Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO CTF GIỮA KỲ

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: Thi CTF giữa kỳ

GVHD: Nguyễn Công Danh

Nhóm: G7

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O21.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Triệu Thiên Bảo	21520155	21520155@gm.uit.edu.vn
2	Nguyễn Thị Minh Châu	21520645	21520645@gm.uit.edu.vn
3	Nguyễn Phương Trinh	21521581	21521581@gm.uit.edu.vn
4	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	
2	Yêu cầu 2	0%	
3	Yêu cầu 3	100%	
4	Yêu cầu 4	100%	
5	Yêu cầu 5	0%	
Điểm tự đánh giá			

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

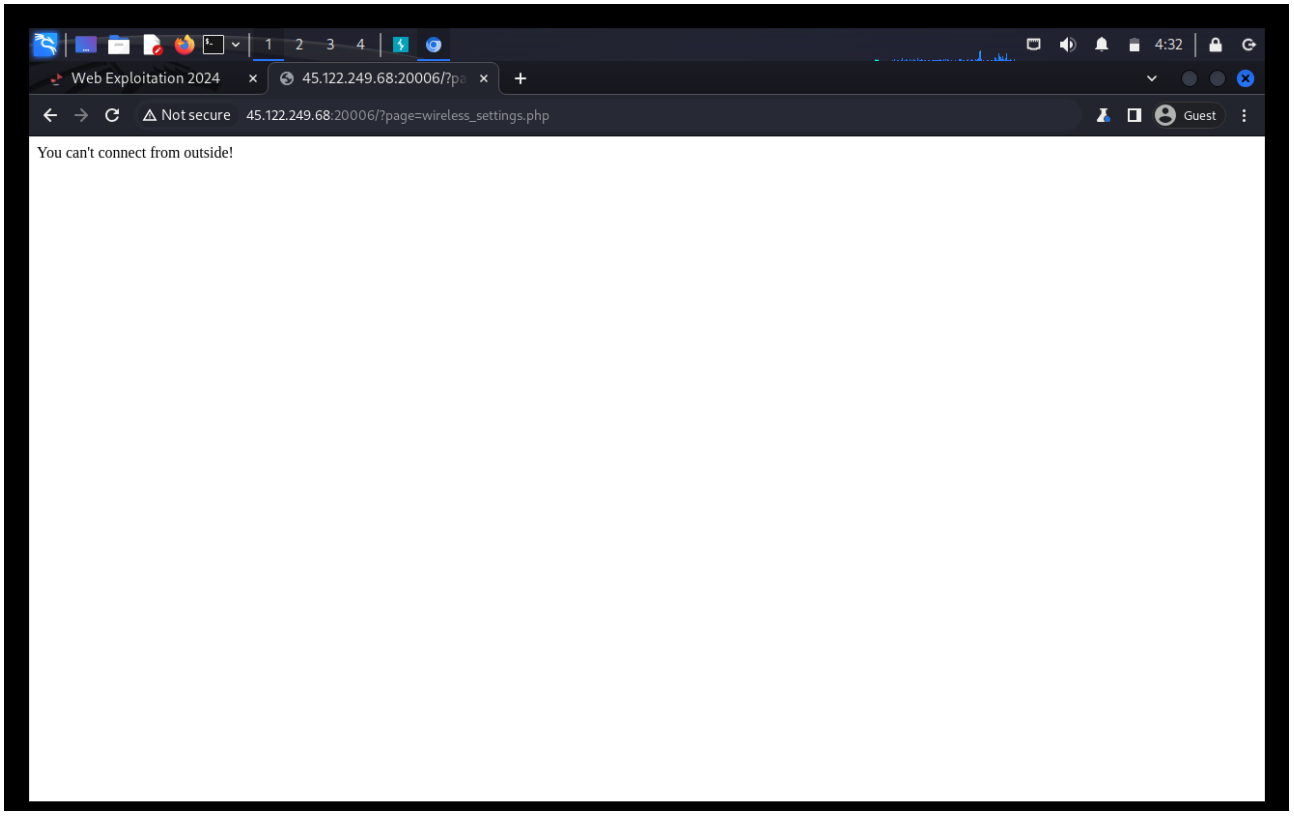
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Nhóm đặt tên là [NT213.O21.ANTT].G.[NOX]

ROUTER EMULATOR

Sau khi vào trang web thì nhóm thấy có 2 page bị khóa đó là wireless_settings và firewall nên có thể flag sẽ nằm trong này .

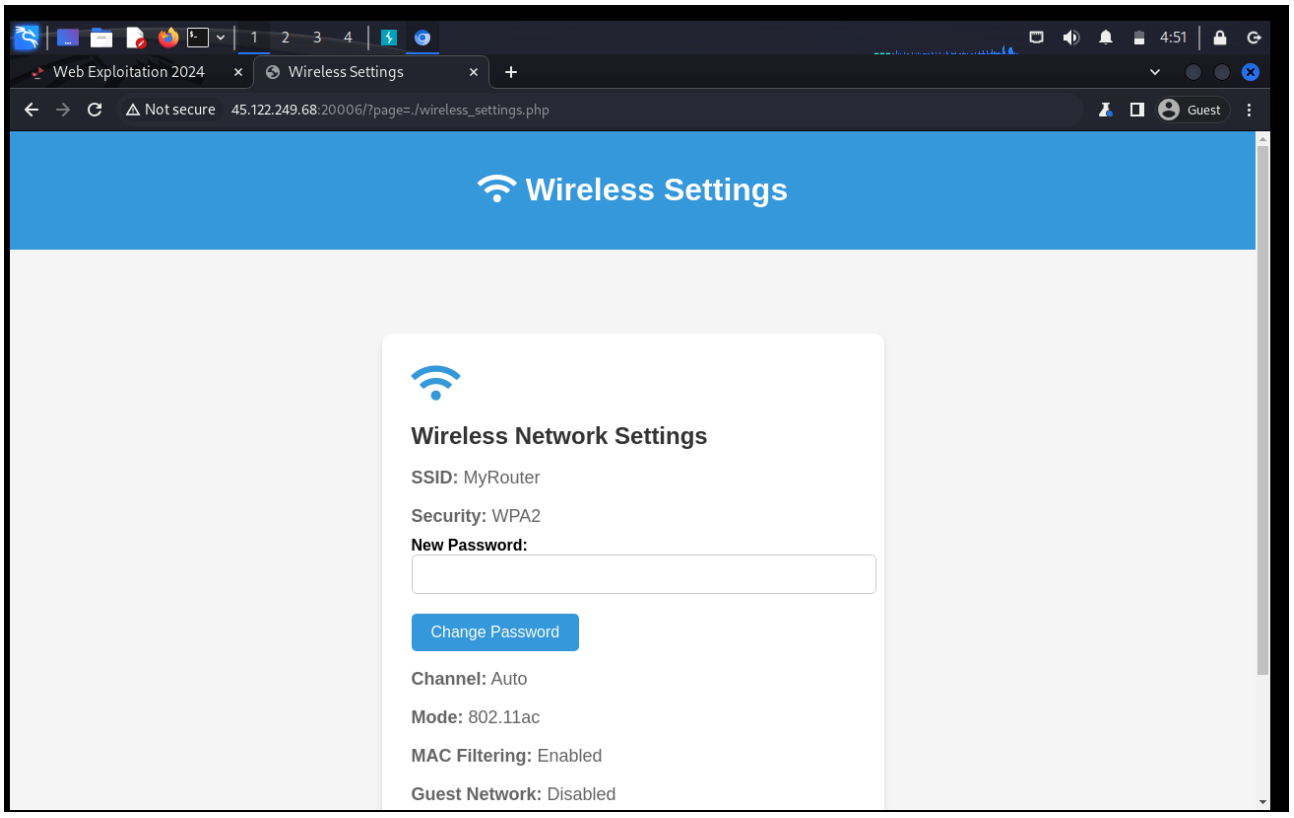


Nhìn qua source code của file wireless_settings.php thì thấy có đoạn code đổi mật khẩu, có lẽ sẽ có ích nên ta thử đổi theo vậy xem sao. Nhưng mà vấn đề hiện tại là page này đang bị khóa nên vẫn chưa truy cập vào được.

Thay vì truy cập như một trang web bình thường theo cú pháp:

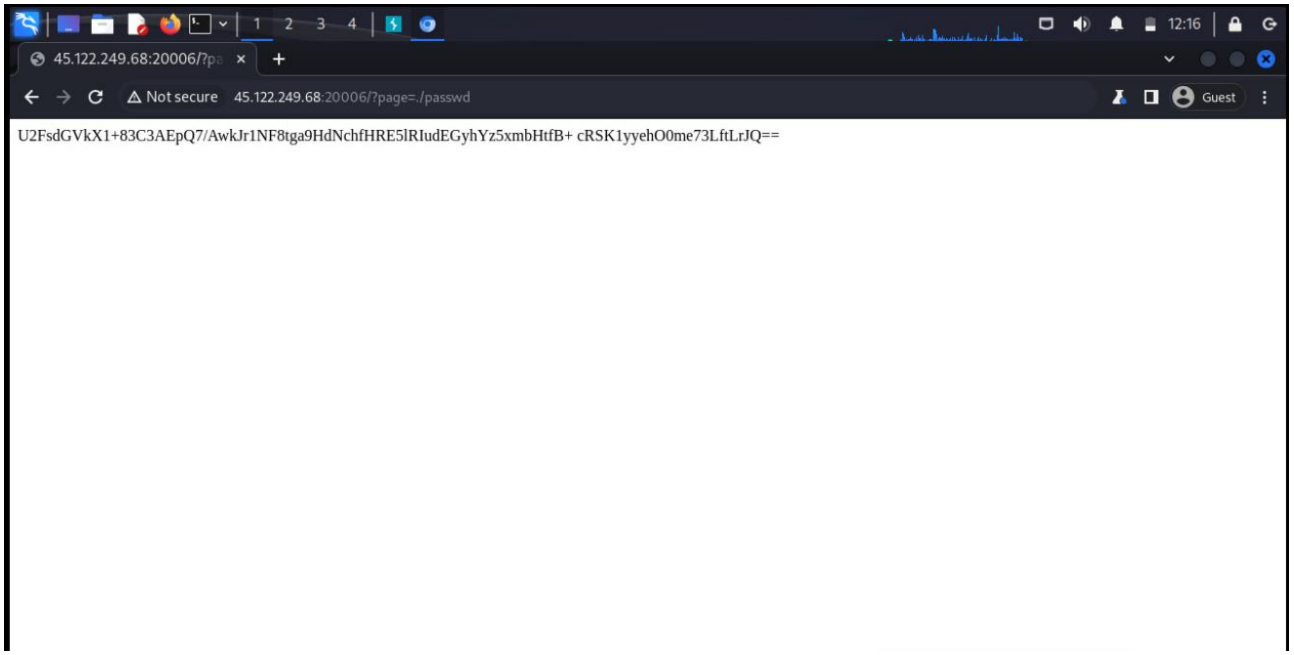
http://45.122.249.68:20006/?page=wireless_settings.php

Nhóm em thử thêm ./ vào trước wireless_settings.php để vào thư mục xem sao thì nó đã hoạt động.



Bây giờ thử đổi mật khẩu thành ‘password’ nhưng nó bị chặn vì url đổi về ban đầu rồi. Vì vậy nhóm thử dùng burpsuite để giúp ta truyền payload vào. Đổi mật khẩu xong ta

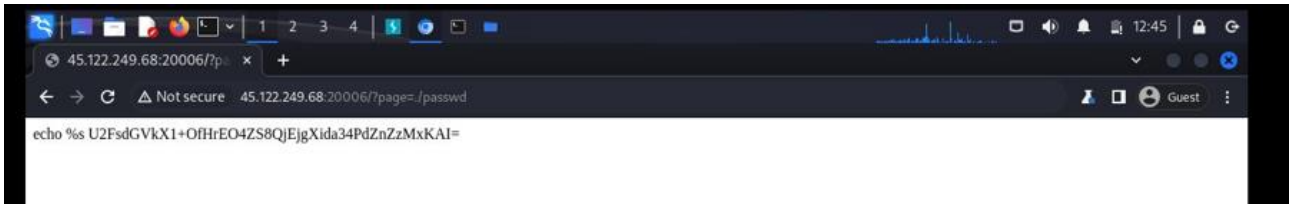
thử xem file ./passwd có gì, và không có gì ngoài mật khẩu đã được mã hóa. Không tìm thấy gì có thể dùng được nên nhóm quyết định đi tìm hướng đi mới.



Trong source code vẫn còn một file readflag.c đầy bí ẩn. Trong đây là đoạn code dùng để in flag ra màn hình, vì vậy việc cần làm là phải làm sao để có thể thực thi file này. Có thể thử injection command vào khung đổi mật khẩu

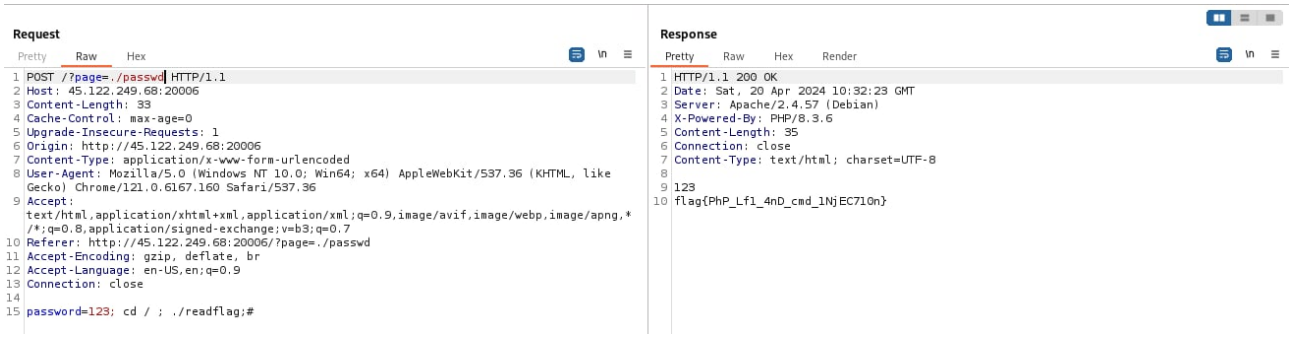
Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
src	File folder					4/7/2024 6:24 PM
compose	Yaml Source File	1 KB	No	1 KB	15%	4/7/2024 6:24 PM
Dockerfile	File	1 KB	No	1 KB	32%	4/7/2024 6:24 PM
flag	Text Document	1 KB	No	1 KB	0%	4/7/2024 6:24 PM
readflag	C Source File	1 KB	No	1 KB	20%	4/7/2024 6:24 PM
readflag	File	2 KB	No	15 KB	88%	4/7/2024 6:24 PM

Thử những câu lệnh mà nhóm tìm được ở trong đống source code nhưng không có kết quả gì.



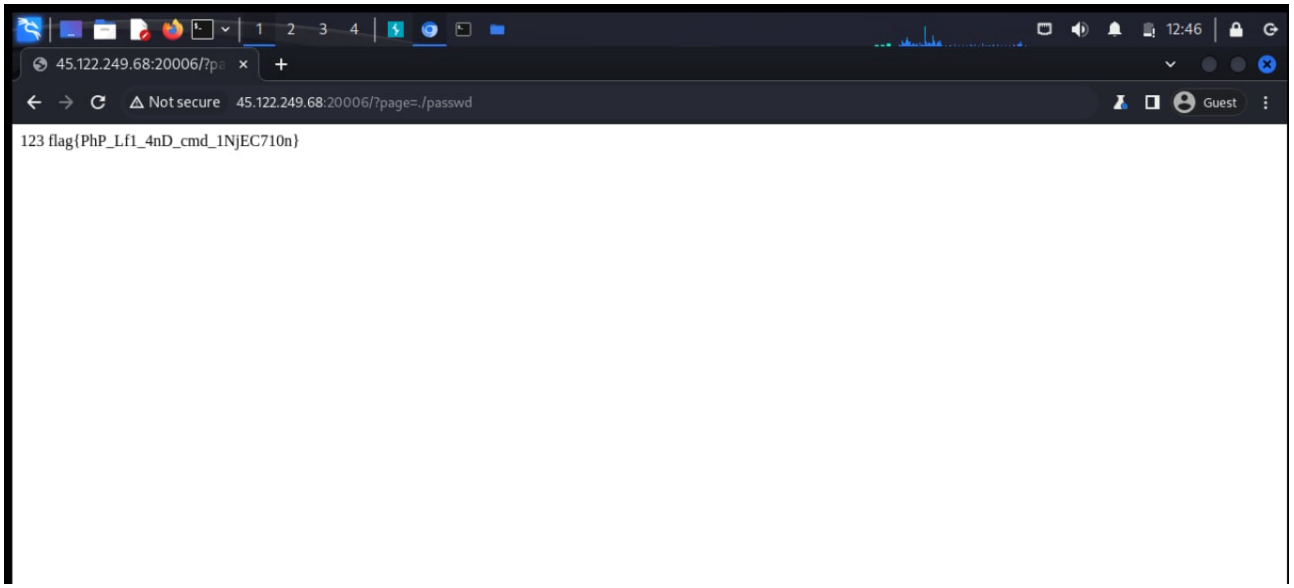
Sau khi thử các cách thì nhóm cũng tìm ra cách giải quyết đó là truyền câu lệnh cd vào trong file password và thực thi.

Payload mà nhóm truyền vào đó là *123; cd / ; ./readflag;#* dùng để cd vào thư mục hiện hành rồi thực thi file readflag.



Kết quả cuối cùng ta lấy được flag.

flag{PhP_Lf1_4nD_cmd_1NjEC710n}



SMART CONTRACT

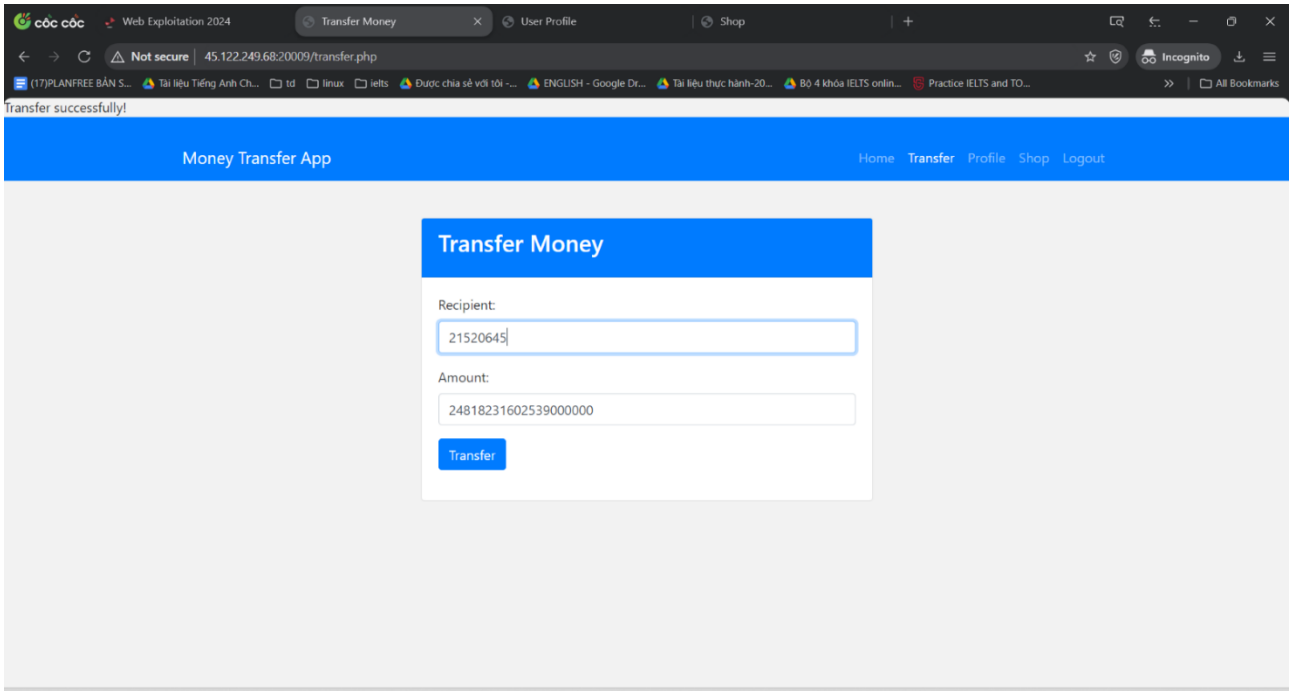
Ta mở file transfer.php để đọc và phân tích code

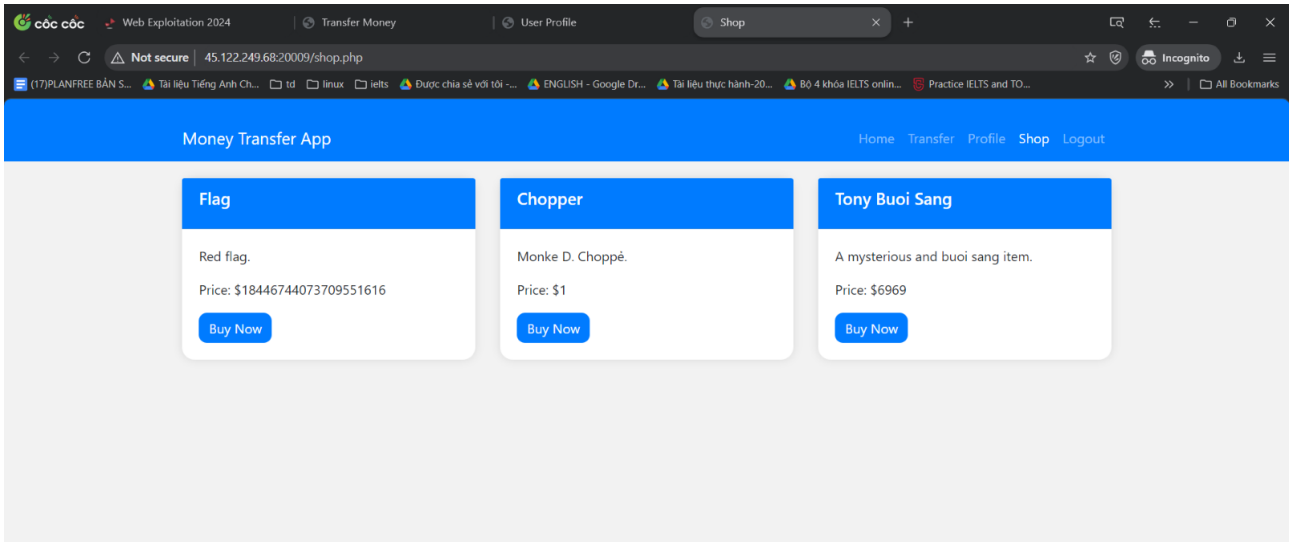
Ở đây ta thấy rằng trong hàm _update thì nó sẽ tiến hành chuyển tiền trước rồi mới update số dư sau cùng. Nghĩa là khi ta tự chuyển tiền từ tài khoản của bản thân tới chính nó thì nó sẽ chuyển trước rồi mới update số dư. Đây là một lỗ hổng vì ta sẽ có thể tự chuyển thêm tới tài khoản của bản thân mà không bị trừ số dư sau cùng. Lúc này tiền đã được chuyển vào tài khoản đích, sau đó nó update tài khoản nguồn với 1 khoản đã trừ đi số tiền đã chuyển. Nhưng tài khoản nguồn và đích là một nên nó đã được update số dư mới mà không bị trừ đi số dư ban đầu.

```
87  }
88
    1 reference
89  function _update($from, $to, $amount)
90  {
91      if (empty($from) || empty($to)) {
92          return;
93      }
94
95      _botCheck($from, $to);
96      $fromBalanceBeforeTransfer = _preCheck($from, $to, $amount);
97
98      $amountAfterTax = $amount - _taxApply($from, $to, $amount);
99      $toBalance = _postCheck($from, $to, $amountAfterTax);
100
101     _updateBalance($from, $fromBalanceBeforeTransfer - $amount);
102     _updateBalance($to, $toBalance);
103 }
```

Vì vậy việc cần làm đơn giản là tự chuyển tiền cho chính mình với số tiền được phép chuyển cho tới khi đủ số dư để mua flag.

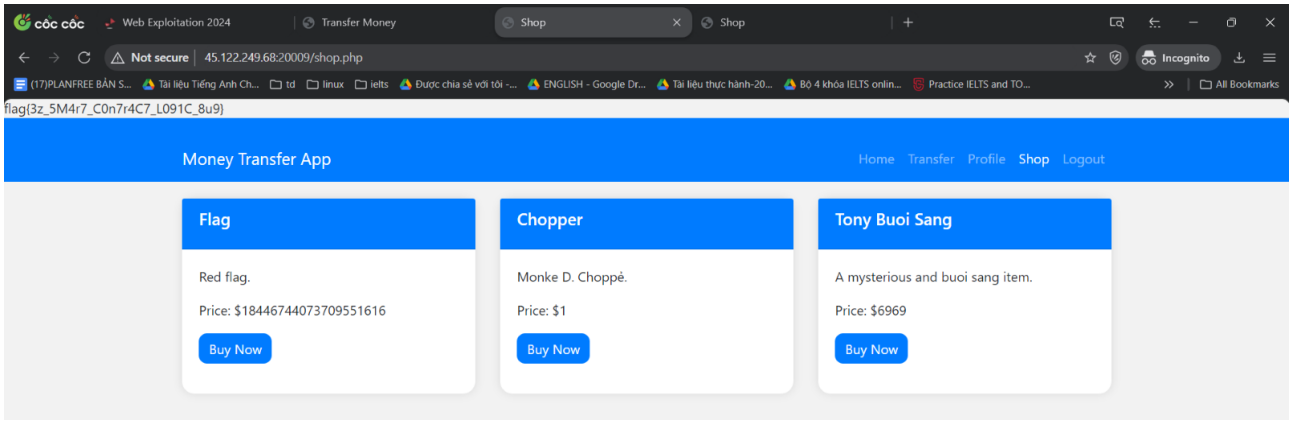
VD: số dư trong tài khoản là 1 đồng thì ta sẽ chuyển 1 đồng đó cho chính mình và khi đó tài khoản sẽ được update lên thành 2 đồng mà không bị trừ 1 đồng đã chuyển.





Sau một khoản thời gian ta đã có đủ tiền và mua được flag.

flag{3z_5M4r7_C0n7r4C7_L091C_8u9}



BOTCHECK AS A SERVICE

Sau khi tạo tài khoản đăng nhập vào web botcheck (username '123123'), nhóm quan sát thấy có 2 tab 'Home' và 'Flag'. Trong đó 'Home' có chứa 1 textbox để nhập URL với mục đích report lên botcheck; và 'Flag' thì có vẻ là sẽ chứa flag của bài nhưng hiện tại chưa lấy được (web hiện ra thông báo 'You are not premium user').

Vậy tổng quan lại thì tài khoản hiện tại của nhóm chỉ là 'normal', vì vậy cần thực hiện nâng cấp nó lên 'premium'.

Nhóm sẽ đi tìm đọc source code đã được cung cấp, sau đó chú ý đến folder manager chứa file index.php có phương thức POST cần chú ý là 'upgrade'. Ở đây có hàm để thực hiện query nhằm mục đích update cột 'premium' = 1 lên để tăng quyền cho user (truyền vào username của user đó).

give_to_player > manager > index.php > ...

```php
<?php

require_once "./db.php";

if (isset($_POST['username']) && isset($_POST['upgrade'])) {
    $username = $_POST['username'];
    if (!is_string($username) || empty($username)) {
        die("Invalid username!");
    }

    $result = $conn->execute_query("UPDATE users SET premium=1 WHERE username=?", [$username]);
    if (!$result) {
        die("Failed to upgrade user!");
    }

    if (!$conn->affected_rows) {
        die("User not found or already upgraded!");
    }

    echo "Upgrade successfully!";
}
```

Theo như gợi ý từ thầy Khoa là auto submit form và liên hệ với đề bài là input link URL để report lên botcheck. Nhóm nghĩ rằng cần tạo một website với chức năng upgrade premium cho user.

Theo đoạn code trên, để thực hiện upgrade user cần phải có trường username và phương thức POST. Do đó nhóm sẽ viết một website để POST username mà nhóm đã tạo lúc nãy là ''123123'' lên.

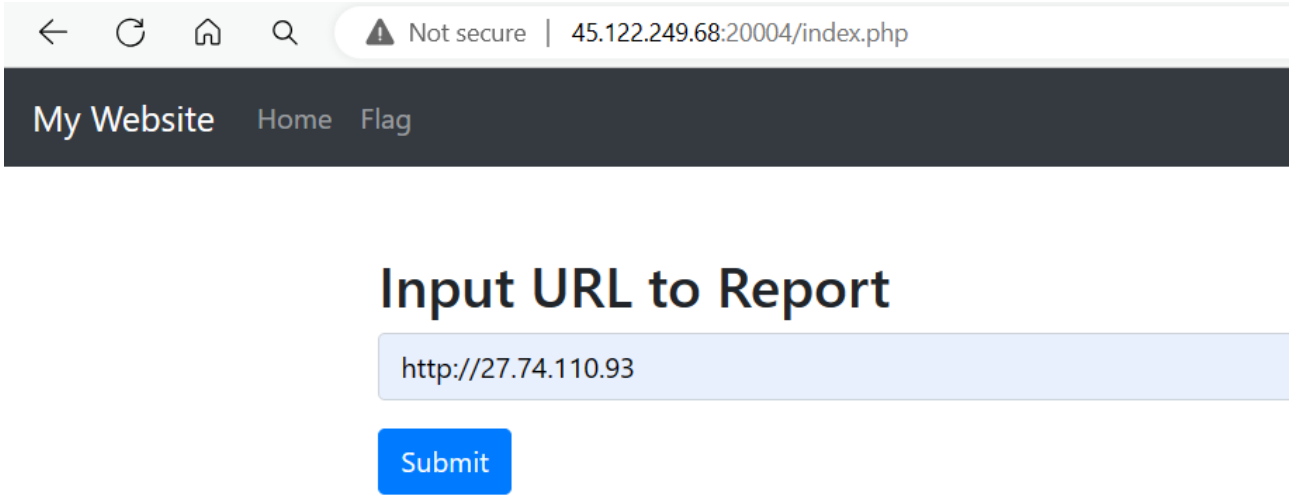
hi.html > body

```html
<body>
    <form id="upgradeForm" action="//manager" method="post">
        <input type="hidden" name="username" value="123123" />
        <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>
```

Sau đó tìm cách host public đoạn code kia lên (chú ý làm thành URL http). Nhóm tham khảo cách 1 ở link dưới (host qua router):

Chia sẻ local website (localhost) ra bên ngoài – Thao Tran (wordpress.com)

Website nhóm có được được đặt theo địa chỉ IP mà nhóm host ra bên ngoài. Dùng địa chỉ website này để thực thi việc upgrade user.



Sau khi user của nhóm được upgrade thành premium thì nhóm thu được flag.

flag{c5rf_45_4_53RV1C3}