Closure Compiler, YUI Compressor, and UglifyJS. Arguably, these processors are just **minifiers with added optimizations to mangle code**.

Secure Login Portal V2.0 | My New Website | PicoCTF2021-Writeup/Mc | Most Cookies

https://jupiter.challenges.picoctf.org/problem/56816/

https://www.evernote.com/client/web#?b=8b3ce6a2-dccf-d150-4129-0492cf938796&n=54b47ddb-dc19-f746-3806-c189af711b10&

26/28



← → ⌂ ⌄

view-source:https://jupiter.challenges.picoctf.org/problem/56816/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB http://mercury.picoctf.... Google Hacking DB OffSe

```

1 <html>
2 <head>
3 <title>Secure Login Portal V2.0</title>
4 </head>
5 <body background="barbed_wire.jpeg">
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>
8
9 <script type="text/javascript">
10 var _0x5a46=['37115','_again_3','this','Password\x20Verified','Incorrect\x20password','getElementById','value','substring','picoCTF{','r
11 </script>
12 <div style="position:relative; padding:5px; top:50px; left:38%; width:350px; height:140px; background-color:gray">
13 <div style="text-align:center">
14 <p>New and Improved Login</p>
15
16 <p>Enter valid credentials to proceed</p>
17 <form action="index.html" method="post">
18 <input type="password" id="pass" size="8" />
19 <br/>
20 <input type="submit" value="verify" onclick="verify(); return false;" />
21 </form>
22 </div>
23 </div>
24 </body>
25 </html>
26

```

this returns "not found"

Not much here

```

DirSearch v0.4.2
First Appearance

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Thread
Output File: /home/biddion/.dirsearch/reports/jupiter.challenges
Error Log: /home/biddion/.dirsearch/logs/errors-22-01-24_15-36-1
Target: https://jupiter.challenges.picoctf.org/problem/56816/
[15:36:10] Starting: picoCTF 2021
[15:36:59] 200 - 2KB - /problem/56816/index.html picoCTF 2020 Mini-Competition
Task Completed

```

These problems are only getting harder. Maybe I'll come back next year.

The End!--for now