BÁO CÁO BÀI TẬP

**Môn học: NT521.O12.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.O12.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 |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-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.**

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

A computer screen shot of a program code

Description automatically generated

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.

A computer screen with text on it

Description automatically generated

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.

A screen shot of a computer code

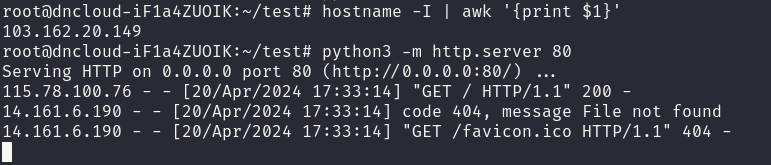
Description automatically generated

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

A black screen with white text

Description automatically generated

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



Và tiến hành gửi url thì thành công.

A screenshot of a computer

Description automatically generated

**Router Emulator**

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

A screenshot of a computer

Description automatically generated

A black background with colorful text

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

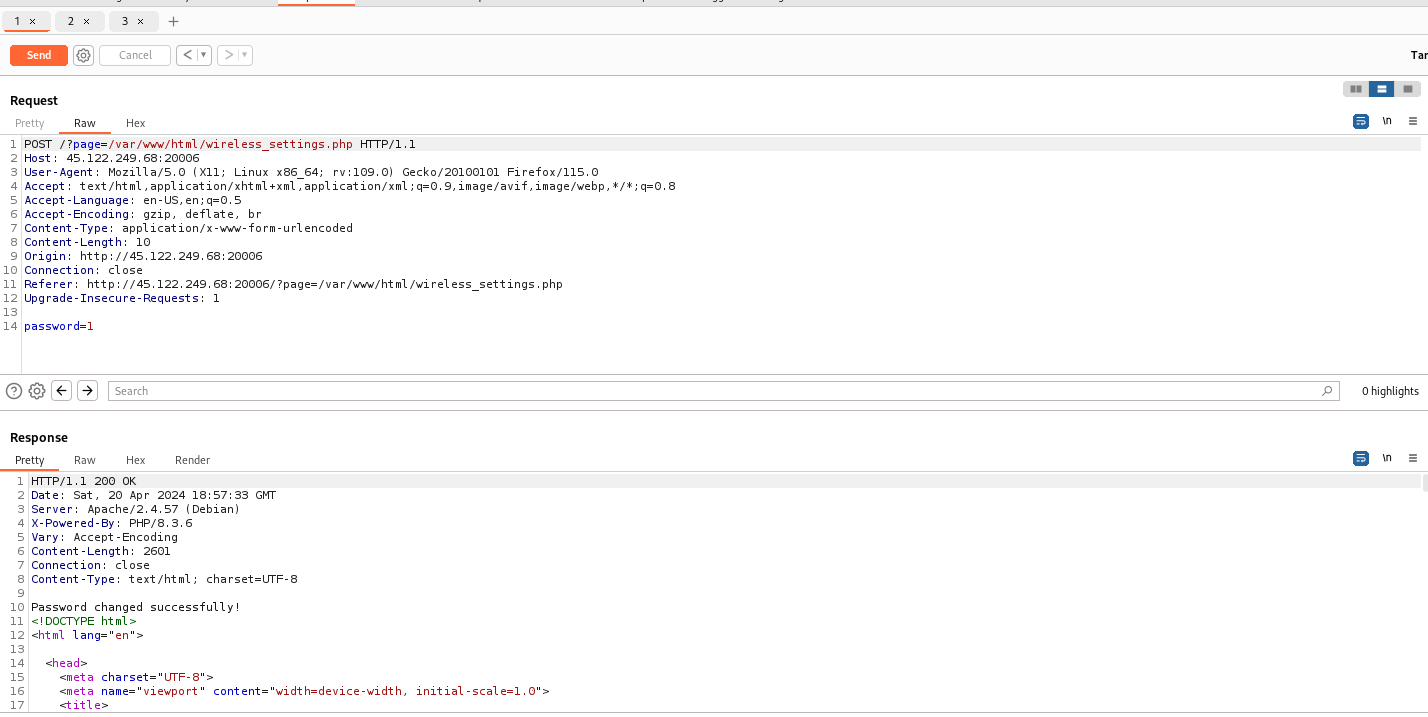
Description automatically generated

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

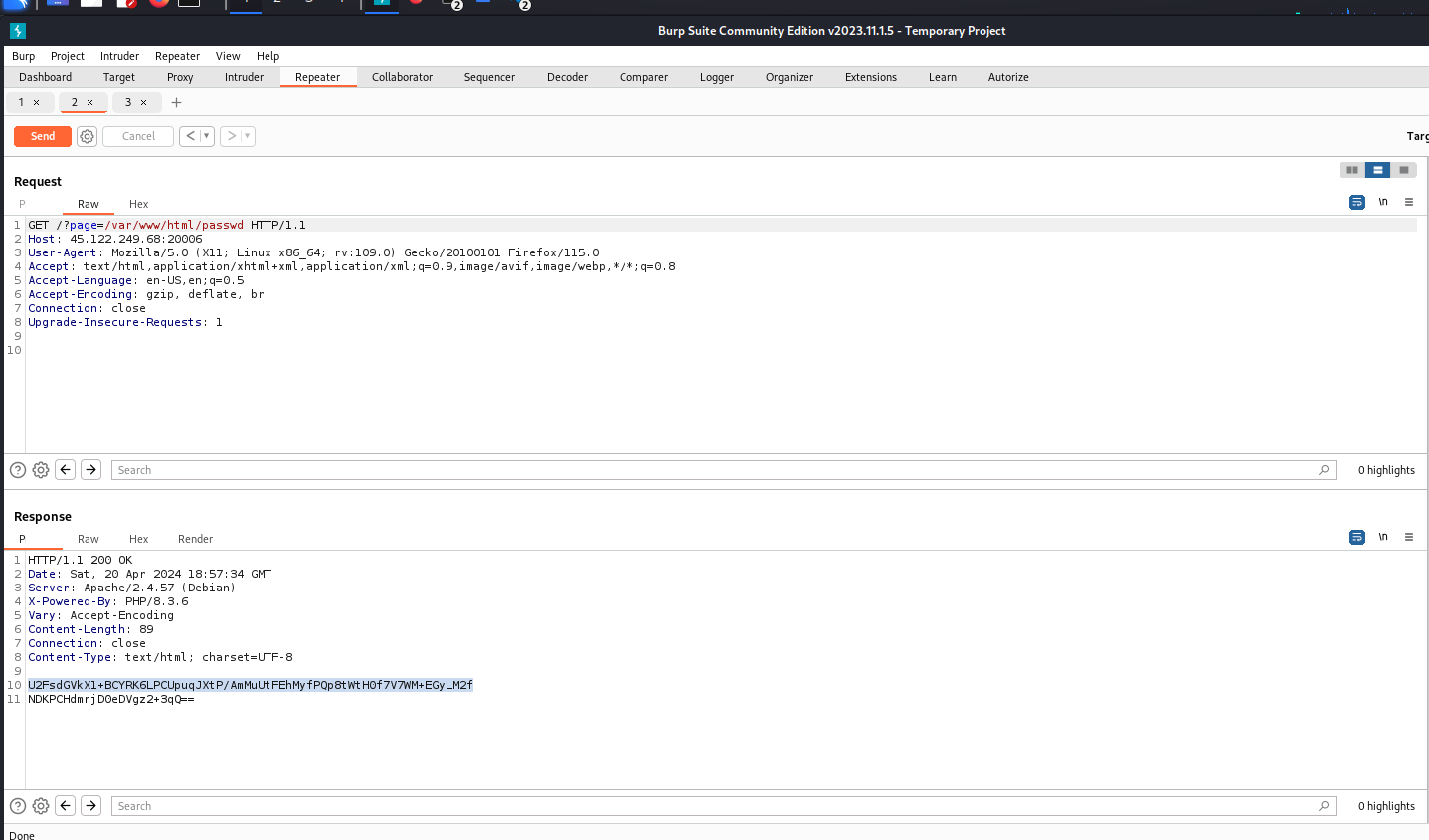
A computer screen shot of a program

Description automatically generated

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

A screen shot of a computer program

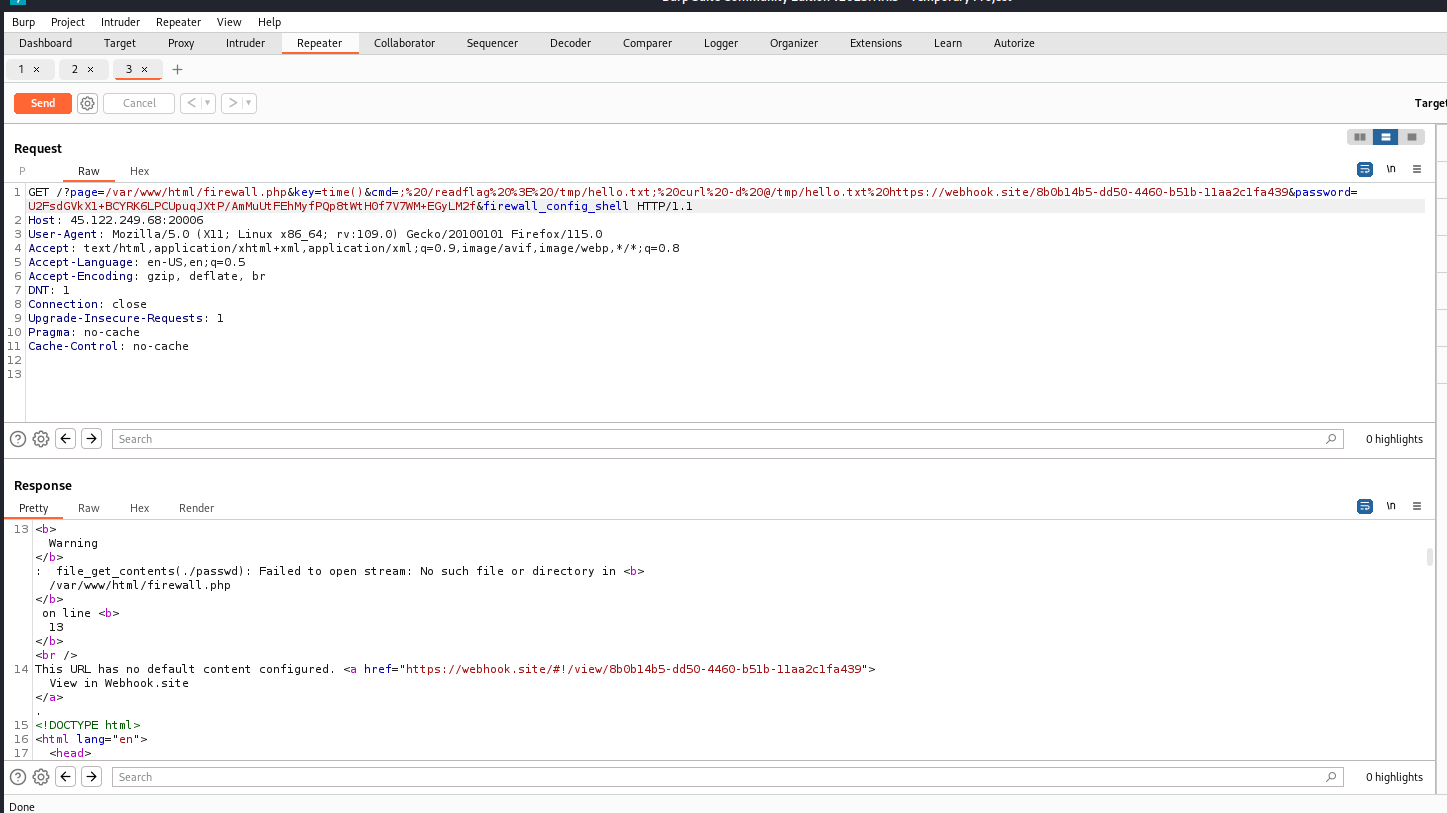
Description automatically generated

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!"

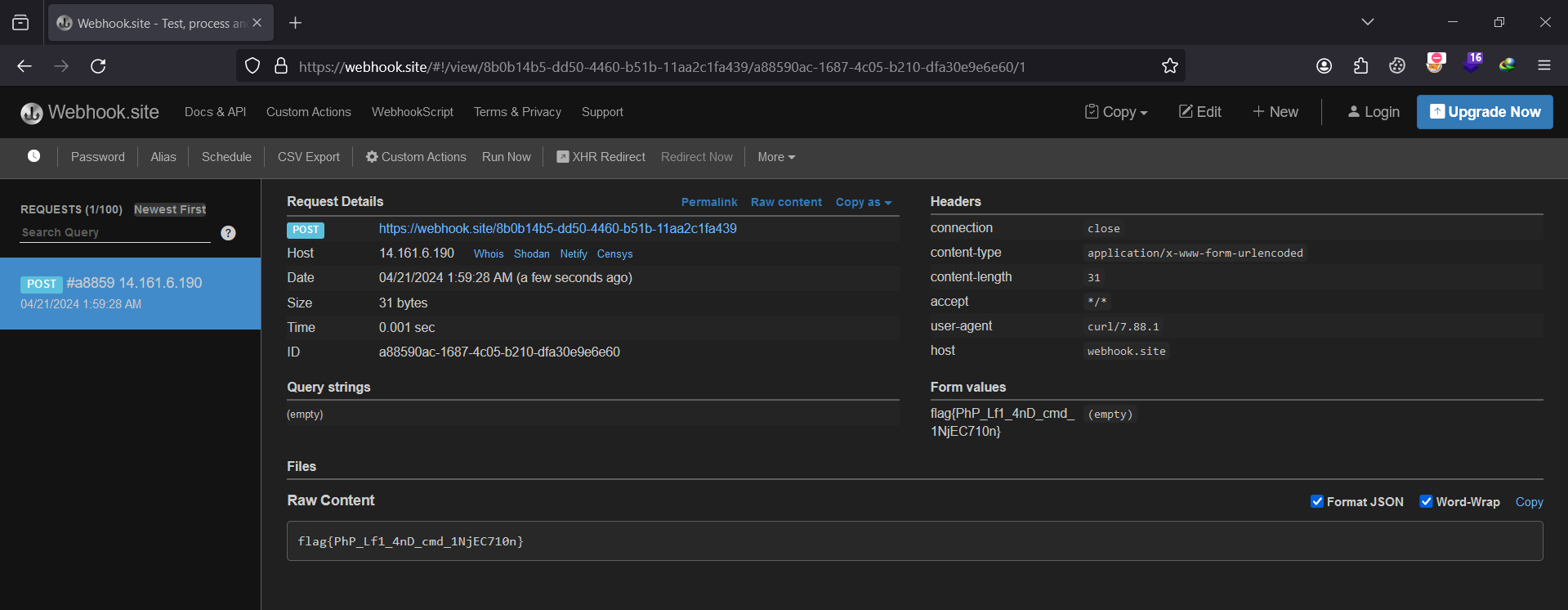
* Vì thế ta có thể lợi dụng điều này để tiến hành thực thi file readflag để lấy flag.

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.



Ta tiến hành truyền 4 tham số mà firewall.php yêu cầu, ta sẽ trỏ output của os command qua file /tmp/hello.txt và bắn nó qua webhook.



Và ta đã thu được flag

**Challenge smart contracts**

Sau khi đăng ký tài khoản và truy cập vào web thì ta thấy được các button như trên. Tiến hành sử dụng trang web như 1 user bình thường. thì ta có thể thấy 1 cài chức năng chính mà ta có thể thao tác được đó chính là transfer và shop.

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

A screen shot of a computer program

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

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

A screen shot of a computer

Description automatically generated

Và đây là flag của challenge này

A screenshot of a computer

Description automatically generated

# **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**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)