JBU CTF

picoCTF writeup

발 표 자 허 송 이

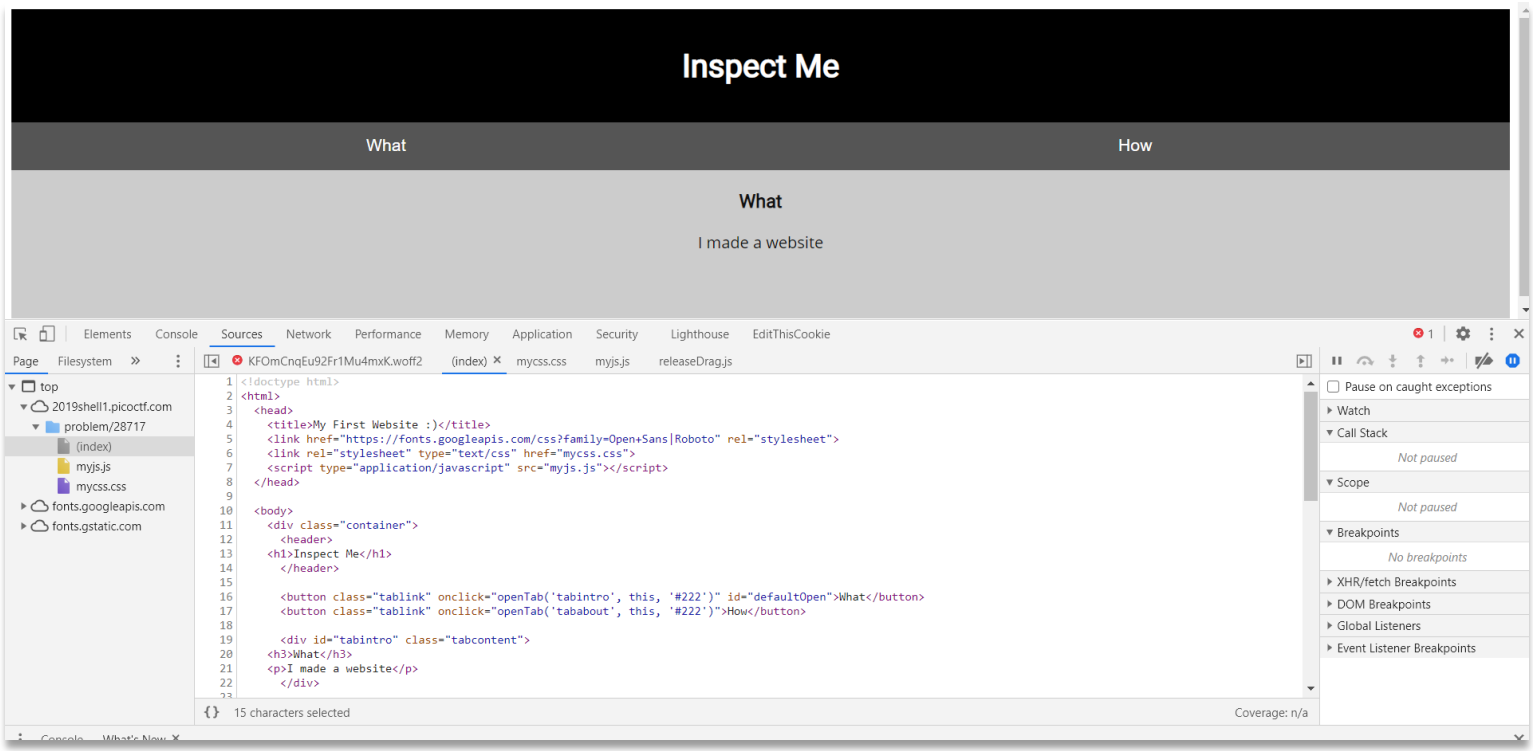
CONTENTS

Insp3ct0r - Points: 50 - (Solves: 31702) Web Exploitation - Solved

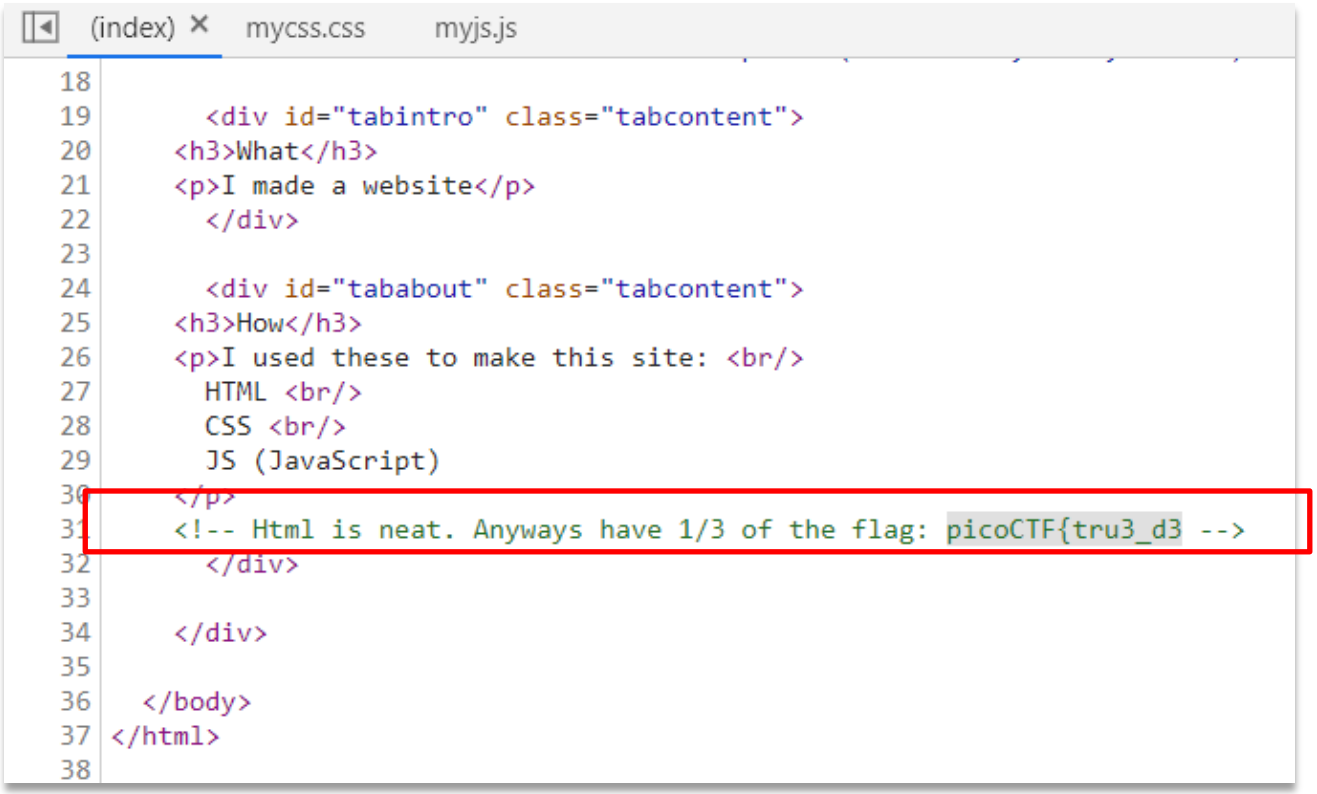
Solve Hints

Kishor Balan tipped us off that the following code may need inspection: `https://2019shell1.picoctf.com/problem/28717/` (link) or http://2019shell1.picoctf.com:28717

Submit! picoCTF{FLAG}



개발자 도구 여는 법: F12


(index)
mycss.css
myjs.js
18
19
20 <h3>What</h3>
21 I made a website
22
23
24
25 <h3>How</h3>
26 I used these to make this site:
27 HTML
28 CSS
29 JS (JavaScript)
30
31 <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
32
33
34
35
36 </body>
37 </html>
38

(index) mycss.css myjs.js ×

```
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?2717d7be} */
```

(index) mycss.css × myjs.js

```
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 */
```

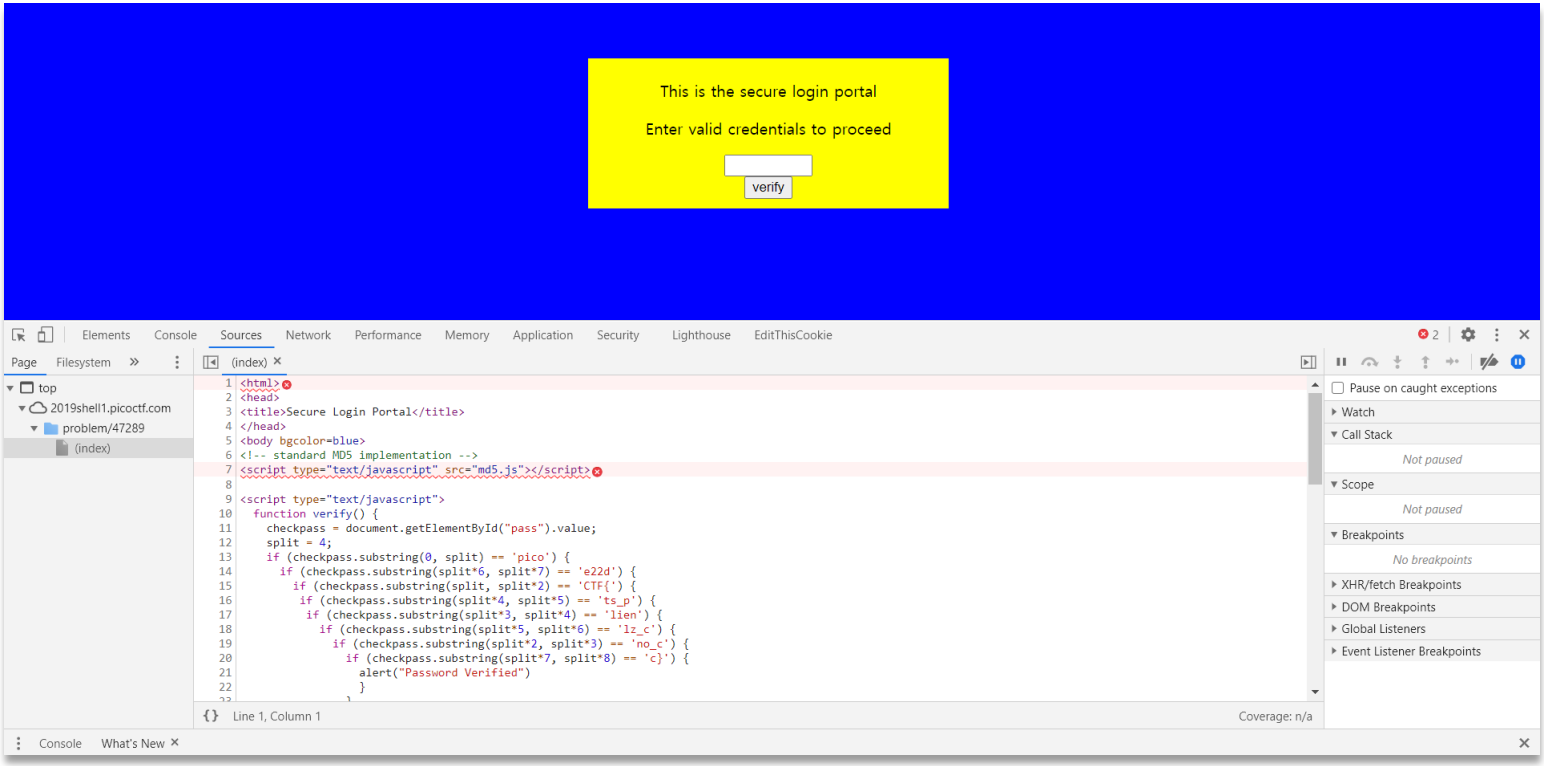
picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2717d7be}

dont-use-client-side - Points: 100 - (Solves: 25278) Web Exploitation - Solved

Solve Hints

Can you break into this super secure portal? `https://2019shell1.picoctf.com/problem/47289/` (link) or http://2019shell1.picoctf.com:47289

Submit! picoCTF{FLAG}


This is the secure login portal
Enter valid credentials to proceed
verify
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
EditThisCookie
Page
Filesystem
(index)
top
2019shell1.picoctf.com
problem/47289
(index)
<html>
<head>
<title>Secure Login Portal</title>
</head>
<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) == 'e22d') {
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_c') {
if (checkpass.substring(split*2, split*3) == 'no_c') {
if (checkpass.substring(split*7, split*8) == 'c}') {
alert("Password Verified")
}
Line 1, Column 1
Coverage: n/a
Pause on caught exceptions
Watch
Call Stack
Not paused
Scope
Not paused
Breakpoints
No breakpoints
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
Console
What's New

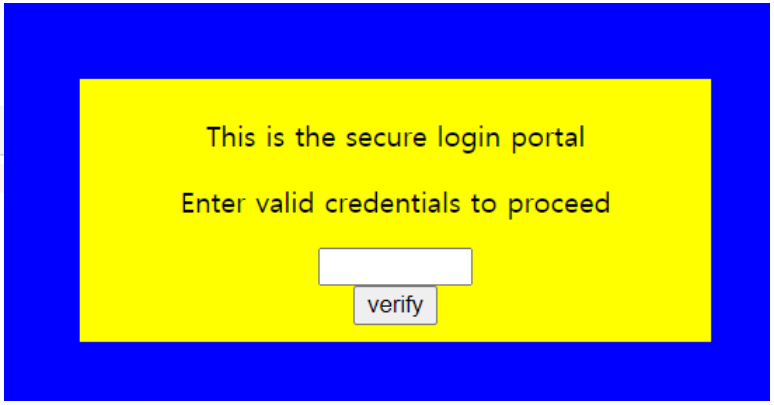
(index) ×

```
<html>
<head>
<title>Secure Login Portal</title>
</head>
<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) == 'e22d') {
        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_c') {
                if (checkpass.substring(split*2, split*3) == 'no_c') {
                  if (checkpass.substring(split*7, split*8) == 'c}') {
                    alert("Password Verified")
                    }
                  }
                }

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

```

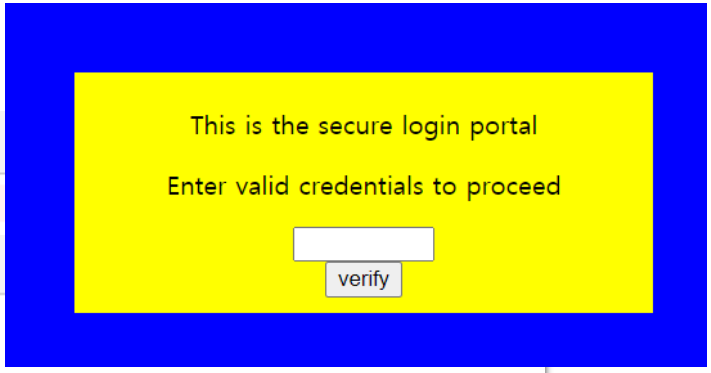


(index)

```
1  <html>
2  <head>
3  <title>Secure Login Portal</title>
4  </head>
5  <body bgcolor=blue>
6  <!-- standard MD5 implementation -->
7  <script type="text/javascript" src="md5.js"></script>
8
9  <script type="text/javascript">
10   function verify() {
11     checkpass = document.getElementById("pass").value;
12     split = 4;
13     if (checkpas
14       if (checkp
15         if (chec
16           if (che
17             if (ch
18               if (
19                 if
20
21
22
23
24                 }
25
26               }
27             }
28           }
29         }
30     }
31     else {
32       alert("Incorrect password");
33     }
34
```

(index)

```
40 <p>Enter valid credentials to proceed</p>
41 <form action="index.html" method="post">
42 <input type="password" id="pass" size="8" />
43 <br/>
44 <input type="submit" value="verify" onclick="verify(); return false;" />
45 </form>
46 </div>
47 </div>
48 </body>
49 </html>
50
```



(index)

```
1  <html>
```

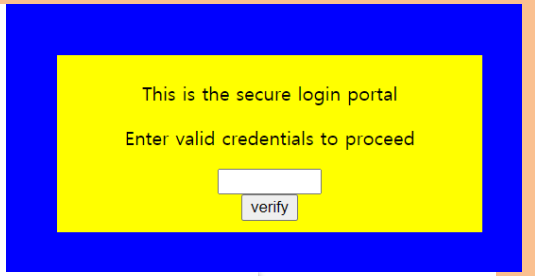
(index)

```
40 <p>Enter valid credentials to proceed</p>
41 <form action="index.html" method="post">
42 <input type="password" id="pass" size="8" />
43 <br/>
```

```
8
9  <script type="text/javascript">
10   function verify() {
11     checkpass = document.getElementById("pass").value;
12     split = 4;
13     if (checkpass.substring(0, split) == 'pico') {
14       if (checkpass.substring(split*6, split*7) == 'e22d') {
15         if (checkpass.substring(split, split*2) == 'CTF{') {
16          if (checkpass.substring(split*4, split*5) == 'ts_p') {
17           if (checkpass.substring(split*3, split*4) == 'lien') {
18             if (checkpass.substring(split*5, split*6) == 'lz_c') {
19               if (checkpass.substring(split*2, split*3) == 'no_c') {
20                 if (checkpass.substring(split*7, split*8) == 'c}') {
21                   alert("Password Verified")
22                   }
```

입력값

Substring(시작 인덱스, 종료 인덱스)
: 시작 인덱스부터 종료 인덱스 전까지 문자열을 자른다.

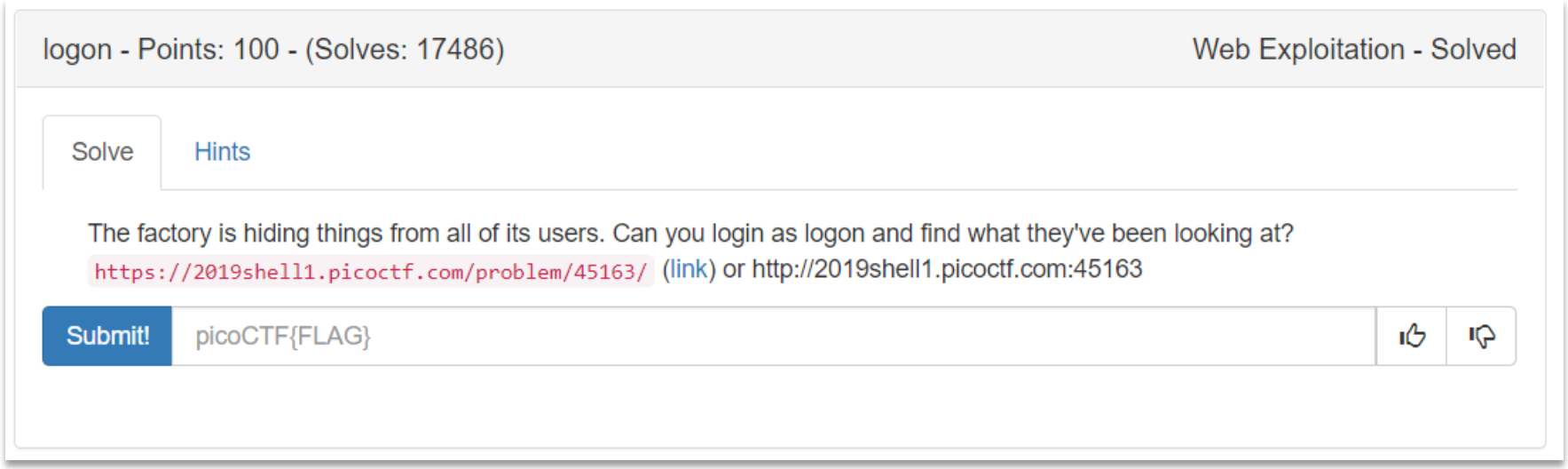


Substring(시작 인덱스, 종료 인덱스)
: 시작 인덱스부터 종료 인덱스 전까지 문자열을 자른다.

```
<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) == 'e22d') {
        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_c') {
                if (checkpass.substring(split*2, split*3) == 'no_c') {
                  if (checkpass.substring(split*7, split*8) == 'c}') {
                    alert("Password Verified")
                    }
```

입력값

pico
CTF{
no_c
lien
ts_p
lz_c
e22d
c}

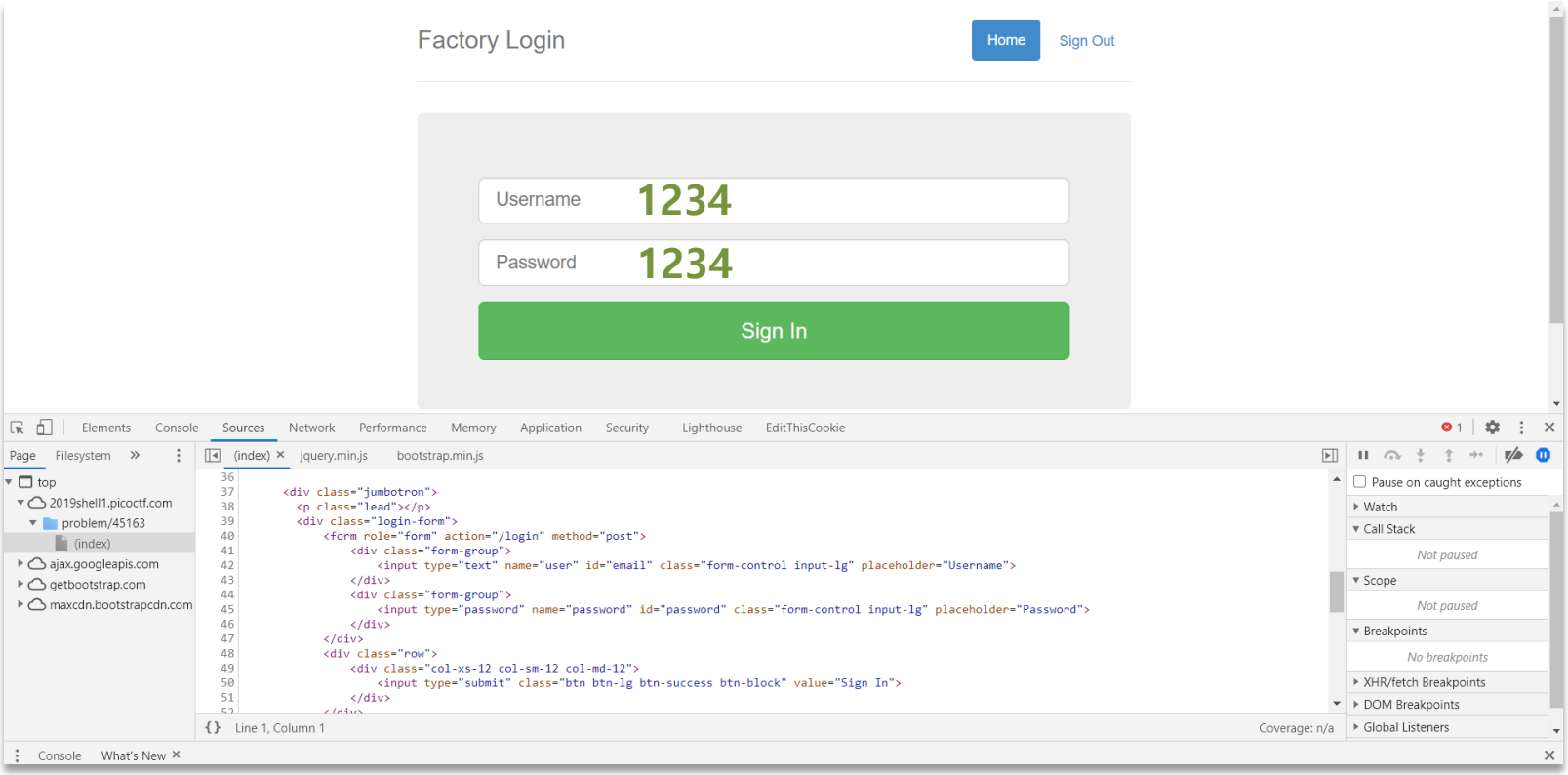


logon - Points: 100 - (Solves: 17486) Web Exploitation - Solved

Solve Hints

The factory is hiding things from all of its users. Can you login as logon and find what they've been looking at?
`https://2019shell1.picoctf.com/problem/45163/` (link) or http://2019shell1.picoctf.com:45163

Submit! picoCTF{FLAG}


Factory Login
Home
Sign Out
Username
1234
Password
1234
Sign In
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
EditThisCookie
Page
Filesystem
(index)
jquery.min.js
bootstrap.min.js
top
2019shell1.picoctf.com
problem/45163
(index)
ajax.googleapis.com
getbootstrap.com
maxcdn.bootstrapcdn.com

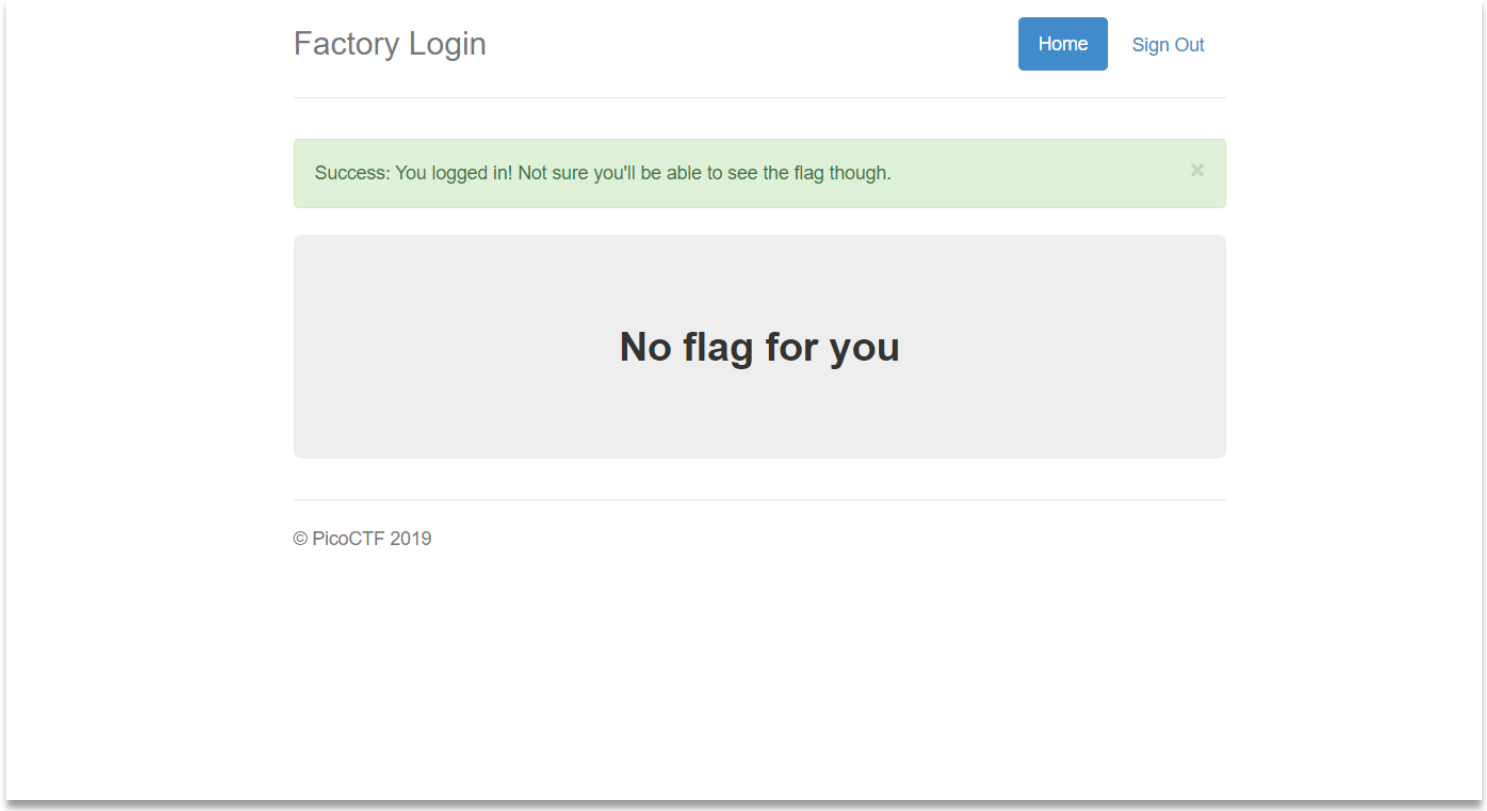
<form role="form" action="/login" method="post">

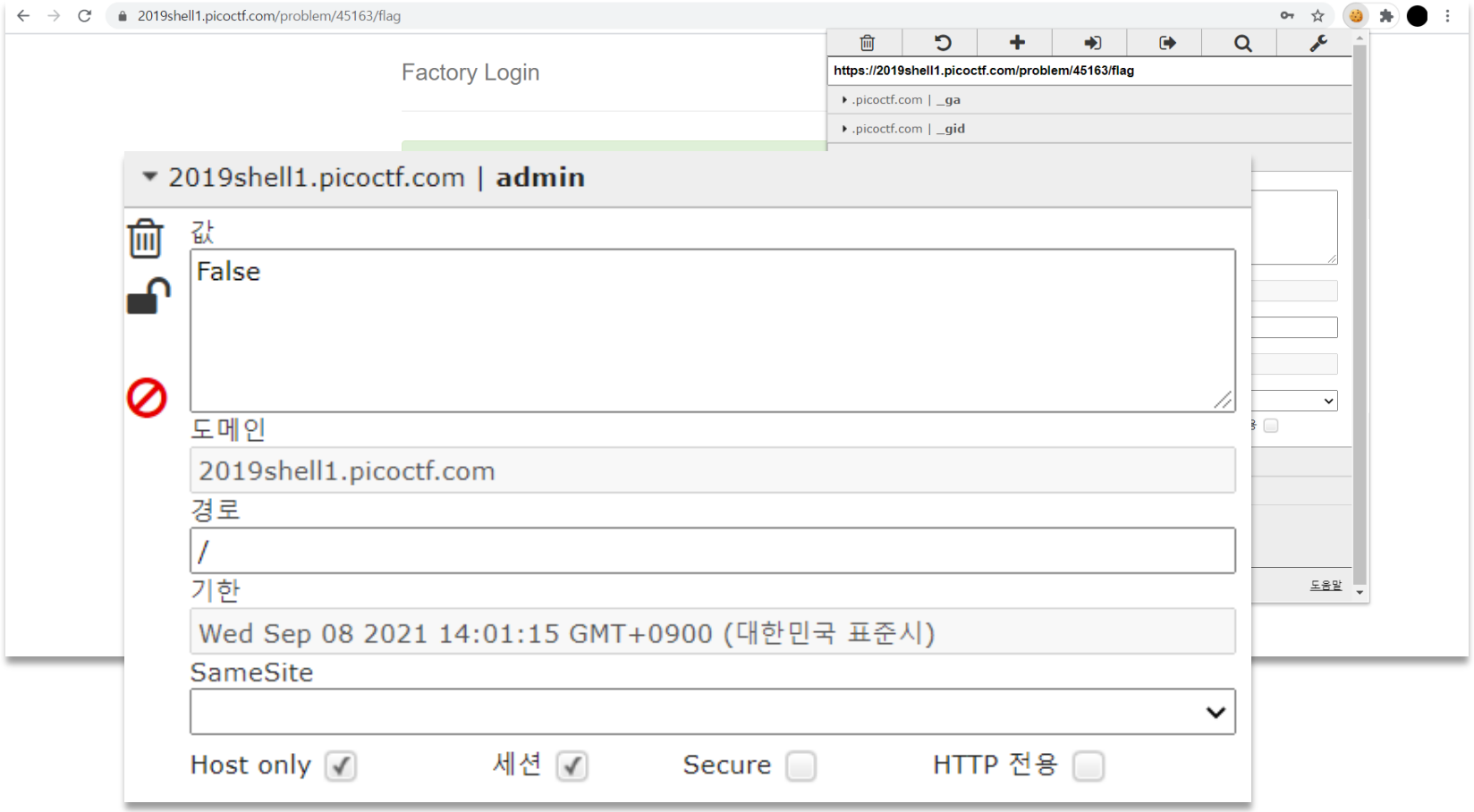
<input type="text" name="user" id="email" class="form-control input-lg" placeholder="Username">

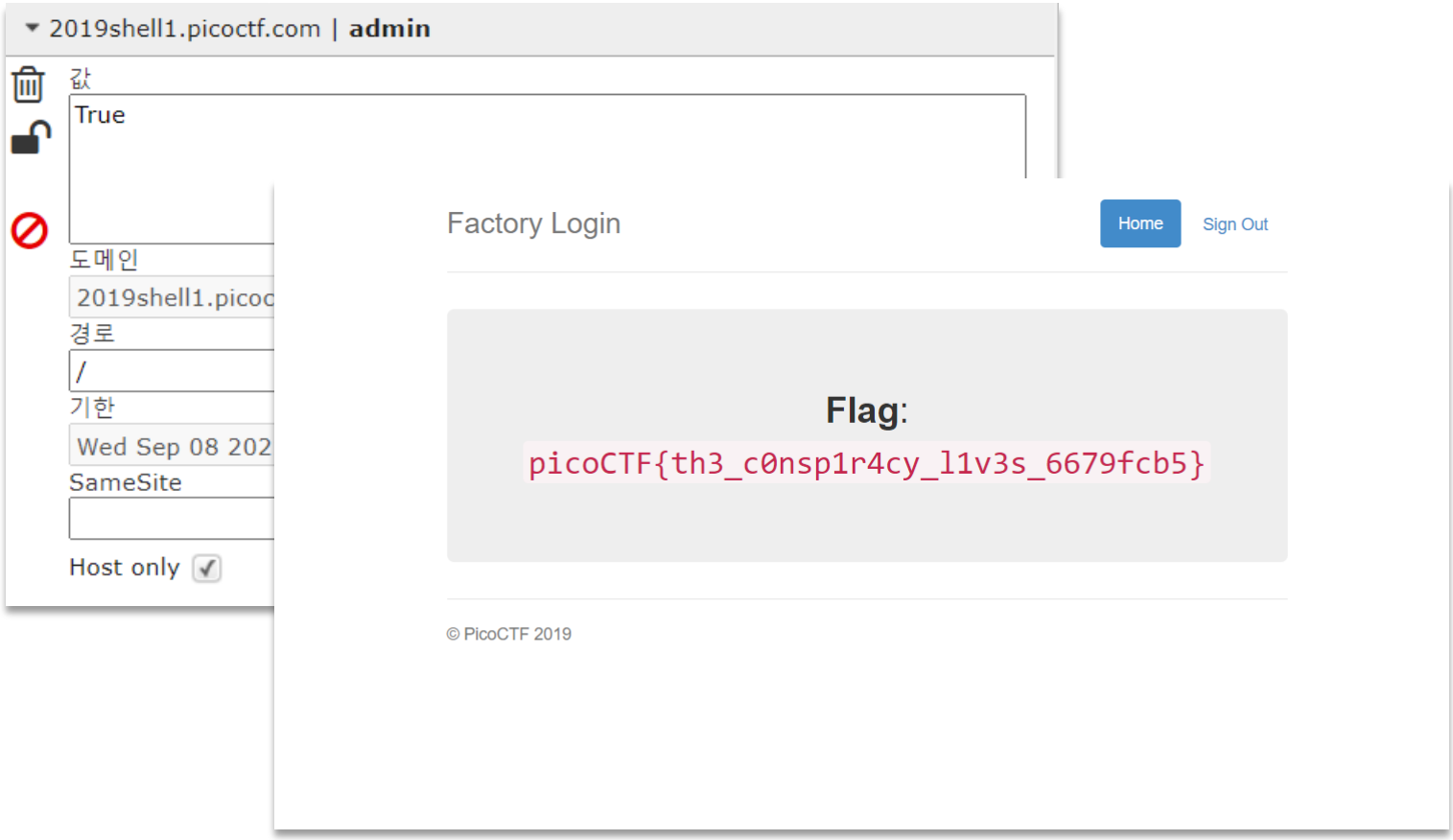
<input type="password" name="password" id="password" class="form-control input-lg" placeholder="Password">

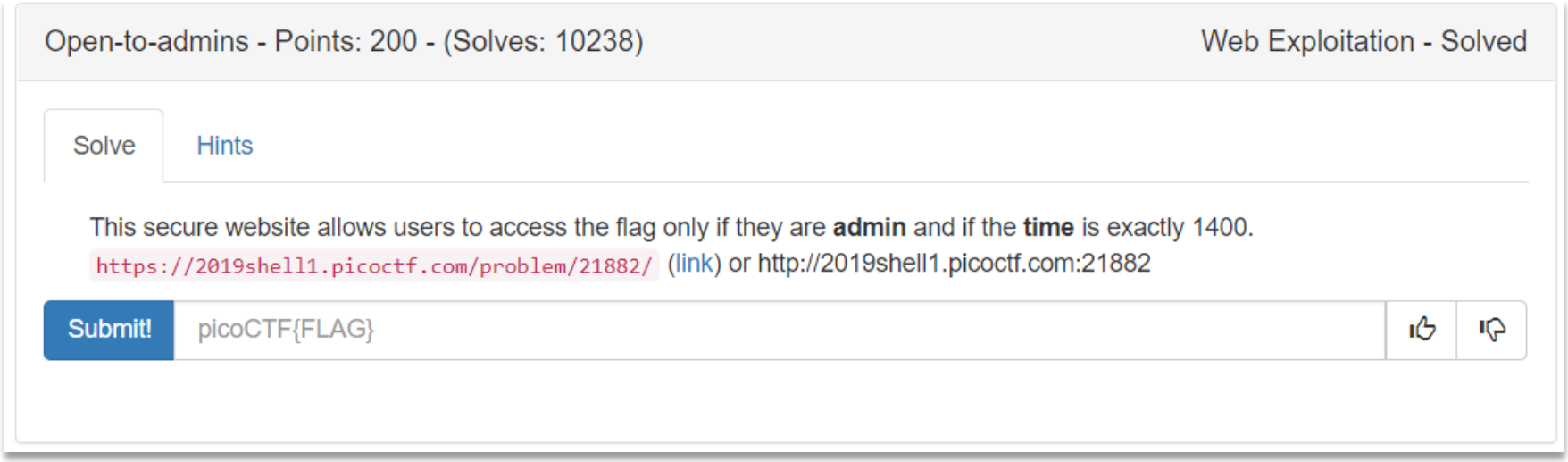
<input type="submit" class="btn btn-lg btn-success btn-block" value="Sign In">

Line 1, Column 1
Coverage: n/a
Pause on caught exceptions
Watch
Call Stack
Not paused
Scope
Not paused
Breakpoints
No breakpoints
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Console
What's New


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


2019shell1.picoctf.com/problem/45163/flag
Factory Login
https://2019shell1.picoctf.com/problem/45163/flag
.picoctf.com | _ga
.picoctf.com | _gid
2019shell1.picoctf.com | admin
값
False
도메인
2019shell1.picoctf.com
경로
/
기한
Wed Sep 08 2021 14:01:15 GMT+0900 (대한민국 표준시)
SameSite
Host only
세션
Secure
HTTP 전용


2019shell1.picoctf.com | admin
값
True
도메인
2019shell1.picoc
경로
/
기한
Wed Sep 08 202
SameSite
Host only
Factory Login
Home
Sign Out
Flag:
picoCTF{th3_c0nsp1r4cy_l1v3s_6679fcb5}
© PicoCTF 2019

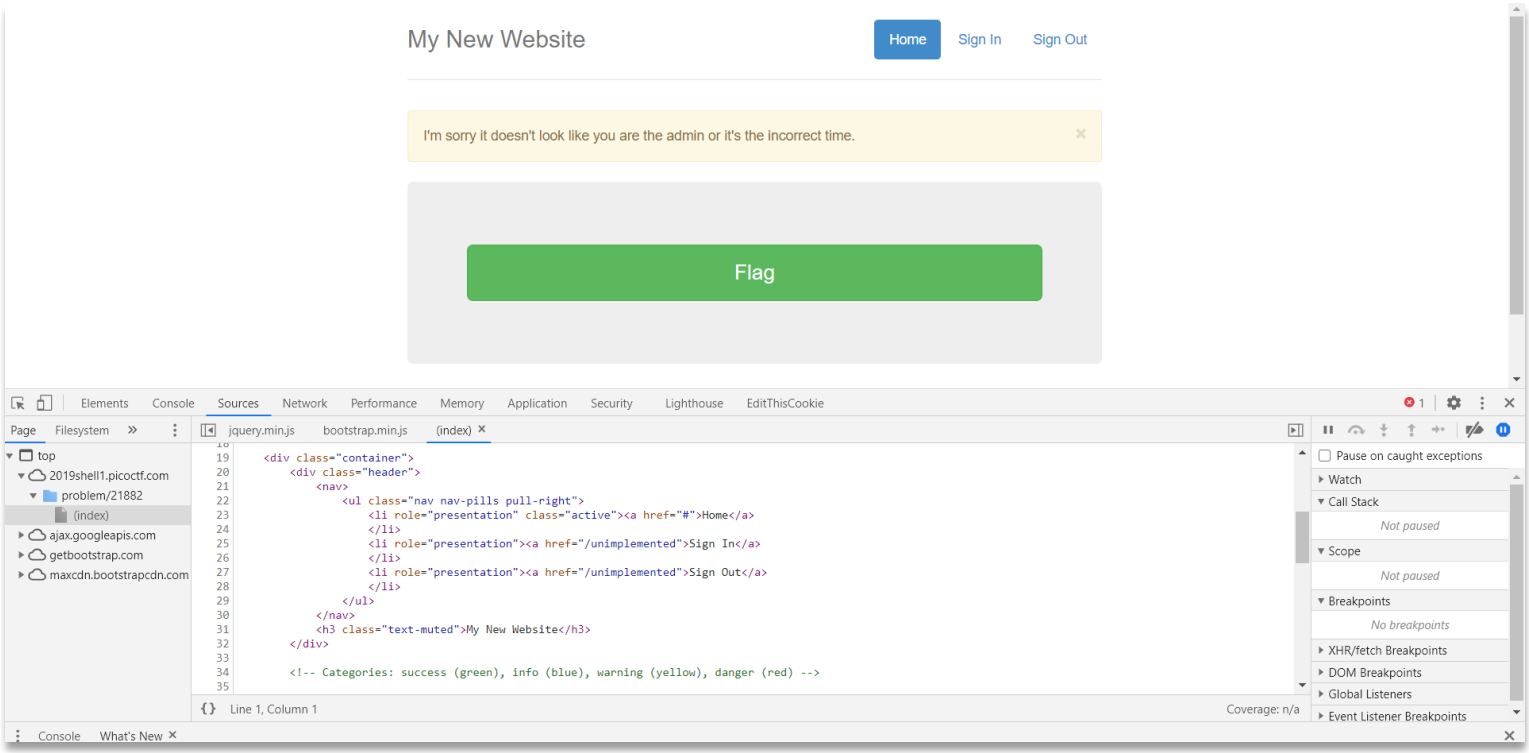


Open-to-admins - Points: 200 - (Solves: 10238) Web Exploitation - Solved

Solve Hints

This secure website allows users to access the flag only if they are **admin** and if the **time** is exactly 1400.
`https://2019shell1.picoctf.com/problem/21882/` (link) or http://2019shell1.picoctf.com:21882

Submit! picoCTF{FLAG}


My New Website
Home
Sign In
Sign Out
I'm sorry it doesn't look like you are the admin or it's the incorrect time.
Flag
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
EditThisCookie
Page
Filesystem
jquery.min.js
bootstrap.min.js
(index)
top
2019shell1.picoctf.com
problem/21882
(index)
ajax.googleapis.com
getbootstrap.com
maxcdn.bootstrapcdn.com

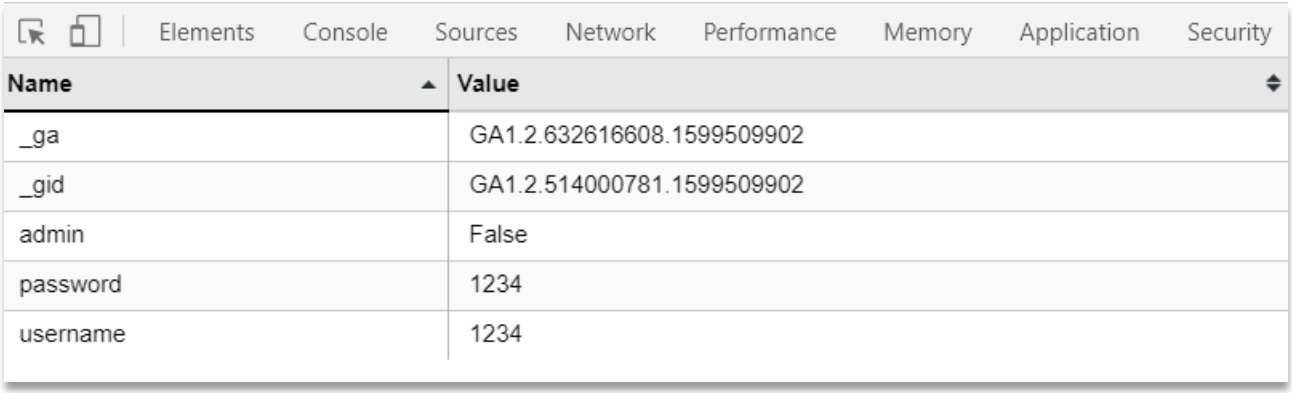
<nav>
<ul class="nav nav-pills pull-right">
<li role="presentation" class="active">Home

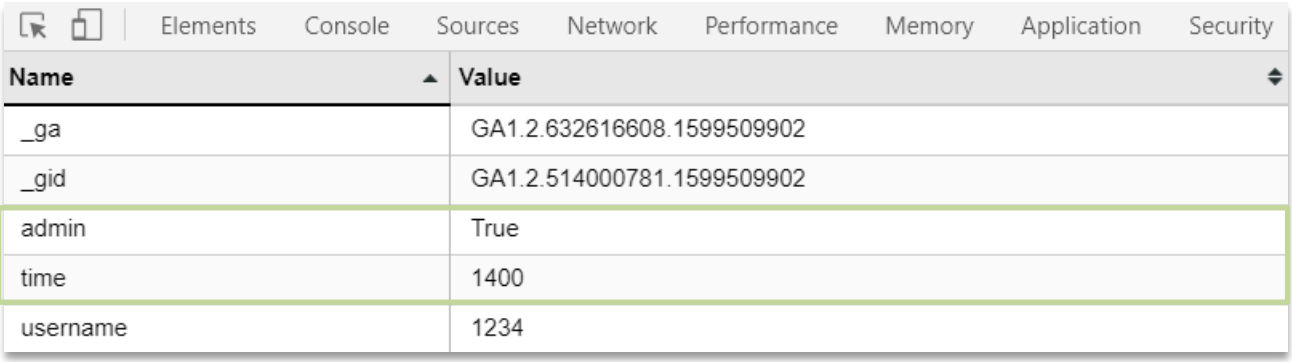
<li role="presentation">Sign In

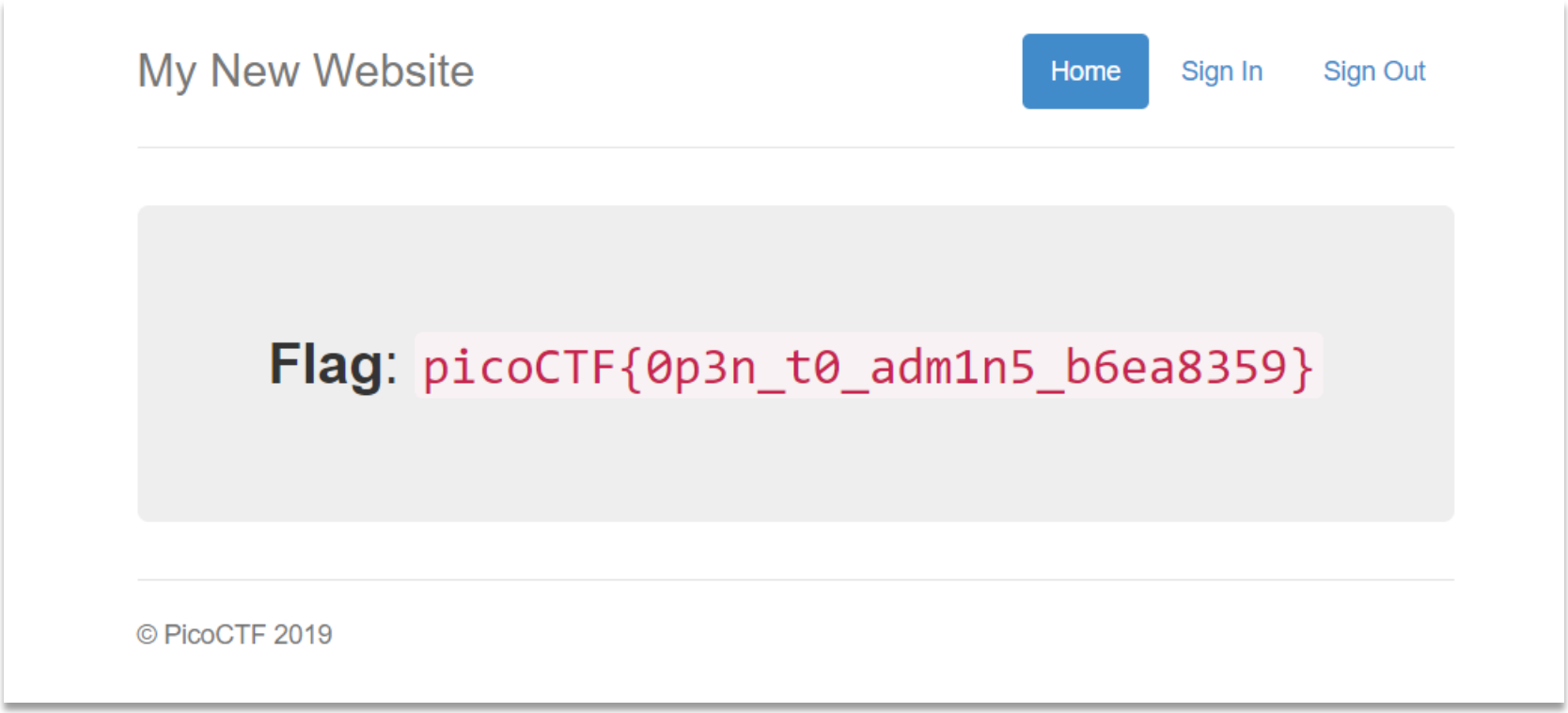
<li role="presentation">Sign Out

</nav>
<h3 class="text-muted">My New Website</h3>

<!-- Categories: success (green), info (blue), warning (yellow), danger (red) -->
Line 1, Column 1
Coverage: n/a
Pause on caught exceptions
Watch
Call Stack
Not paused
Scope
Not paused
Breakpoints
No breakpoints
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
Console
What's New


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Name
Value
_ga
GA1.2.632616608.1599509902
_gid
GA1.2.514000781.1599509902
admin
False
password
1234
username
1234


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Name
Value
_ga
GA1.2.632616608.1599509902
_gid
GA1.2.514000781.1599509902
admin
True
time
1400
username
1234

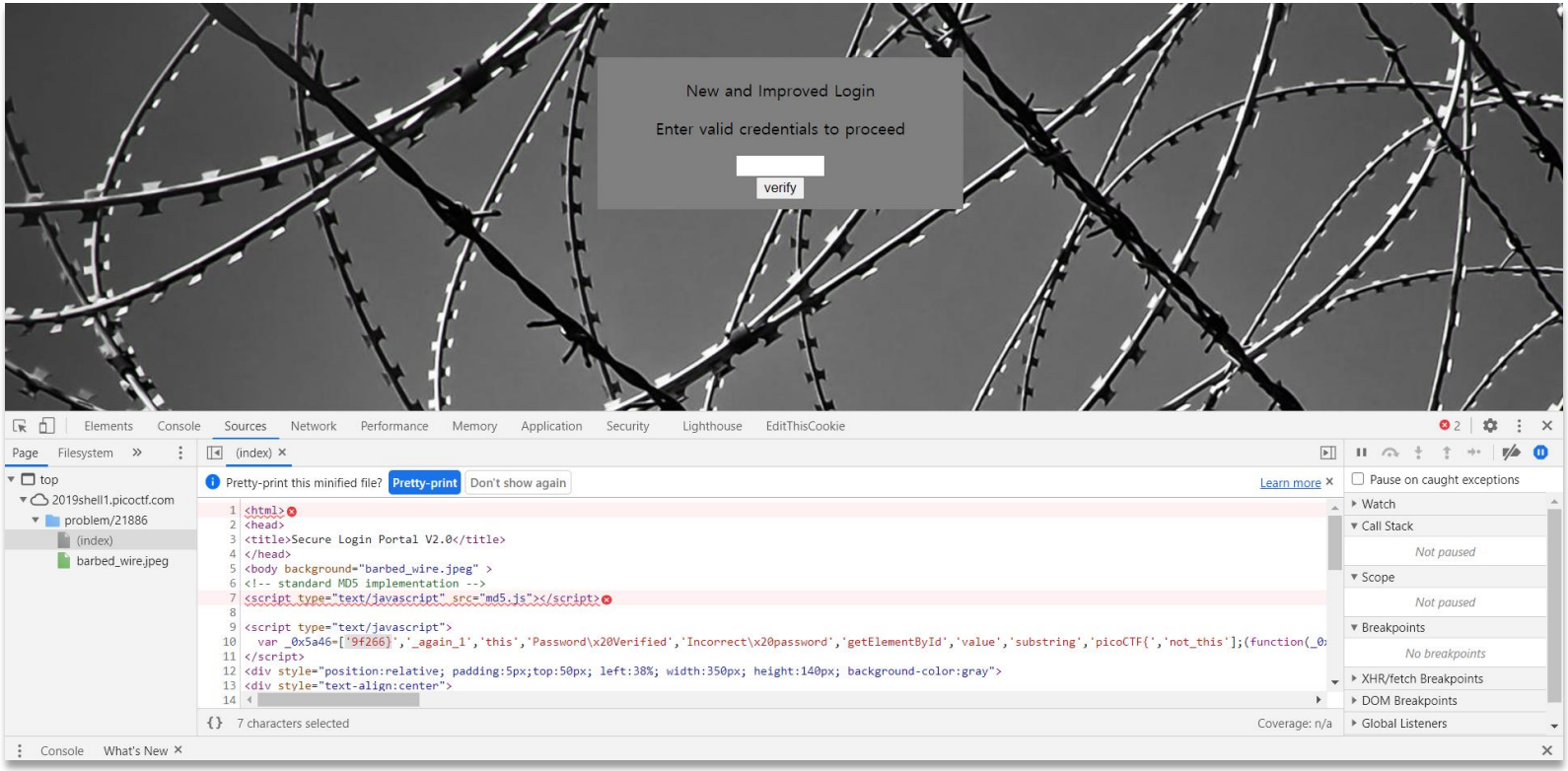

My New Website
Home
Sign In
Sign Out
Flag: picoCTF{0p3n_t0_adm1n5_b6ea8359}
© PicoCTF 2019

Client-side-again - Points: 200 - (Solves: 13213) Web Exploitation - Solved

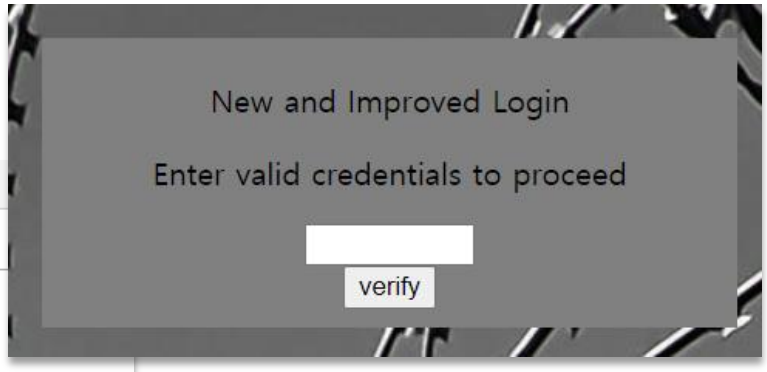
Solve Hints

Can you break into this super secure portal? `https://2019shell1.picoctf.com/problem/21886/` (link) or http://2019shell1.picoctf.com:21886

Submit! picoCTF{FLAG}


New and Improved Login
Enter valid credentials to proceed
verify
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
EditThisCookie
Page
Filesystem
top
2019shell1.picoctf.com
problem/21886
(index)
barbed_wire.jpeg
Pretty-print this minified file?
Pretty-print
Don't show again
Learn more
<html>
<head>
<title>Secure Login Portal V2.0</title>
</head>
<body background="barbed_wire.jpeg" >
<!-- standard MD5 implementation -->
<script type="text/javascript" src="md5.js"></script>
<script type="text/javascript">
var _0x5a46=['9f266}','_again_1','this','Password\x20Verified','Incorrect\x20password','getElementById','value','substring','picoCTF{','not_this'];(function(_0
</script>

7 characters selected
Coverage: n/a
Pause on caught exceptions
Watch
Call Stack
Not paused
Scope
Not paused
Breakpoints
No breakpoints
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Console
What's New



(index) ×

Pretty-print this minified file? Pretty-print Don't show again

```
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>
```

(index) ×

Pretty-print this minified file? Pretty-print Don't show again

```
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=['9f266}','_again_1','this','Password\x20Verified','Incorrect\x20password','getElementById','value','substring','picoCTF{','not_this'];(
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
```

{} 7 characters selected

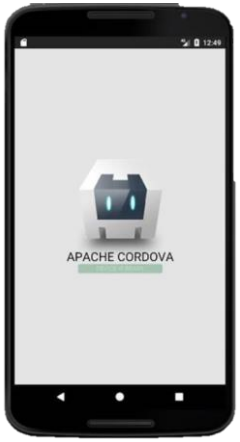
(index) :formatted ×

```
<script type="text/javascript">
    var _0x5a46 = ['9f266}', '_again_1', 'this', 'Password\x20Verified', 'Incorrect\x20password', 'getElementById', 'value', 'substring', 'picoCTF{', 'not_this'];
    (function(_0x4bd822, _0x2bd6f7) {
        var _0xb4bdb3 = function(_0x1d68f6) {
            while (--_0x1d68f6) {
                _0x4bd822['push'](_0x4bd822['shift']());
            }
        };
        _0xb4bdb3(++_0x2bd6f7);
    }(_0x5a46, 0x1b3));
    var _0x4b5b = function(_0x2d8f05, _0x4b81bb) {
        _0x2d8f05 = _0x2d8f05 - 0x0;
        var _0x4d74cb = _0x5a46[_0x2d8f05];
        return _0x4d74cb;
    };
    function verify() {
        checkpass = document[_0x4b5b('0x0')]('pass')[_0x4b5b('0x1')];
        split = 0x4;
        if (checkpass[_0x4b5b('0x2')](0x0, split * 0x2) == _0x4b5b('0x3')) {
            if (checkpass[_0x4b5b('0x2')](0x7, 0x9) == '{n') {
                if (checkpass[_0x4b5b('0x2')](split * 0x2, split * 0x2 * 0x2) == _0x4b5b('0x4')) {
                    if (checkpass[_0x4b5b('0x2')](0x3, 0x6) == 'oCT') {
                        if (checkpass[_0x4b5b('0x2')](split * 0x3 * 0x2, split * 0x4 * 0x2) == _0x4b5b('0x5')) {
                            if (checkpass['substring'](0x6, 0xb) == 'F{not') {
                                if (checkpass[_0x4b5b('0x2')](split * 0x2 * 0x2, split * 0x3 * 0x2) == _0x4b5b('0x6')) {
                                    if (checkpass[_0x4b5b('0x2')](0xc, 0x10) == _0x4b5b('0x7')) {
                                        alert(_0x4b5b('0x8'));
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
```

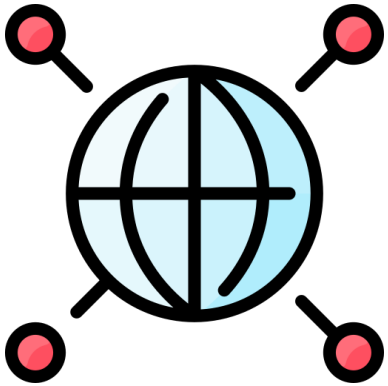
Line 9, Column 28 Coverage: n/a

개발자 도구란?

Debugging



Emulator



Network analysis

...

Console

스크립트 명령어를 입력하는 패널로,

break를 건 시점의 변수를 확인할 수 있고

값을 평가하거나 수정할 수 있다.

```
function verify() {
    checkpass = document[_0x4b5b('0x0')]('pass')[_0x4b5b('0x1')];
    split = 0x4;
    if (checkpass[_0x4b5b('0x2')](0x0, split * 0x2) == _0x4b5b('0x3')) {
        if (checkpass[_0x4b5b('0x2')](0x7, 0x9) == '{n') {
            if (checkpass[_0x4b5b('0x2')](split * 0x2, split * 0x2 * 0x2) == _0x4b5b('0x4')) {
                if (checkpass[_0x4b5b('0x2')](0x3, 0x6) == 'oCT') {
                    if (checkpass[_0x4b5b('0x2')](split * 0x3 * 0x2, split * 0x4 * 0x2) == _0x4b5b('0x5')) {
                        if (checkpass['substring'](0x6, 0xb) == 'F{not') {
                            if (checkpass[_0x4b5b('0x2')](split * 0x2 * 0x2, split * 0x3 * 0x2) == _0x4b5b('0x6')) {
```

```
function verify(){
    checkpass=document['getElementById']('pass')['value'];
    split=0x4;
    if(checkpass['substring'](0x0,split*0x2)=='picoCTF{'){
        if(checkpass['substring'](0x7,0x9)=='{n'){
            if(checkpass['substring'](split*0x2,split*0x2*0x2)=='not_this'){
                if(checkpass['substring'](0x3,0x6)=='oCT'){
                    if(checkpass['substring'](split*0x3*0x2,split*0x4*0x2)=='9f266}'){
                        if(checkpass['substring'](0x6,0xb)=='F{not'){
                            if(checkpass['substring'](split*0x2*0x2,split*0x3*0x2)=='_again_1'){
                                if(checkpass['substring'](0xc,0x10)=='this'){
                                    alert('Password Verified');
                                }
                            }
                        }
                    }
                }
            }
        }
    }
    else{
        alert('Incorrect password');
    }
}
```

```
function verify(){
    checkpass=document['getElementById']('pass')['value'];
    split=0x4;
    if(checkpass['substring'](0x0,split*0x2)=='picoCTF{'){
        if(checkpass['substring'](0x7,0x9)=='{n'){
            if(checkpass['substring'](split*0x2,split*0x2*0x2)=='not_this'){
                if(checkpass['substring'](0x3,0x6)=='oCT'){
                    if(checkpass['substring'](split*0x3*0x2,split*0x4*0x2)=='9f266}'){
                        if(checkpass['substring'](0x6,0xb)=='F{not'){
                            if(checkpass['substring'](split*0x2*0x2,split*0x3*0x2)=='_again_1'){
                                if(checkpass['substring'](0xc,0x10)=='this'){
                                    alert('Password Verified');
                                }
                            }
                        }
                    }
                }
            }
        }
    }
    else{
        alert('Incorrect password');
    }
}
```

picoCTF{ not_this _again_19f266}

https://subicura.com/2018/02/14/javascript-debugging.html#%ED%81%AC%EB%A1%AC-%EA%B0%9C%EB%B0%9C%EC%9E%90-%EB%8F%84%EA%B5%AC-devtools

1. 소스코드만 보면 풀 수 있는 문제

2. 소스코드 이해와 감이 필요한 문제

THANK YOU

발 표 자 허 송 이