

Web Exploitation

1

Insp3ct0r

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ZARATEC/DANNY

Description

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>

Solution

Inspect Me

What

How

How

I used these to make this site:
HTML
CSS
JS (JavaScript)

Looking at the website, it says HTML, CSS and JS have been used to make the website. Hence the flag is stored in parts in all the 3 components.

```
<button class="tablink" onclick="openTab('tababout', this, '#222')"
style="background-color: rgb(34, 34, 34);">How</button>
<div id="tabintro" class="tabcontent" style="display: none;"></div>
<div id="tababout" class="tabcontent" style="display: block;">
  <h3>How</h3>
  <p></p>
  <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3 d3 -->
</div>
</div>
</body>
</html>
```

Inspecting the HTML, we come across the first part of the flag.

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

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

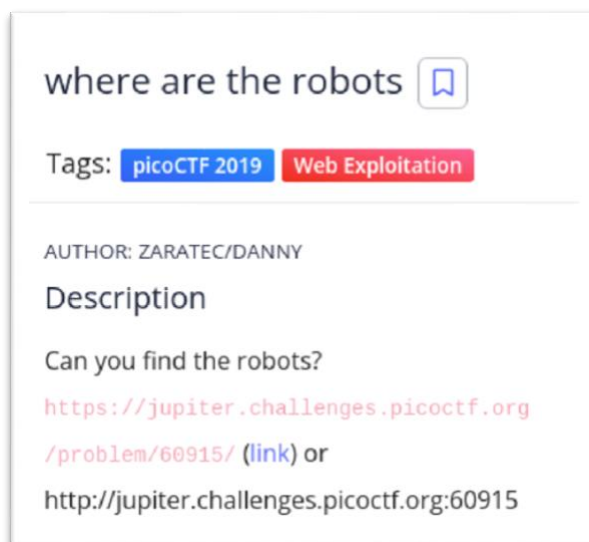
/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```

Looking at the CSS, we come across the second part of the flag.

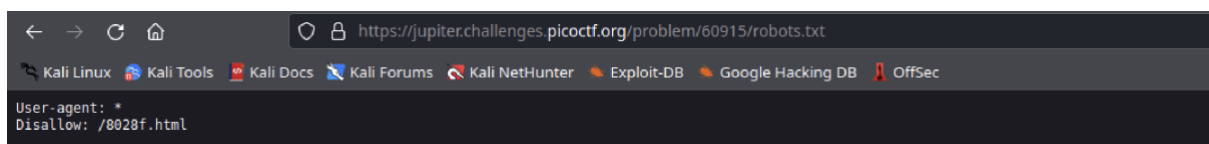
```
if(elmnt.style != null) {  
    elmnt.style.backgroundColor = color;  
}  
  
window.onload = function() {  
    openTab('tabintro', this, '#222');  
}  
  
/* Javascript sure is neat. Anyways part 3/3 of the flag: lucky?f10be399 */
```

The JS has the third part of the flag. Putting all the 3 together, we have the final flag.

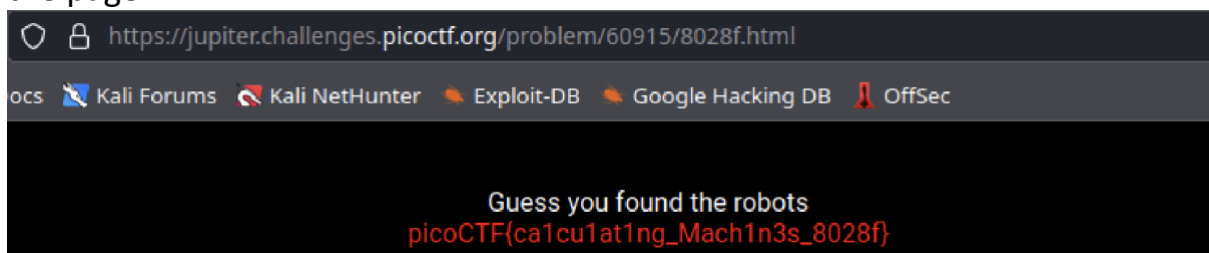
2.



Solution



Accessing the robots.txt page using the URL, gives us a disallowed section of the page.



Accessing that page, we find the flag.

3.

logon

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>

Solution

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

No flag for you

er

Network

Style Editor

Performance

Memory

Storage

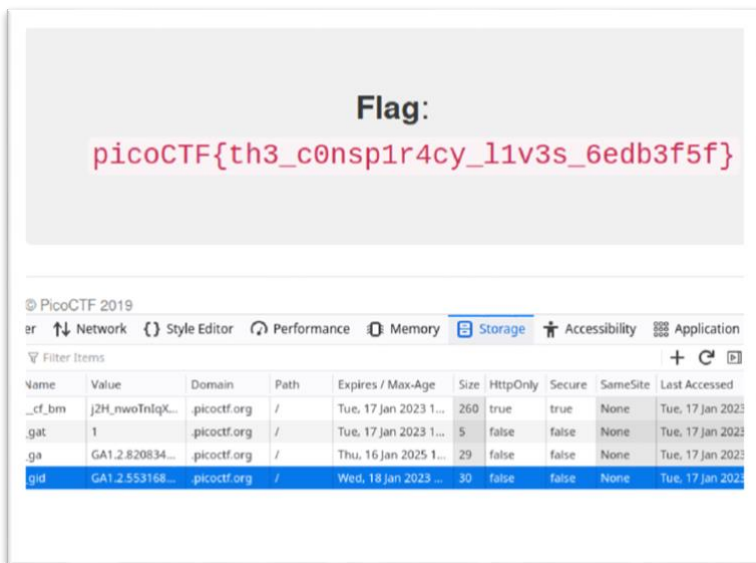
Accessibility

Application

Filter Items

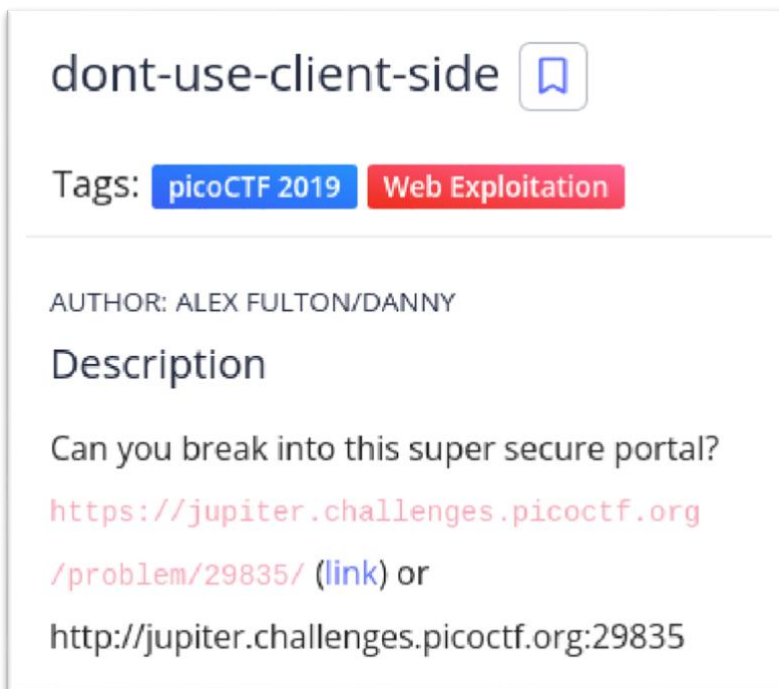
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__cf_bm	1nqavo6.KT133...	.picoctf.org	/	Tue, 17 Jan 2023 1...	260	true	true	None	Tue, 17 Jan 2023
.gat	1	.picoctf.org	/	Tue, 17 Jan 2023 1...	5	false	false	None	Tue, 17 Jan 2023
.ga	GA1.2.820834...	.picoctf.org	/	Thu, 16 Jan 2025 1...	29	false	false	None	Tue, 17 Jan 2023
.gid	GA1.2.553168...	.picoctf.org	/	Wed, 18 Jan 2023 ...	30	false	false	None	Tue, 17 Jan 2023
admin	false	jupiter.chall...	/	Session	10	false	false	None	Tue, 17 Jan 2023
password	password	jupiter.chall...	/	Session	16	false	false	None	Tue, 17 Jan 2023
username	lne	jupiter.chall...	/	Session	11	false	false	None	Tue, 17 Jan 2023

After trying to login as Joe with a random password, we get this admin declared as false.



Toggling it to true from false and then reloading the page, we find the password.

4.



Solution

```

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")
              }
            }
          }
        }
      }
    }
  }
}

```

The JavaScript of the page reveals the flag in a jumbled order. Rearranging it, we arrive at the flag.

5.

It is my Birthday

Tags:
picoCTF 2021
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:63578/>

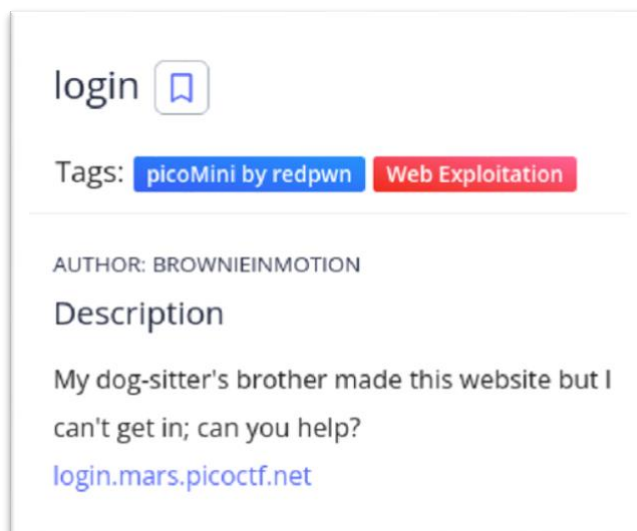
Solution

```
// FLAG: picoCTF{c0ngr4ts u_r lnvlt3d 5c8c5ce2}
```

Submitting 2 pdf's taken from the website -

<https://www.mathstat.dal.ca/~selinger/md5collision/> we get the flag displayed on the page.

6.



Solution

Using burpsuite's repeater to change the credentials as needed.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1				27 <p class="lead">			
2 Host: mercury.picoctf.net:36622				28 </p>			
3 User-Agent: PicoBrowser				29 <div class="row">			
4 Accept:				30 <div class="col-xs-12 col-sm-12 col-md-12">			
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8				<h3 style="color:red">			
Accept-Language: en-US,en;q=0.5				Only people who use the official PicoBrowser are			
Accept-Encoding: gzip, deflate				allowed on this site!			
Connection: close				</h3>			
Upgrade-Insecure-Requests: 1				</div>			
Cache-Control: max-age=0				</div>			
				33 			

The website shows that only people who use PicoBrowser are allowed in here. So changing the User-Agent to PicoBrowser.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1				19 </head>			
2 Host: mercury.picoctf.net:36622				20			
3 User-Agent: PicoBrowser				21 <body>			
4 Accept:				22			
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8				23 <div class="container">			
Accept-Language: en-US,en;q=0.5				24 <div class="jumbotron">			
Accept-Encoding: gzip, deflate				25 <p class="lead">			
Connection: close				26 </p>			
Referer: mercury.picoctf.net:36622				27 <div class="row">			
Upgrade-Insecure-Requests: 1				28 <div class="col-xs-12 col-sm-12 col-md-12">			
Cache-Control: max-age=0				29 <h3 style="color:red">			
				30 I don't trust users visiting from another site.			
				</h3>			

The website now says it doesn't trust visitors from other sites. Hence we update the referrer to the original site name.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1				23 <body>			
2 Host: mercury.picoctf.net:36622				24			
3 Date: Wed, 21 Oct 2018 07:28:00 GMT				25 <div class="container">			
4 User-Agent: PicoBrowser				26 <div class="jumbotron">			
5 Accept:				27 <p class="lead">			
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8				28 </p>			
Accept-Language: en-US,en;q=0.5				29 <div class="row">			
Accept-Encoding: gzip, deflate				30 <div class="col-xs-12 col-sm-12 col-md-12">			
Connection: close				<h3 style="color:red">			
Referer: mercury.picoctf.net:36622				Sorry, this site only worked in 2018.			
Upgrade-Insecure-Requests: 1				</h3>			
Cache-Control: max-age=0				</div>			
				</div>			

The website says that the site has worked only in 2018. So we update the date accordingly.

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:36622 3 Date: Wed, 21 Oct 2018 07:28:00 GMT 4 User-Agent: PicoBrowser 5 DNT:1 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 Connection: close 10 Referer: mercury.picoctf.net:36622 11 Upgrade-Insecure-Requests: 1 12 Cache-Control: max-age=0 </pre>			<pre> 20 21 </head> 22 23 <body> 24 25 <div class="container"> 26 <div class="jumbotron"> 27 <p class="lead"> 28 </p> 29 <div class="row"> 30 <div class="col-xs-12 col-sm-12 col-md-12"> 31 <h3 style="color:red"> 32 I don't trust users who can be tracked. 33 </h3> </pre>			

As the site says it doesn't trust users who can be tracked, we update DNT to 1

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:36622 3 Date: Wed, 21 Oct 2018 07:28:00 GMT 4 User-Agent: PicoBrowser 5 DNT:1 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 Connection: close 10 X-Forwarded-For: 80.217.1.0 11 Referer: mercury.picoctf.net:36622 12 Upgrade-Insecure-Requests: 1 13 Cache-Control: max-age=0 </pre>			<pre> 20 21 </head> 22 23 <body> 24 25 <div class="container"> 26 <div class="jumbotron"> 27 <p class="lead"> 28 </p> 29 <div class="row"> 30 <div class="col-xs-12 col-sm-12 col-md-12"> 31 <h3 style="color:red"> 32 This website is only for people from Sweden. 33 </h3> </pre>			

As the website is only for Sweden, a Swiss IP address is used as the generating IP.

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:36622 3 Date: Wed, 21 Oct 2018 07:28:00 GMT 4 User-Agent: PicoBrowser 5 DNT:1 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 7 Accept-Language: sv-sv,sv;q=0.5 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 X-Forwarded-For: 80.217.1.0 11 Referer: mercury.picoctf.net:36622 12 Upgrade-Insecure-Requests: 1 13 Cache-Control: max-age=0 </pre>			<pre> 24 25 <div class="container"> 26 <div class="jumbotron"> 27 <p class="lead"> 28 </p> 29 <div class="row"> 30 <div class="col-xs-12 col-sm-12 col-md-12"> 31 <h3 style="color:red"> 32 You're in Sweden but you don't speak Swedish? 33 </h3> 34 </div> 35 </div> 36
 37 </pre>			

The accept language must be changed from English to Swedish for this to work.

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET / HTTP/1.1 2 Host: mercury.picoctf.net:36622 3 Date: Wed, 21 Oct 2018 07:28:00 GMT 4 User-Agent: PicoBrowser 5 DNT:1 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 7 Accept-Language: sv-sv,sv;q=0.5 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 X-Forwarded-For: 80.217.1.0 11 Referer: mercury.picoctf.net:36622 12 Upgrade-Insecure-Requests: 1 13 Cache-Control: max-age=0 </pre>			<pre> 27 <p class="lead"> 28 </p> 29 <div class="row"> 30 <div class="col-xs-12 col-sm-12 col-md-12"> 31 <h3 style="color:green"> 32 What can I say except, you are welcome 33 </h3> 34 </div> 35 </div> 36
 37 38 picoCTF{http_h34d3rs_v3ry_c00l_much_w0w_0da16bb2} 39 </pre>			

And finally, we are presented with the flag.

7.

picobrowser

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ARCHIT

Description

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

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

[/problem/50522/](#) ([link](#)) or

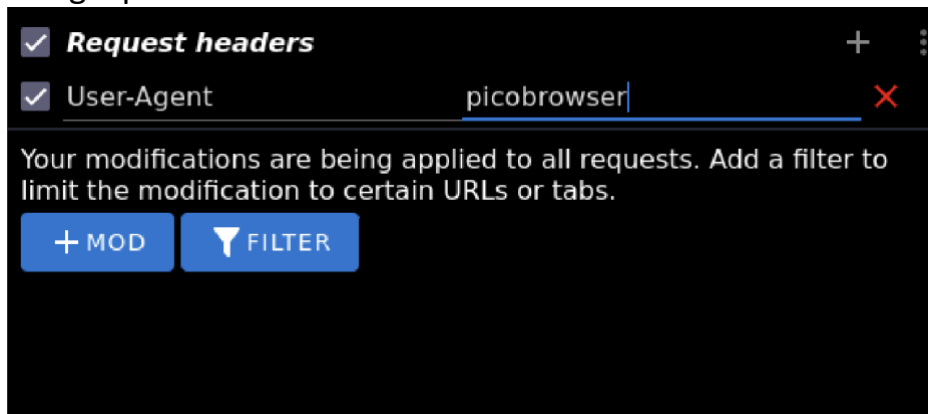
<http://jupiter.challenges.picoctf.org:50522>

Solution

You're not picobrowser! Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0 ×

Flag

If we try to access the flag using the browser, it doesn't allow as we are not using a picobrowser.



Using an extension called modheader to change the user-agent to picobrowser

picobrowser!



Flag:

picoCTF{p1c0_s3cr3t_ag3nt_51414fa7}

The flag is now displayed.