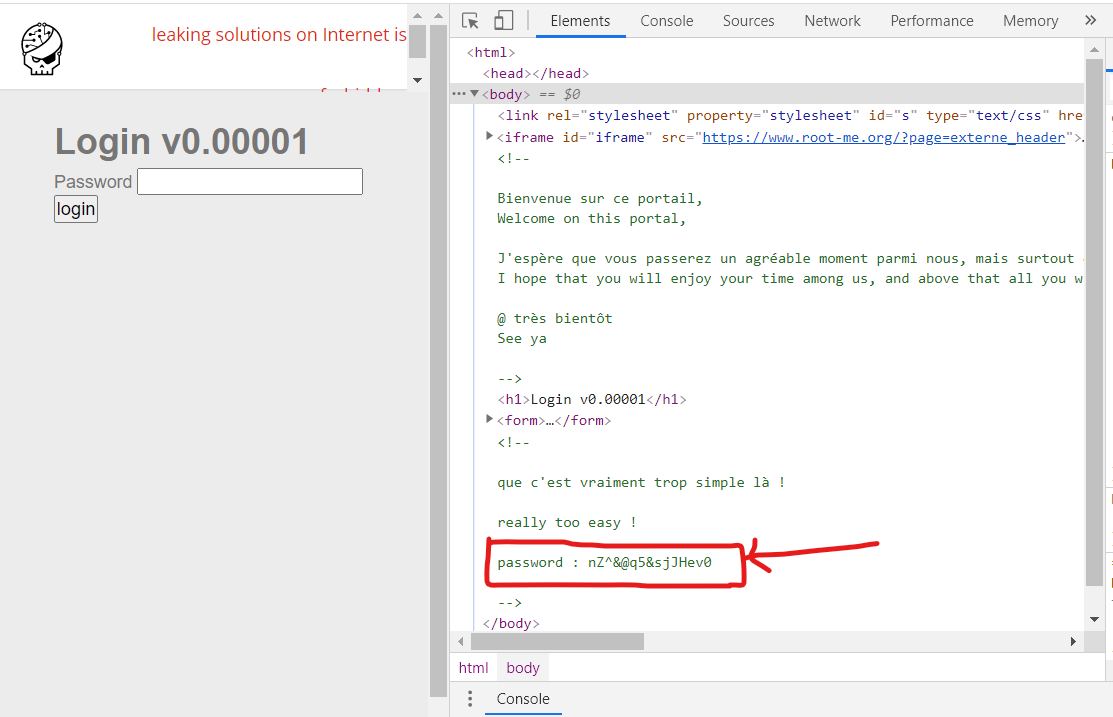
## **1. HTML – Source code**

Nhìn tiêu đề ta thấy ngay từ source code, ta chỉ cần show source là thấy password

Vào site challenge, nhấn F12 là thấy ngay password trong phần comment

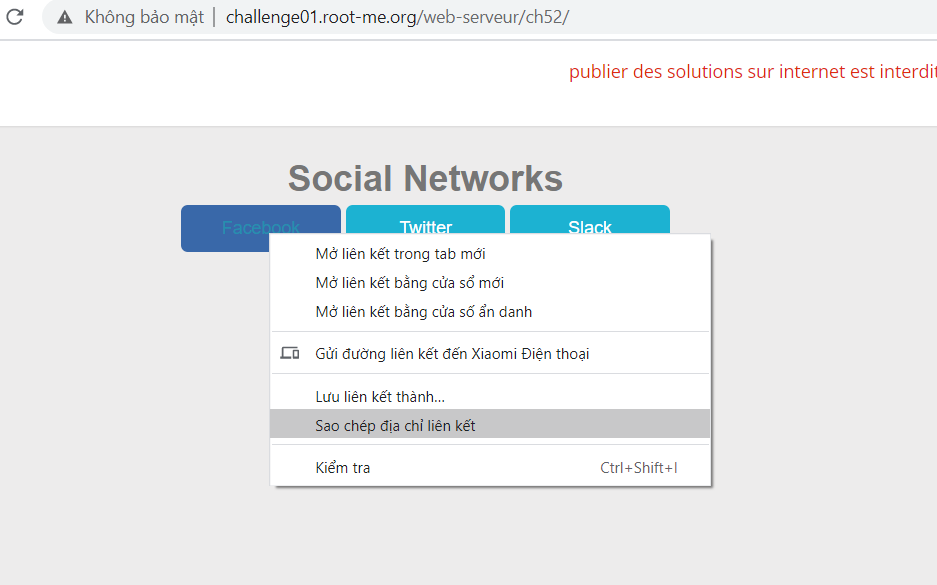
Copy và submit thôi



## **2. HTTP -Open redirect**

Yêu cầu của đề bài là bắt mình redirect đến một trang web khác với 3 trang đã cho

Sao chép địa chỉ của 1 site bất kỳ:

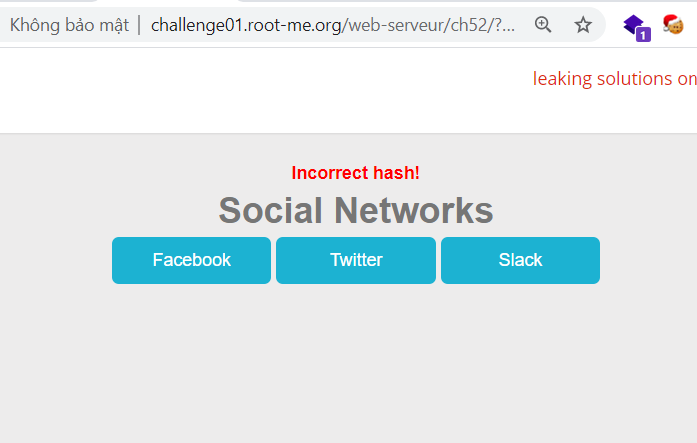


Giả sử mình sao chép địa chỉ của button Facebook được url như sau:

<http://challenge01.root-me.org/web-serveur/ch52/?url=https://facebook.com&h=a023cfbf5f1c39bdf8407f28b60cd134>

Ta thấy có tham số url có value là site đích, ta thử thay thành site khác (abc.com) xem sao:

<http://challenge01.root-me.org/web-serveur/ch52/?url=https://abc.com&h=a023cfbf5f1c39bdf8407f28b60cd134>

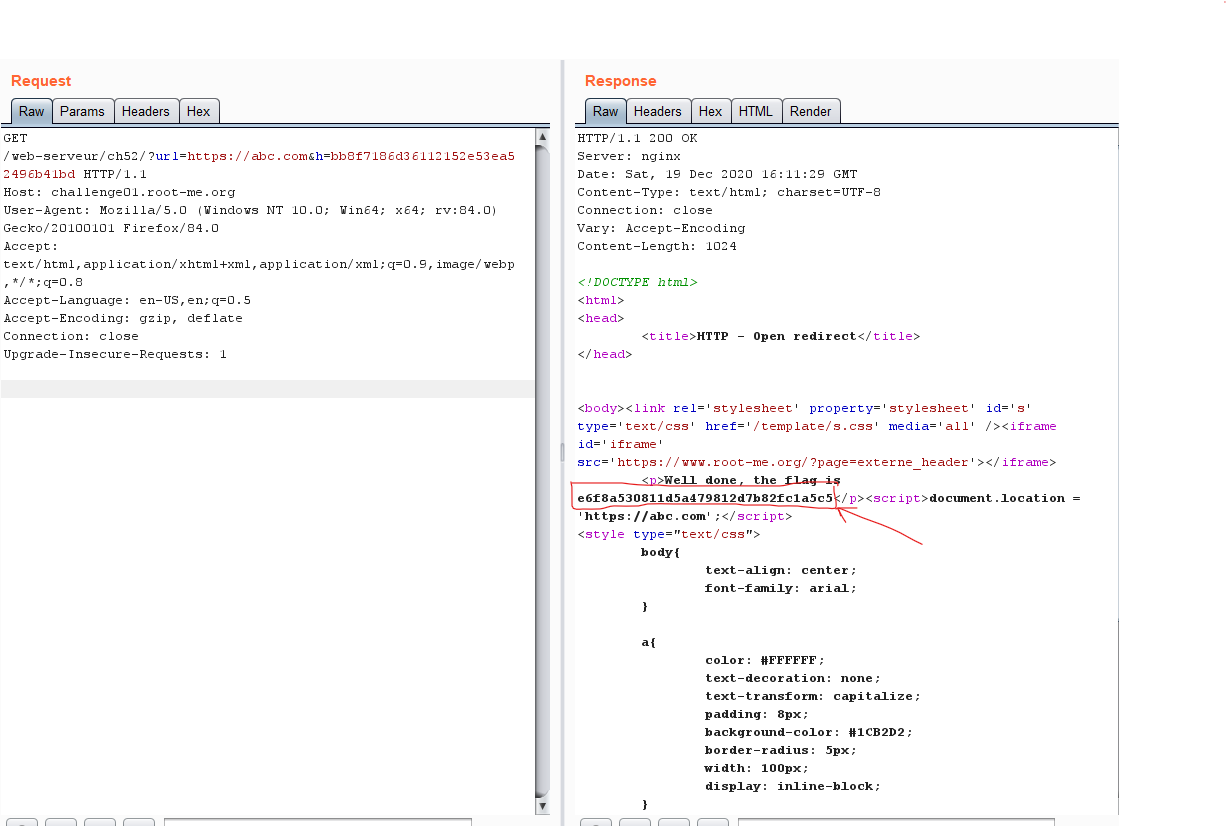


Site thông báo lỗi Incorrect hash. Bây giờ ta để ý còn một tham số h trong địa chỉ trên.

Ta thử encrypt md5 địa chỉ site đích rồi thay thế vào phần value của h xem sao

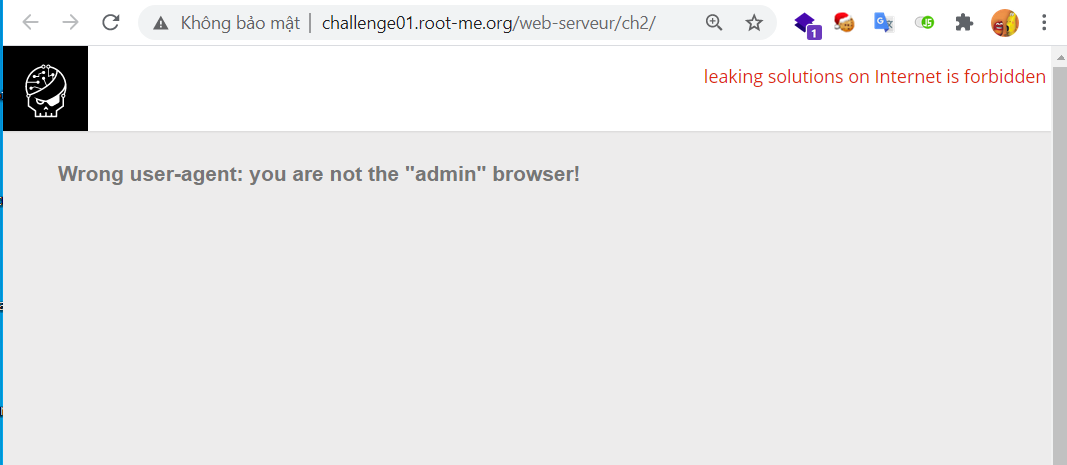
[http://challenge01.root-me.org/web-serveur/ch52/?url=](http://challenge01.root-me.org/web-serveur/ch52/?url=https://abc.com&h=bb8f7186d36112152e53ea52496b41bd)[https://abc.com&h=bb8f7186d36112152e53ea52496b41bd](http://challenge01.root-me.org/web-serveur/ch52/?url=https://abc.com&h=bb8f7186d36112152e53ea52496b41bd)

encrypt Dùng chức năng Repeater trong Burp Suite để bắt lại response ta được flag như sau:



## **3. HTTP -User-agent**

Mở challenge ra ta thấy ngay dòng chữ Wrong user-agent:



Điều ta cần làm là sửa lại user- agent cho đúng

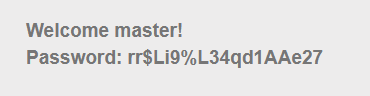
Theo mình biết User – agent là header dùng để lưu thông tin trình duyệt

Trong chalenge này có cụm từ “admin browser”. Vì vậy ta cần sử User agent thành admin

Sử dụng Burp Suite, ta đổi giá trị của header User agent thành admin rồi nhấn forward



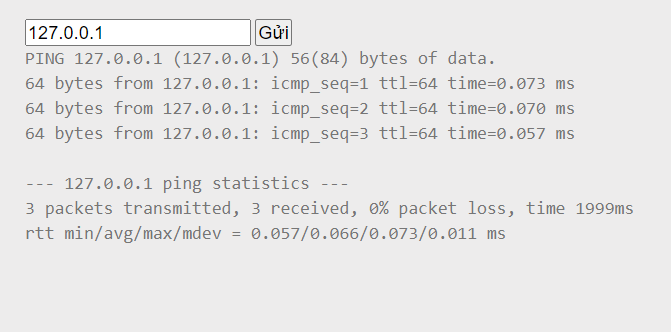
Ok. Ta lấy được password sau:



## **4. PHP – Command injection**

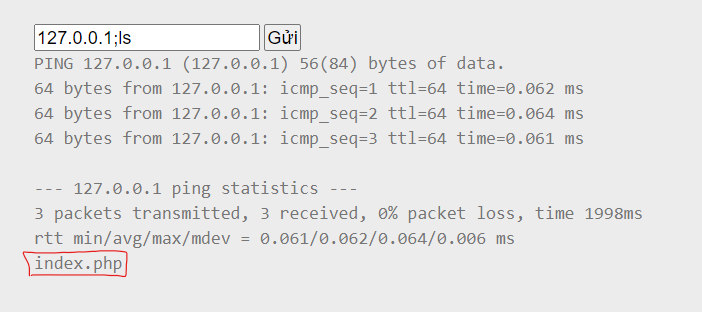
Mở site ra , ta thấy trang web cho chúng ta Ping service

Thử nhập input 127.0.0.1 xem sao, mọi thứ bình thường, ping thành công:



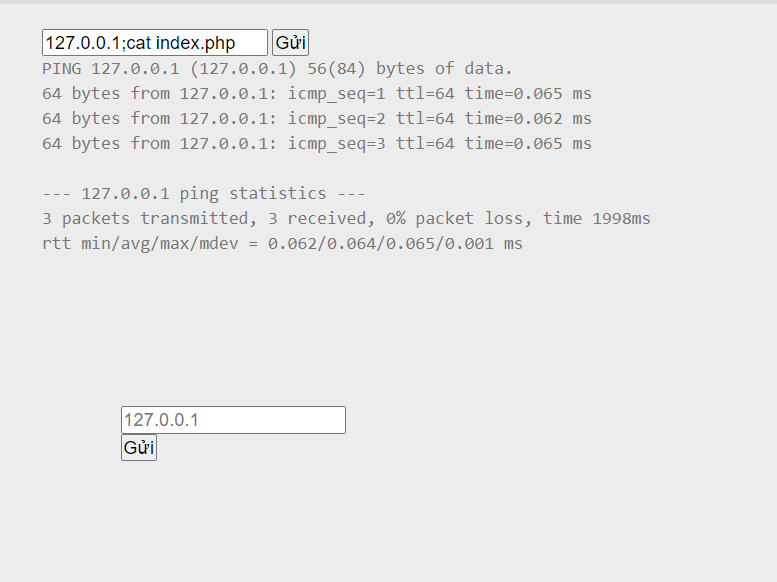
Mục đích của ta là bypass để đọc được nội dung file trên máy chủ

Bây giờ thay vì chỉ nhập input 127.0.0.1 ta thêm ;ls vào sau:



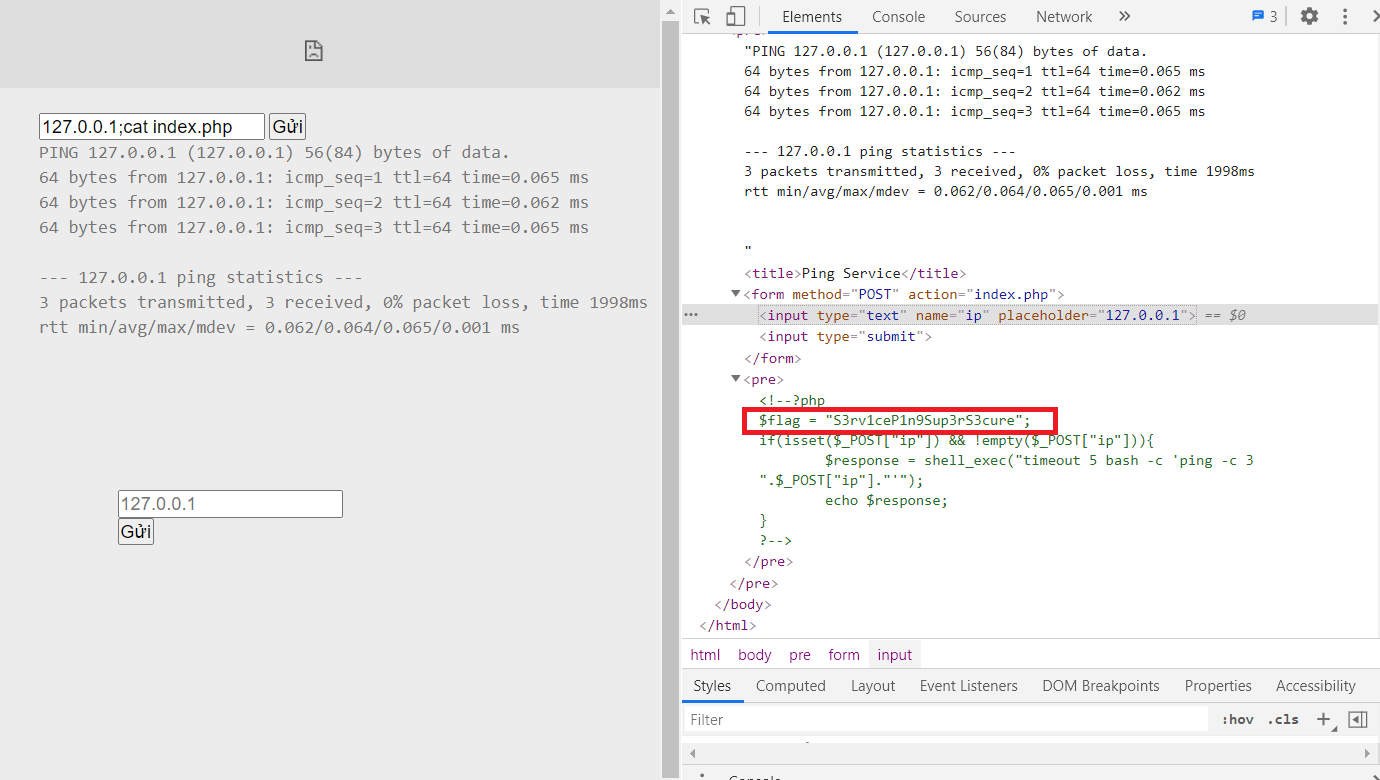
Ta thấy lệnh ls được thực thi, cho output là index.php

Thử đọc file index.php bằng lệnh cat xem sao:



File index.php được đọc thành công !

Nhấn F12, nhìn vào tab Element ta thấy có flag:

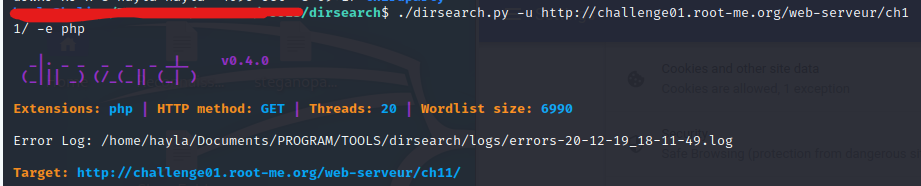


## **5. HTTP - Backup file**

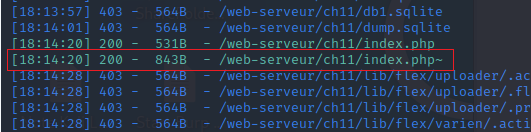
Yêu cầu của bài này là bắt chúng ta phải tìm ra file backup trong ứng dụng web.

Để làm được điều này ta có thể dùng công cụ dirsearch. Sử dụng lệnh sau:

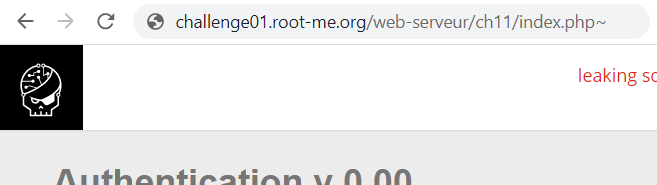
$ ./dirseach -u http://challenge01.root-me.org/web-serveur/ch11/ -e php



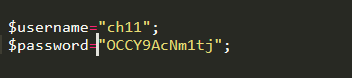
Sau khi chờ đợi ta thấy có output sau:



Truy cập bằng trình duyệt:

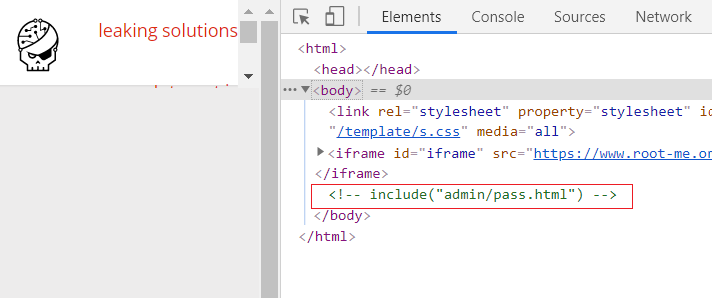


Tải file về rồi mở lên, ta lấy được password, copy và submit thôi:

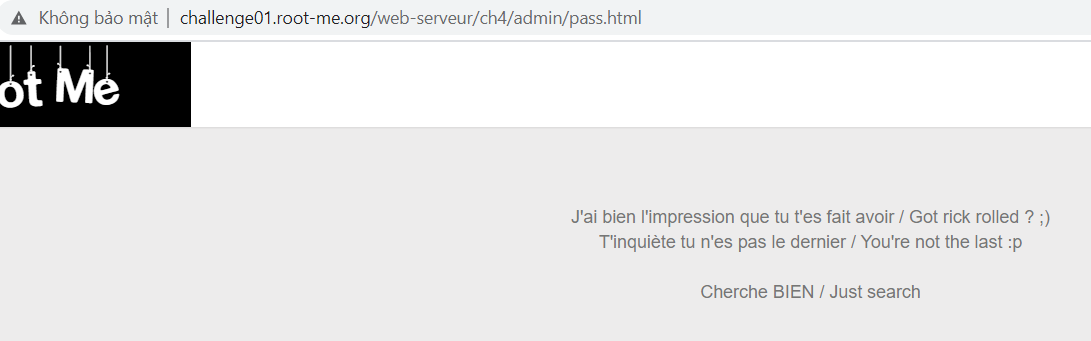


## **6. HTTP - Directory Indexing**

Yêu Mở challenge ra ta thấy trang một page trắng trơn, thử vào soure code xem sao

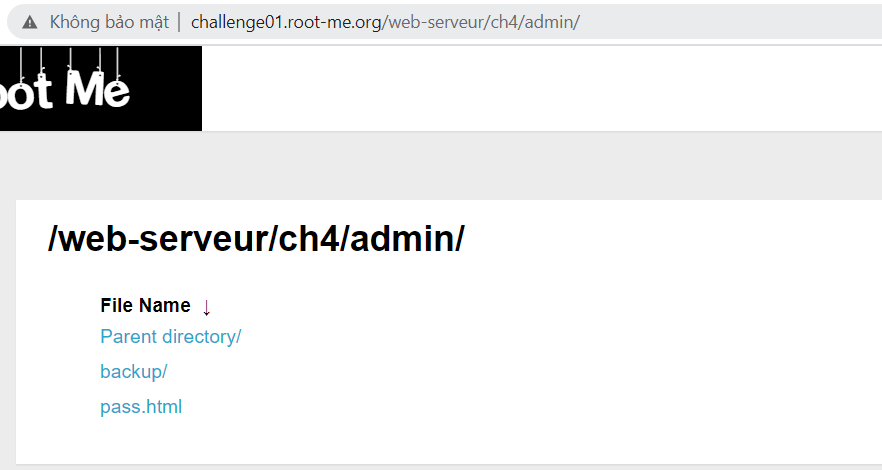


Ta thấy có một đường dẫn là admin/pass.html . Truy cập đường dẫn bằng trình duyệt thử xem:

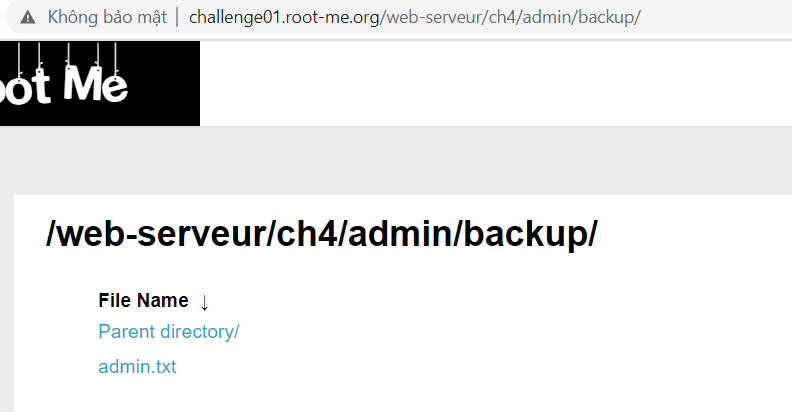


Ta thấy hiện lên thông điệp, đại khái là “bạn không ở cuối cùng, hãy cuộn trở lại”

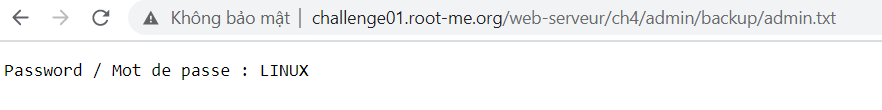
Mình thử truy cập thư mục cha của file hiện tại được kết quả sau:



Ta thấy hiện ra có thư mục backup/. Thử truy cập vào thư mục này, thấy có file admin.txt

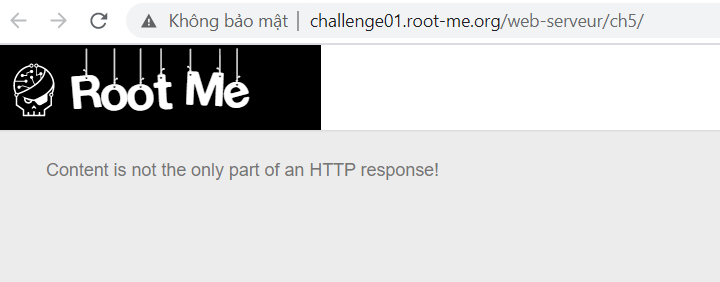


Mở file admin.txt xem thì thấy có mật khẩu bên trong:

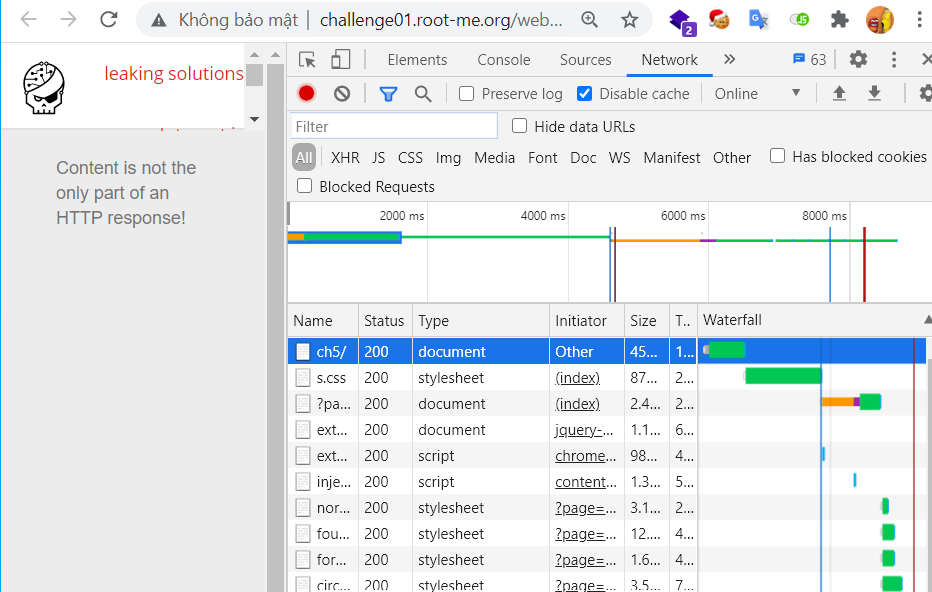


## **7. HTTP – Headers**

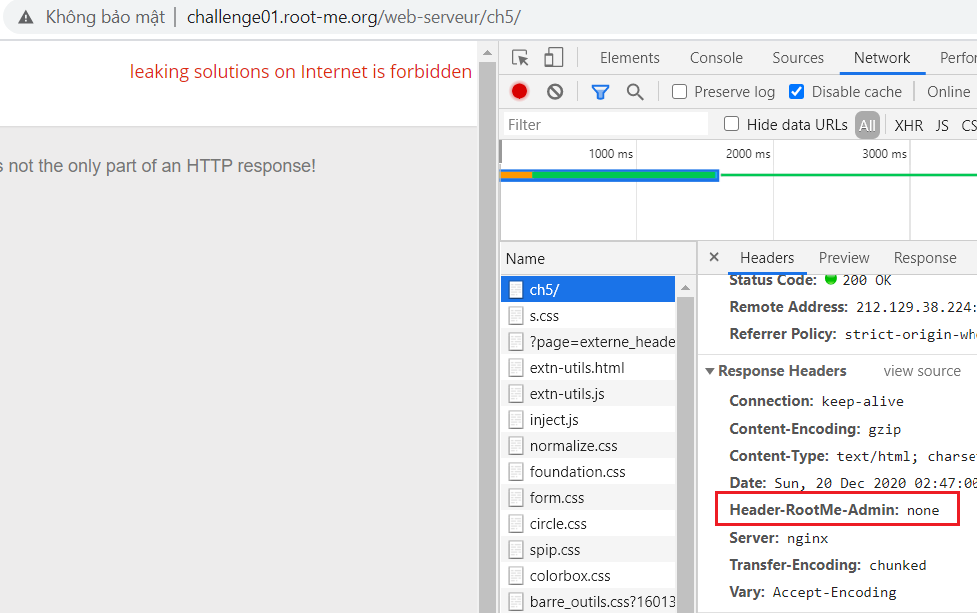
Mở challenge ra ta thấy thông báo:



Thử check HTTP response bằng cách nhấn F12, vào tab Network, reload lại trang

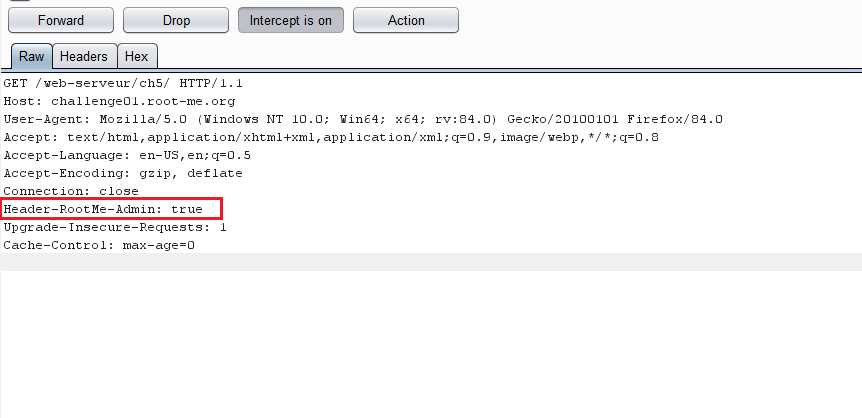


Click vào path đầu tiên ch5/, trong phần Response Headers , ta thấy có một header đáng chú ý là Header-RootMe-Admin: none

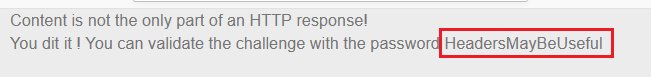


Vậy ta thử tạo một request với header Header-RootMe-Admin với giá trị là true xem sao

Để làm được điều này ta dùng Burp Suite để bắt Request rồi chèn thêm header này vào.



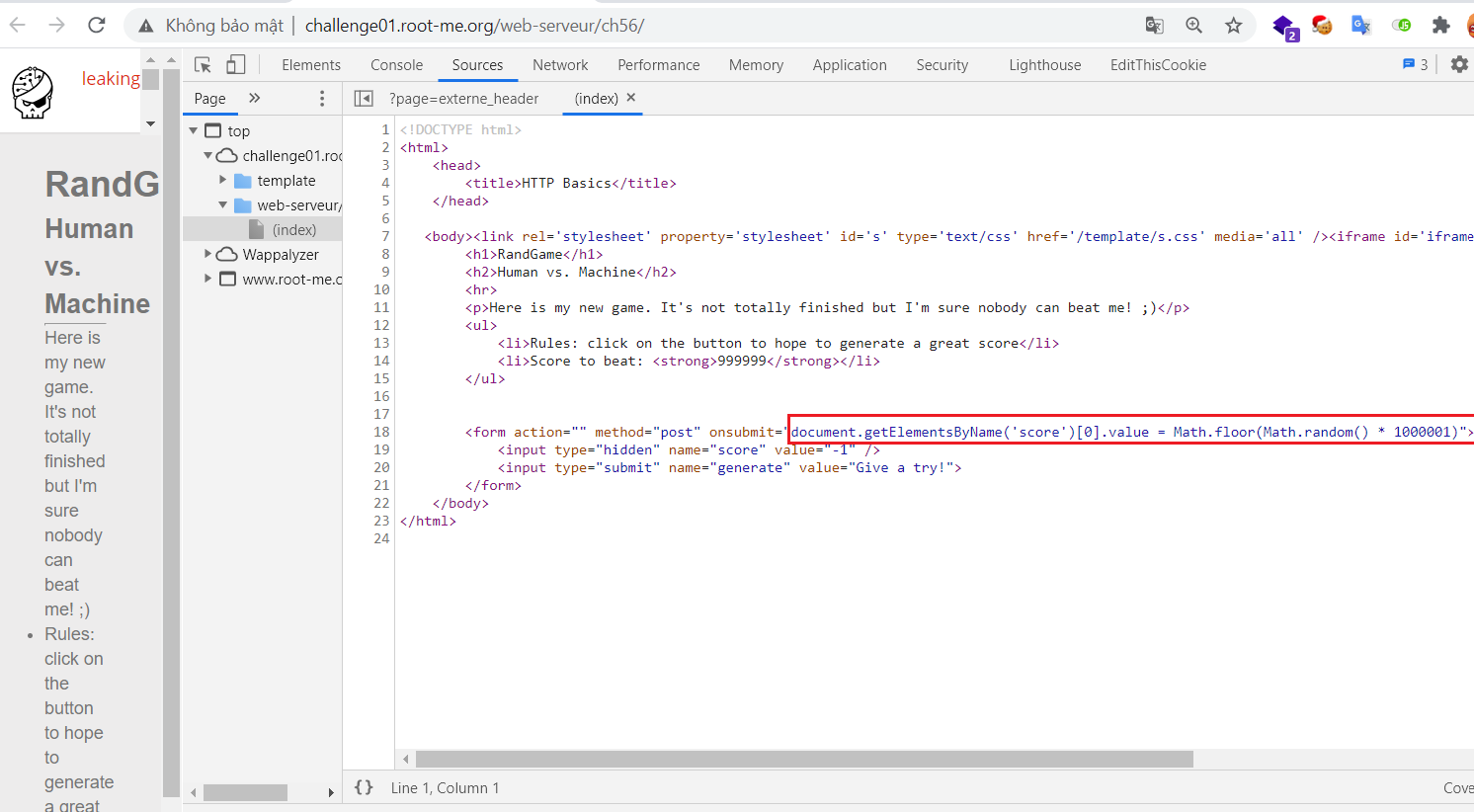
Sau đó nhấn Forward, ta thu được password sau:



## **8. HTTP - POST**

Bài này là một trò chơi random. Nếu bạn random ra một số lớn hơn 999999 thì Flag sẽ hiện ra

Xem source code trong tab Sources, ta thấy có hàm random như hình:



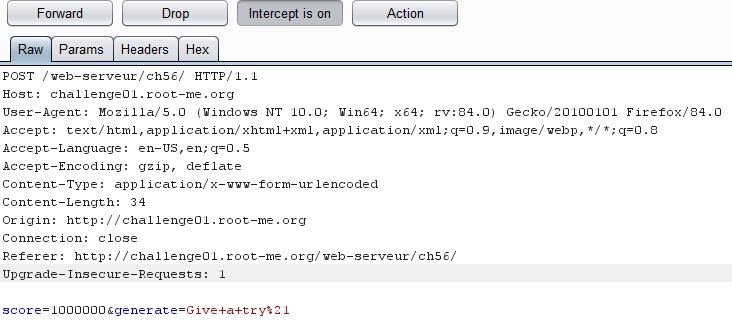
Giá trị score do hàm này trả về có giá trị từ 0 – 1000001. Như vậy chỉ có 2 số 1000000 và 1000001 thỏa mãn bài toán.

Vậy xác xuất quay trúng là 2/1000002 => Rất thấp. Phải may mắn lắm mới quay được số này

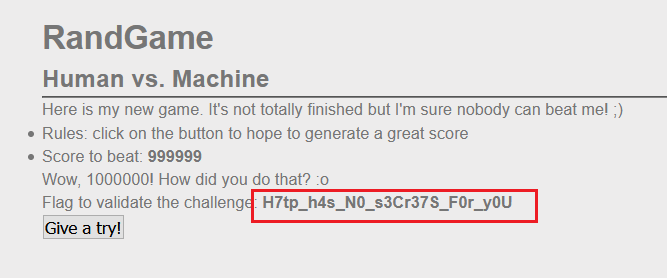
Vậy làm cách nào để đơn giản và nhanh hơn

Ta nhận thấy rằng score sau khi random sẽ được gửi request lên server để check điều kiện. Như vậy ta có thể bắt request và sửa giá trị score trước khi gửi cho server

Để làm được điều này ta có thể dùng Burp Suite



Thay đổi value của score thành 1000000 rồi Forward, ta thu được Flag sau:



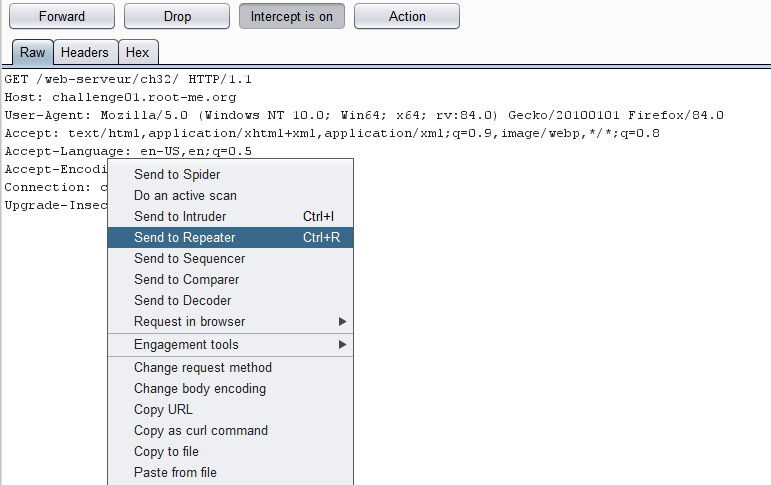
## **9. HTTP – Improper redirect**

Lỗi ở bài này là sau khi thực hiện redirect bằng header Location , lập trình viện không kết thúc chương trình với hàm exit() hoặc die() nên phần code bên dưới vẫn được thực thi.

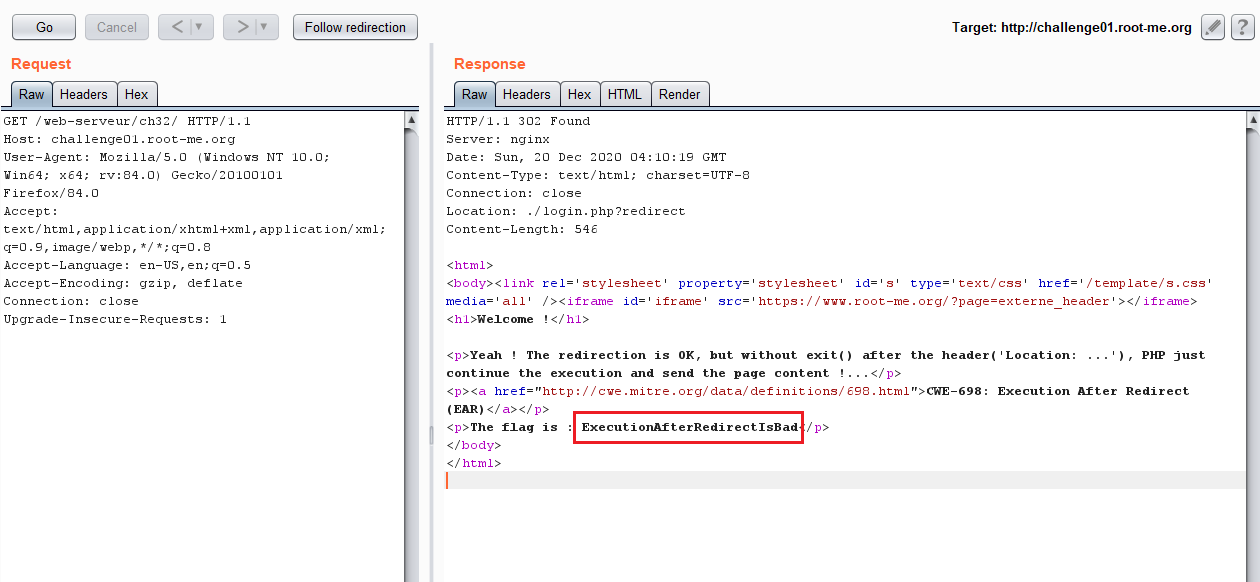
Vậy công việc của chúng ta là bắt response trước khi redirect đến trang khác

Để làm được điều này thì ta dùng Burp Suite.

Đầu tiên, bắt lại Request rồi Send to Repeater



Chuyển sang tab Repeater, click Go, ta thu được Response ở bên tay phải, kèm theo flag



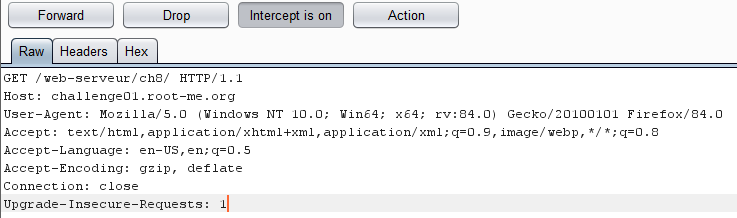
Copy và submit thôi

## **10. HTTP – Verb tampering**

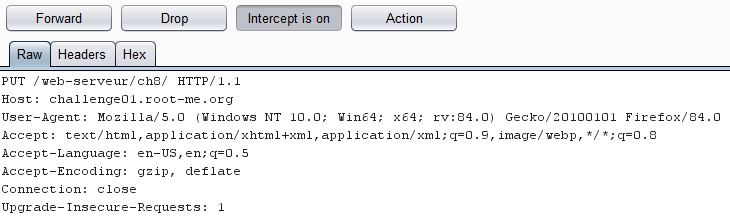
Như tiêu đề Verb tampering , dịch ra tiếng Việt là Giả mạo động từ

Đối với bài này chúng ta cần giả mạo request method, mình có thể dùng bất kì method nào ngoài GET và POST

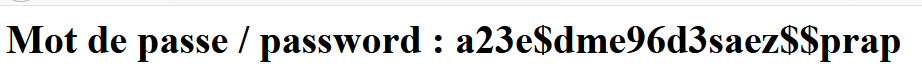
Để làm được điều này ta có dùng Burp Suite bắt request



Ở đây method đang là GET, ta chỉ cần thay thế nó thành method khác là được.Ở đây mình thay thành PUT



Sau đó nhấn Forward, và password hiện ra :

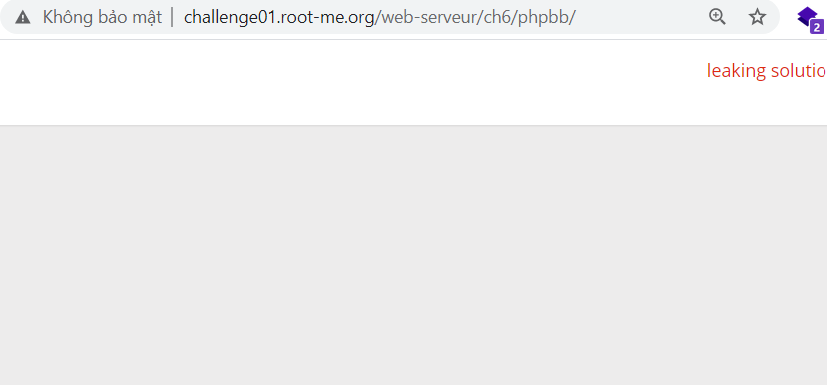


## **11. Install files**

Mở challenge ra thấy một page trắng trơn, mở source code ra thấy trong comment có đường dẫn đến thư mục php



Truy cập đến đường dẫn này ta tiếp tục thấy mộ page trắng trơn



Lỗi ở đây là sau khi cài đặt phần mềm thì web master không xóa file cài đặt đi. Nếu attacker có được những file này sẽ có những thông tin nhạy cảm về trang web

## **8. HTTP - POST**

B

## **8. HTTP - POST**

B

## **8. HTTP - POST**

B