

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

-----o0o-----



CHUYÊN ĐỀ AN TOÀN PHẦN MỀM

HƯỚNG DẪN BÀI THỰC HÀNH
PTIT-PATH_TRAVERSAL

Giảng viên : Ths.Ninh Thị Thu Trang

Nhóm : 07

Thành viên: Phạm Khải Hoàn

Lã Mạnh Cường

Nguyễn Đức Sinh Cung

Bùi Đức Hiệp

Hà Nội - 2023

MỤC LỤC

I.	Cách thực hiện	1
1.	Khởi động bài lab.....	1
2.	Task 1: Xem source code.....	1
3.	Task 2: Xem được nội dung file /etc/passwd.....	2
4.	Task 3: Xem nội dung file /home/viewme.txt	2
5.	Task 4: Submit flag	2
6.	Checkwork	3

I. Cách thực hiện

1. Khởi động bài lab

- Mở bài lab

```
^Cstudent@ubuntu:~/labtainer/labtainer-student$ labtainer -r ptit-path_traversal

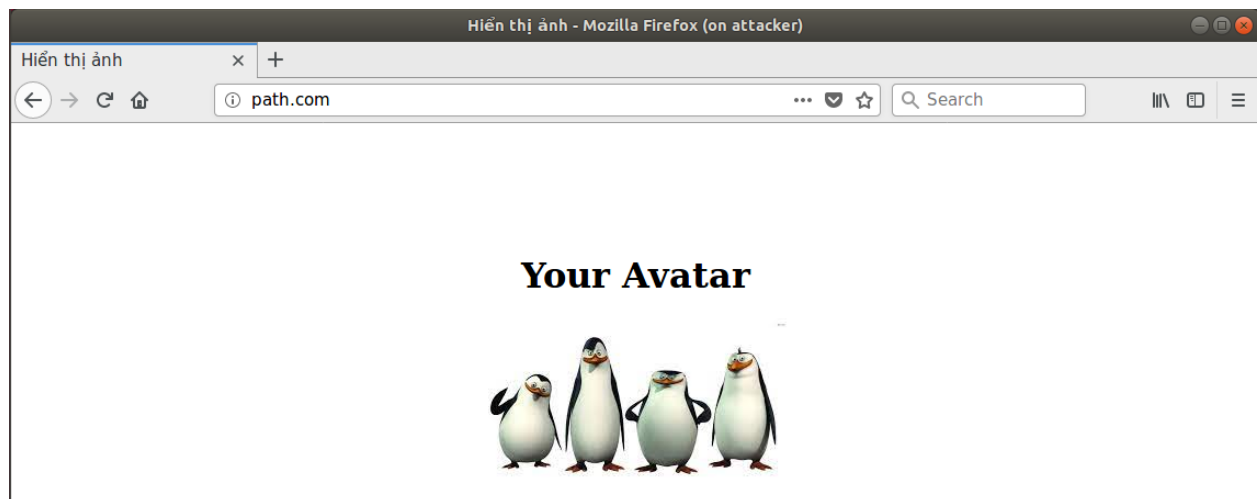
Please enter your e-mail address: [B19DCAT063]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.

The lab manual is at
  file:///home/student/labtainer/trunk/labs/ptit-path_traversal/docs/pathphp.pdf

You may open the manual by right clicking
and select "Open Link".

Press <enter> to start the lab
```

Sau khi mở bài lab sẽ có 2 container hiện lên là web-server và attacker, trình duyệt firefox hiện ra với đường dẫn path.com



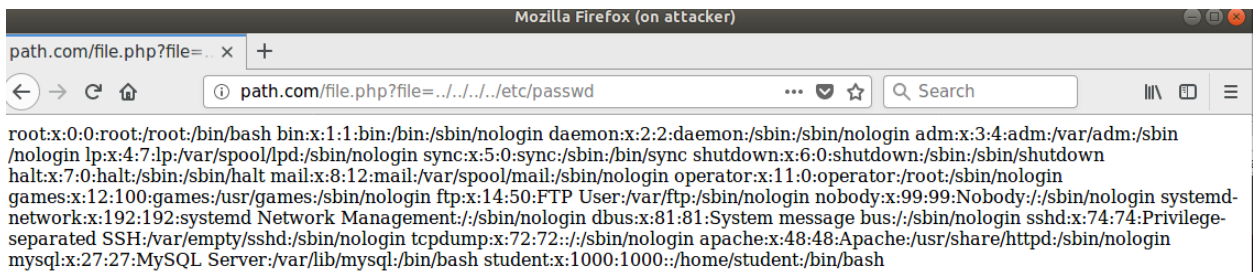
2. Task 1: Xem source code

-Để hoàn thành task 1 ở máy attacker ta dùng câu lệnh curl + url để xem source code

```
student@attacker:~$ curl path.com
<!DOCTYPE html>
<html>
<head>
  <title>Hiển thị ảnh</title>
  <style>
    body {
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
      margin: 0;
      flex-direction: column;
      text-align: center;
    }
  </style>
</head>
<body>
  <img alt="Placeholder for an image" data-bbox="400 200 600 800"/>
</body>
</html>
```

3. Task 2: Xem được nội dung file /etc/passwd.

Dùng kĩ thuật path traversal để bypass bằng cách sử dụng ../ để lùi thư mục, ta sẽ thử dần dần và sau đó sẽ thu được kết quả

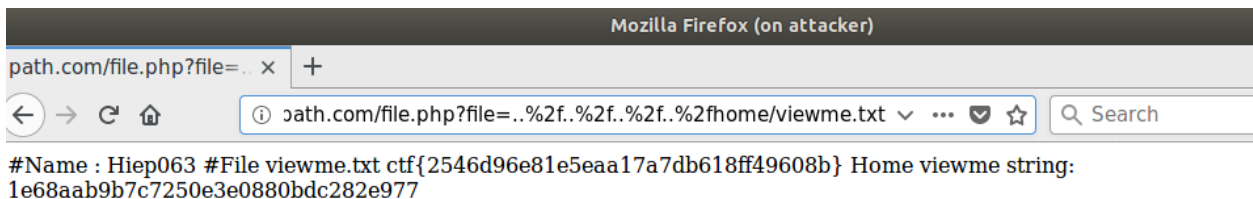


```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin systemd-network:x:192:192:systemd Network Management:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin tcpdump:x:72:72::/sbin/nologin apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash student:x:1000:1000:/home/student:/bin/bash
```

-Từ máy attack sử dụng lệnh curl + đường dẫn để hoàn thành task này.

4. Task 3: Xem nội dung file /home/viewme.txt

-Tương tự task 2 nhưng ở đây các bạn cũng có thể dùng kĩ thuật encode-url để đọc được nội dung file



```
#Name : Hiep063 #File viewme.txt ctf{2546d96e81e5eaa17a7db618ff49608b} Home viewme string: 1e68aab9b7c7250e3e0880bdc282e977
```

-Từ máy attack sử dụng lệnh curl + đường dẫn để hoàn thành task này.

5. Task 4: Submit flag

Sau khi hoàn thành task 3 ta sẽ thu được flag giờ công việc của các bạn chỉ là submit flag bằng cách chạy chương trình C với input là flag

```
student@attacker:~$ ./submit ctf{2546d96e81e5eaa17a7db618ff49608b}  
Correct!
```

6. Checkwork

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork  
Results stored in directory: /home/student/labtainer_xfer/ptit-path_traversal  
Labname ptit-path_traversal
```

Student	path_home	view_code	passwd	submit_flag
B19DCAT063	Y	Y	Y	Y

What is automatically assessed for this lab: