

Web Exploitation

dont-use-client-side

Author: Alex Fulton/Danny

Description

Can you break into this super secure

portal? <https://jupiter.challenges.picoctf.org/problem/29835/> ([link](#)) or

<http://jupiter.challenges.picoctf.org:29835>

```
<body bgcolor=blue>
<!-- standard MD5 implementation -->
<script type="text/javascript" src="md5.js"></script>

<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) == '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")
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Conditions in order:

1. `substring(0,4) == "pico"` → **pico**
2. `substring(4,8) == "CTF{"` → **CTF{**
3. `substring(8,12) == "no_c"` → **no_c**
4. `substring(12,16) == "lien"` → **lien**
5. `substring(16,20) == "ts_p"` → **ts_p**
6. `substring(20,24) == "lz_7"` → **lz_7**

7. `substring(24,28) == "723c"` → **723c**

8. `substring(28,32) == "e}"` → **e}**

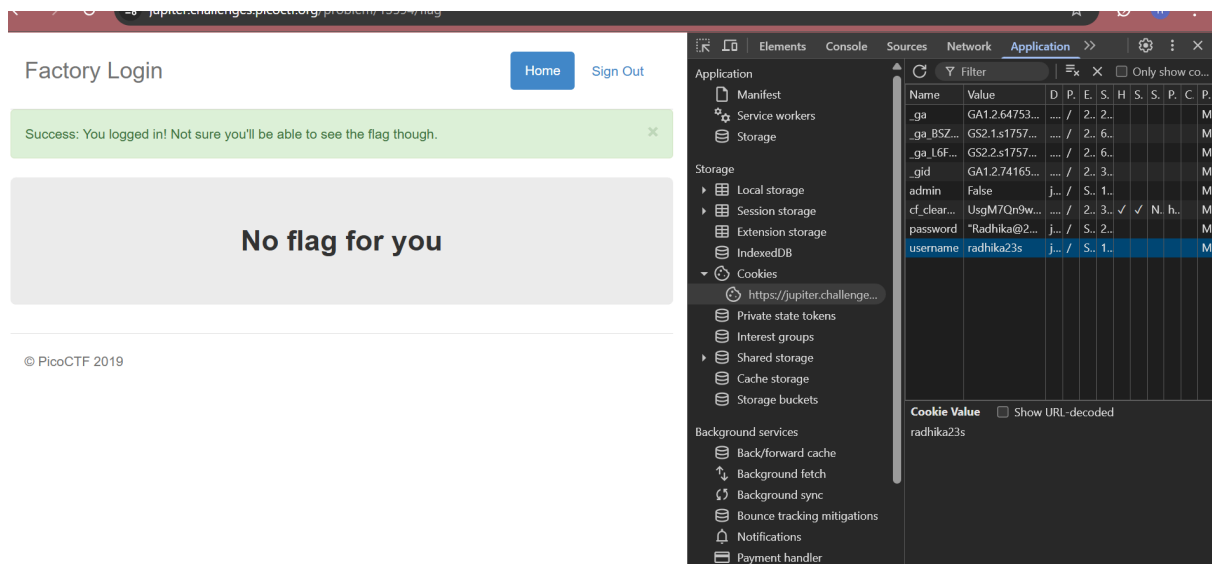
flag:picoCTF{no_clients_plz_7723ce}

logon

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>



Change:in application tab(in cookies)

- `username` → `Joe`
- `admin` → `True`

Flag:

picoCTF{th3_c0nsp1r4cy_l1v3s_d1c24fef}

© PicoCTF 2019

Insp3ct0r

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>

Hints

How do you inspect web code on a browser?

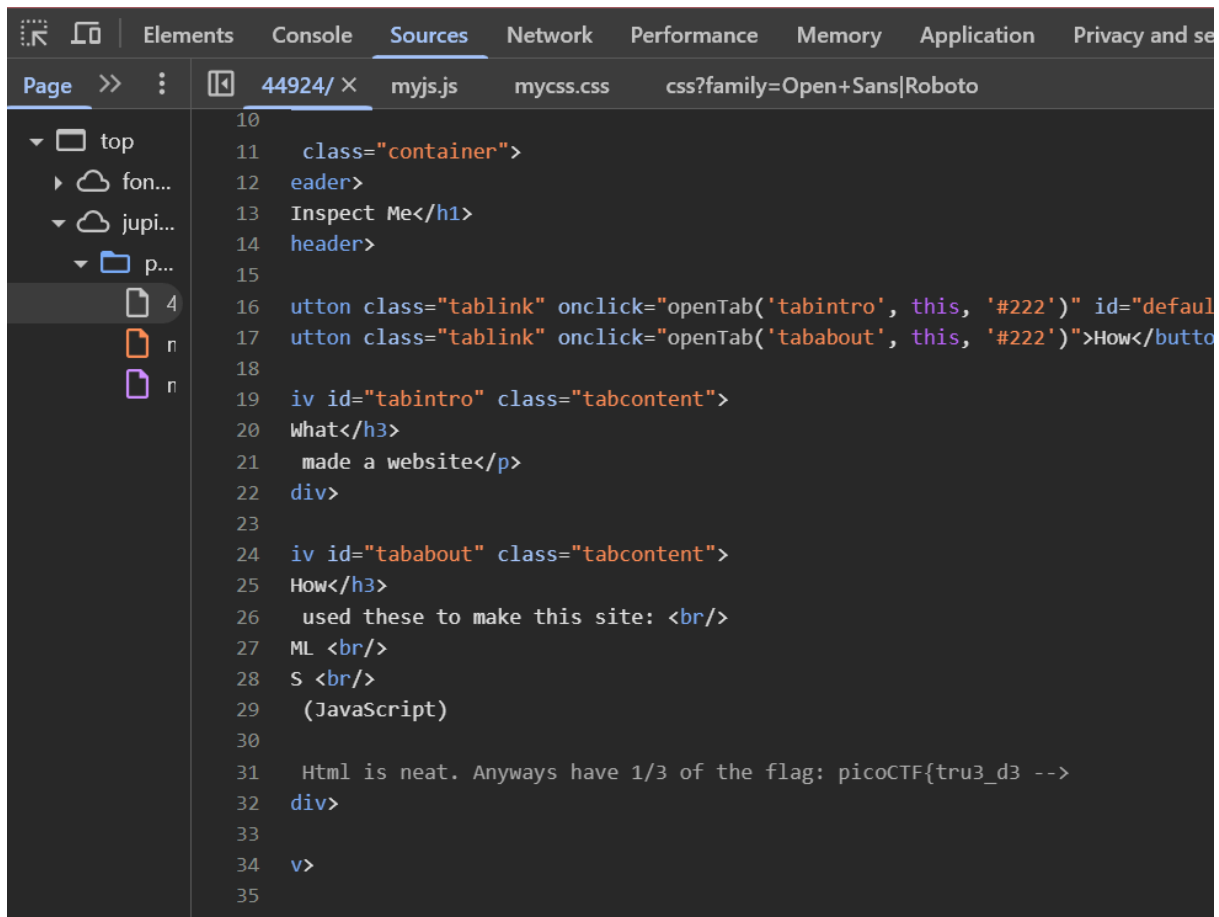
There's 3 parts

Insp3ct0r

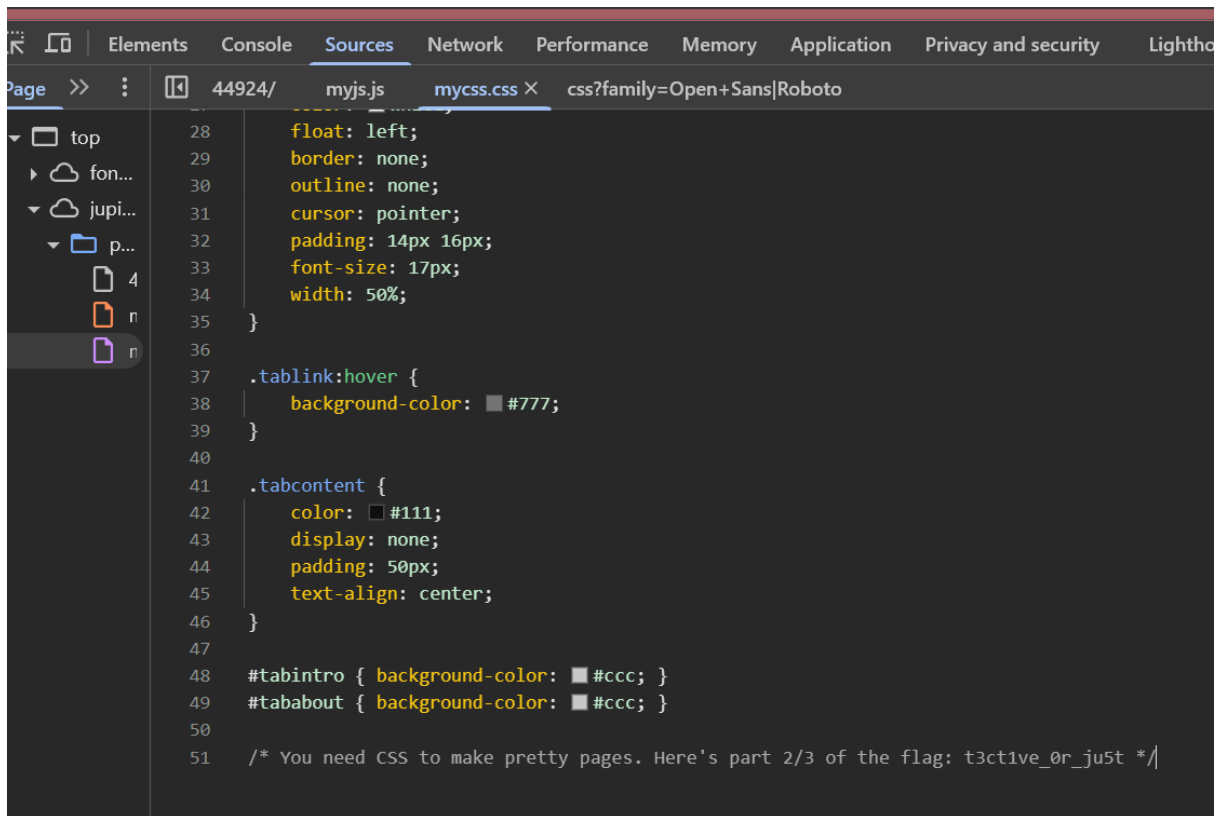
Author: zaratec/danny

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>



```
10
11   class="container">
12   eader>
13   Inspect Me</h1>
14   header>
15
16   utton class="tablink" onclick="openTab('tabintro', this, '#222')" id="default"
17   utton class="tablink" onclick="openTab('tababout', this, '#222')">How</button>
18
19   iv id="tabintro" class="tabcontent">
20   What</h3>
21   made a website</p>
22   div>
23
24   iv id="tababout" class="tabcontent">
25   How</h3>
26   used these to make this site: <br/>
27   ML <br/>
28   S <br/>
29   (JavaScript)
30
31   Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
32   div>
33
34   v>
35
```



```
28   float: left;
29   border: none;
30   outline: none;
31   cursor: pointer;
32   padding: 14px 16px;
33   font-size: 17px;
34   width: 50%;
35 }
36
37 .tablink:hover {
38   background-color: #777;
39 }
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 /* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```

```
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');
}

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

so flag:picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?f10be399}

where are the robots

Author: zaratec/Danny

Description

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

debug info: [u:880571 e: p: c:4 i:365]

Hints

What part of the website could tell you where the creator doesn't want you to look?

- Open the base site:

```
http://jupiter.challenges.picoctf.org:36474/
```

It only shows a simple message: *"Where are the robots?"*

- Append `/robots.txt` to the URL (standard trick in CTFs):

```
http://jupiter.challenges.picoctf.org:36474/robots.txt
```

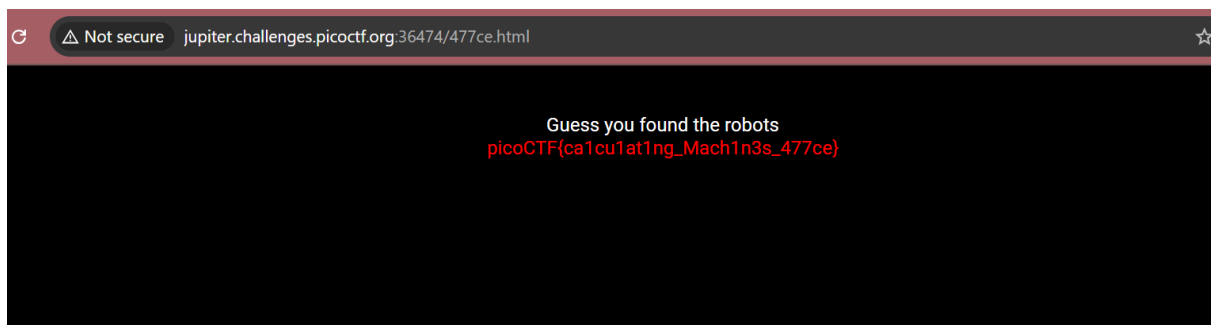
This shows:

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

- Visit the disallowed page:

```
http://jupiter.challenges.picoctf.org:36474/477ce.html
```

- That page contains the **flag**.



Client-side-again

Author: Danny

Description

Can you break into this super secure portal? <https://jupiter.challenges.picoctf.org/problem/60786/> ([link](#)) or <http://jupiter.challenges.picoctf.org:60786>

debug info: [u:880571 e: p: c:69 i:334]

Hints

What is obfuscation?

Array of strings

JS :

```
var _0x5a46=[  
'f49bf}', // [0]  
'_again_e', // [1]  
'this',    // [2]  
'Password Verified',  
'Incorrect password',  
'getElementById',  
'value',  
'substring',  
'picoCTF{', // [8]  
'not_this' // [9]  
];
```

Code logic (simplified)

```
function verify() {  
    checkpass = document.getElementById('pass').value;  
    split = 4;  
  
    if (checkpass.substring(0, 8) == "picoCTF{") {  
        if (checkpass.substring(7, 9) == "{n") {  
            if (checkpass.substring(8, 16) == "not_this") {  
                if (checkpass.substring(3, 6) == "oCT") {  
                    if (checkpass.substring(16, 24) == "_again_e") {  
                        if (checkpass.substring(6, 11) == "F{not") {  
                            if (checkpass.substring(24, 29) == "f49bf}") {  
                                if (checkpass.substring(12, 16) == "this") {  
                                    alert("Password Verified");  
                                }  
                            }  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```

```

    }
  }
}
}
}
}
}
}
} else {
  alert("Incorrect password");
}
}

```

3. Extracting the flag pieces

From conditions:

- `substring(0,8)` → `picoCTF{`
- `substring(8,16)` → `not_this`
- `substring(12,16)` → `this` ✓ (fits inside `not_this`)
- `substring(16,24)` → `_again_e`
- `substring(24,29)` → `f49bf}`
- Combined:

```
picoCTF{not_this_again_ef49bf}
```