Programming Assignment 5 - SEC 522: Cybersecurity Lab

**Sumaya Altamimi 442203026**

Finding, Exploiting, and Fixing Vulnerabilities

in Web Apps

Table of Contents

[Introduction 2](#_Toc68695225)

[Summary of the vulnerabilities 6](#_Toc68695226)

[Metasploitable Network 6](#_Toc68695227)

[(Information Exposure/ Root access) 6](#_Toc68695228)

[Mutillidae 6](#_Toc68695229)

[1. Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) 6](#_Toc68695230)

[2.(Persistent XSS) 7](#_Toc68695231)

[3.Cross-Site Request Forgery (CSRF) 9](#_Toc68695232)

[4. Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) 11](#_Toc68695233)

[5. Information Exposure 12](#_Toc68695234)

[6. Improper Authentication 13](#_Toc68695235)

[7. Incorrect Permission Assignment for Critical Resource 14](#_Toc68695236)

[8. Improper Privilege Management 16](#_Toc68695237)

[9.Improper Input Validation 18](#_Toc68695238)

[DVWA 19](#_Toc68695239)

[10. Improper Neutralization of Special Elements used in an SQL Command (SQL Injection) 19](#_Toc68695240)

[11.Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) 20](#_Toc68695241)

[12. Improper Limitation of a Pathname to a Restricted Directory (Path Traversal) 22](#_Toc68695242)

[13. Unrestricted Upload of File with Dangerous Type 24](#_Toc68695243)

[14. Improper Restriction of Excessive Authentication Attempts 26](#_Toc68695244)

[Using msfconsole 30](#_Toc68695245)

# Introduction

In this lab, I am going to use Metasploitable Linux virtual machine. Which is a vulnerable for the purpose of practicing penetration testing techniques

Instructions:

* You can download it through this link <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>.
* Use the default login and password msfadmin,msfadmin.
* Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).

Find the IP address of the VM

Look for vulnerabilities in the web services

(Enter IP into web browser)

Using static analysis tools to assist the search.

Summary of the vulnerabilities

at least 15 different types of vulnerabilities

Discovery

How you discovered the vulnerability (tools, code analysis).

Attack vector

Description of the attack vector exploiting the vulnerability (you need to actually exploit the vulnerability).

Mitigation

How you mitigated (fixed) the vulnerability (description / code).

Screenshots

Find an actual exploit for each vulnerability

You should find at least 15 (of the CWE/SANS Top 25) different types of vulnerabilities you discovered in the site (VM image).

Fix the code

in order to prevent the vulnerability from reoccurring.

You should show how to fix any 10 of these.

Hint: The **Mutillidae** web service on this image (a link can be found when you enter the VM IP address in your browser) has each of the OWASP Top 10 vulnerabilities. You only need to find 5 others.

Other useful tools that will help you include **FireBug, Burp-Suite, Wireshark, etc**.

Use the hints in the application as a last resort (your analysis cannot be a regurgitation of the hints).

Also, be mindful of the Security setting in the application as it can make your job harder if set too high.

In addition, please avoid simply repeating the examples shown in class using Damn Vulnerable Web Application (DVWA).

Information Gathering

Metasploitable IP (Using Ifconfig)

172.16.235.2

Open ports (Using nmap -sV 172.16.235.2)

**PORT STATE SERVICE VERSION**

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

# **Summary of the vulnerabilities**

# **Metasploitable Network**

## (Information Exposure/ Root access)

I found the ftp port open, with service called vsftpd 2.3.4. This version allowed me to gain root access of the machine. The reason is that it might contain backdoor by the attacker.

# Mutillidae

## 1. Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)

Go to the directory below:

Graphical user interface, application

Description automatically generated

Write javascript code to test the service, I wrote simple alert:

Graphical user interface, application

Description automatically generated

and it worked:

A picture containing shape

Description automatically generated

In order to make a real exploit will try to display cookie instead of random characters in the alert.

*<script>alert(document.cookie)</script>*

and It worked:

Text

Description automatically generated

Session IDs could be used to steal someone else session, by sending an email with a link

asking to login, that also activate the script when he arrived at it. The victim will click on a link and run the scrip on his computer, attacker can take the session id and can act on behalf of the victim.

## 2.(Persistent XSS)

Go to Add to your blog

Graphical user interface, text, application

Description automatically generated

Table

Description automatically generated with low confidence

So, whenever you go to the blogs page, the alert will pop up as follow:

Shape

Description automatically generated with low confidence

## 3.Cross-Site Request Forgery (CSRF)

Go to add blog

Graphical user interface, application

Description automatically generated

Capture the traffic using Burp Suite and Add a blog:

Graphical user interface, text, application, email

Description automatically generated

Note the added traffic in Burp Suite:

Graphical user interface, text, application, email

Description automatically generated

Sign-in to a different user (or later send the url to another user). Change the blog content as follow:

csrf-token=SecurityIsDisabled&blog\_entry=Exploited!!!!&add-to-your-blog-php-submit-button=Save+Blog+Entry

Graphical user interface, text, application, email

Description automatically generated

By right click and send the request, the url request will be automatically generated by Burp Suite. Select current browser session.

Graphical user interface, application

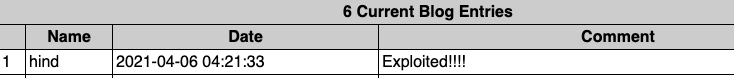
Description automatically generated

Stop capturing and open the copied url in your browser. This shows the second account that you signed in (the victim account):

Graphical user interface, text, application

Description automatically generated

This is the new blog added:



## 4. Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

Graphical user interface

Description automatically generated with low confidence

We can find all files listed

Text

Description automatically generated

Fix:

Escaping charactres, whitelist acceptable values.

## 5. Information Exposure

Before you inject, you need to replace ‘metasploitable’ with ‘owasp10’ in the virtual machine /var/www/mutillidae/config.inc. Then go the User info tab.

Text

Description automatically generated

Write the following command:

Graphical user interface, text, application

Description automatically generated

And it worked:

Table

Description automatically generated with low confidence

## 6. Improper Authentication

Go to Login

A screenshot of a computer

Description automatically generated with medium confidence

Type the following command:

Graphical user interface, text, application

Description automatically generated

and It worked:

Graphical user interface, text

Description automatically generated

## 7. Incorrect Permission Assignment for Critical Resource

Graphical user interface, text

Description automatically generated

Inspect the file menu:

Graphical user interface, text, application

Description automatically generated

Change the option value to “/etc/passwd”

Text

Description automatically generated

and it worked:

Graphical user interface, text, application, email

Description automatically generated

Fix:

Require authentication for each object in the web server and check for privileges.

## 8. Improper Privilege Management

Install some cookie editor (browser plugin) and register to make new account.

Graphical user interface, text, application

Description automatically generated

Note that your name appeared at the corner:

Graphical user interface, text, application

Description automatically generated

Go to Broken authentication page and select login.

Graphical user interface, application

Description automatically generated

In the cookie editor, chane the uid to 1 (typically it is either 0 or 1)

Graphical user interface, text, application, email

Description automatically generated

Save the change by using the save icon.

Graphical user interface, application

Description automatically generated

Refresh the page, note the new name:

Graphical user interface, text, application

Description automatically generated

Now, you have all admin privileges.

## 9.Improper Input Validation

Go to credits

Graphical user interface, text, application

Description automatically generated

Start capturing Using Burp Suit. Click on Owasp link and go back to Burp Suit.

Change the forward value to another link of your choice. In my case it is:

<http://172.16.235.2/mutillidae/index.php?page=redirectandlog.php&forwardurl=http://www.google.org>

By right click and send the request, the url request will be automatically generated by Burp Suite. Select current browser session and copy the url.

Graphical user interface, application

Description automatically generated

Stop capturing and Sign-in to a different account to use that url. It will redirect you to the attacker url.

Graphical user interface, text, application

Description automatically generated

# DVWA

## 10. Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)

Text

Description automatically generated with medium confidence

Try to guess table names:

' or 1=1 UNION SELECT \* FROM TABLES#

Take advantages of error messages:

A picture containing text

Description automatically generated

When tried ' or 1=1 UNION SELECT \* FROM users# :



Which means table exist. After several trials, this worked as follow:

' or 1=1 UNION SELECT user,password FROM users#

Background pattern

Description automatically generated

## 11.Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

Text

Description automatically generated

This indicates current path of DVWA is two folders after the root, to gain root access will do the following: 172.16.235.2 & dir ../../

Text

Description automatically generated

AS shown, there is a config file which seems interesting. We can use 172.16.235.2 & dir ../../config

Text

Description automatically generated

We can use 172.16.235.2 & type ../../config/config.inc.php to read the file but it is not readable. So will copy the content to another file using the command:

172.16.235.2 & cp ../../config/config.inc.php ../../mynewconfig

**Text

Description automatically generated**

Now we can access the file from the url:

[**http://172.16.235.2/dvwa/mynewconfig**](http://172.16.235.2/dvwa/mynewconfig)

**Graphical user interface, text, application

Description automatically generated**

We have all information about the database. We can connect to it remotely.

## 12. Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

Go to File inclusion

**Graphical user interface, text, application

Description automatically generated**

We can change the url from:

[**http://172.16.235.2/dvwa/vulnerabilities/fi/?page=include.php**](http://172.16.235.2/dvwa/vulnerabilities/fi/?page=include.php)

To:

[**http://172.16.235.2/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd**](http://172.16.235.2/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd)

And it worked:

**A screenshot of a computer

Description automatically generated**

In the same way, we can access other files. You can find the original directory to access to other files there and determine their path:

<http://172.16.235.2/dvwa/vulnerabilities/?page=index.php>. Php information file is another example:

**Application

Description automatically generated with medium confidence**

## 13. Unrestricted Upload of File with Dangerous Type

Change the security level to medium. Go to file upload to upload jpg image.

**Graphical user interface

Description automatically generated with medium confidence**

This file can be accessed from the url:

**Graphical user interface, text, application

Description automatically generated**

Try ton upload non-jpg/jpeg file:

**Graphical user interface

Description automatically generated with medium confidence**

Because it only accepts jpeg images, as shown in the source code:

****

Now, will try to upload non-jpeg images. Upload a text file. Intercept the request using Burp Suite.

****

Change the content type to jpeg and forward the request. It will be uploaded and confirm that in the url.

****

And it worked. We could upload any script and any file type to harm the site.

**Graphical user interface

Description automatically generated with medium confidence**

To confirm, visit the url:

**Graphical user interface, text, application, email

Description automatically generated**

## 14. Improper Restriction of Excessive Authentication Attempts

Before performing Brute Force, try to login with fake credentials and intercept the request using Burp Suite.

**Graphical user interface, text, application, email

Description automatically generated**

Right click and send the request to intruder.

**Graphical user interface

Description automatically generated with low confidence**

In the position tab, select the type of the attack as Cluster bomb.

**Graphical user interface, text, application, email

Description automatically generated**

Click clear and add the username and password keywords:

**Graphical user interface, text, application

Description automatically generated**

At the payload tab, set the payload to 1 (username) and add common keywords.

**Graphical user interface, text, application, email

Description automatically generated**

Set the payload to 2 (password) and add common passwords.

**Graphical user interface, table

Description automatically generated**

At the options tab, set the keywords that will match the result in case of successful access:

**Graphical user interface, text, application

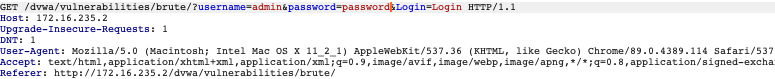
Description automatically generated**

In the same page click start attack. In my case, there are 36 probabilities and only one success:

**Table

Description automatically generated**

Now, confirm with sign-in to the server with the obtained passwords for admin:

****

After forwarding the request, it worked:

**Graphical user interface, text, application

Description automatically generated**

## 15.Information Exposure

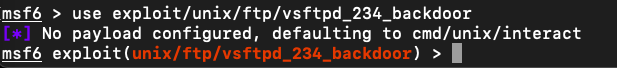
First, will use Nmap to discover open ports and services. One service I notices is vsftpd.

Now, will use msfconsole to search for **vsftpd**:

Text

Description automatically generated

\*You have to make sure if it is the same version. Then use command:



Set our host IP and run “Show options” command.

Text

Description automatically generated

Exploit

Text

Description automatically generated

List files

A picture containing text

Description automatically generated

And it worked, this is root:

Shape

Description automatically generated with medium confidence

**Discovery:**

**view source / hints / guess with common used names/ error messages**

**Fixes:**

**Solution is in youtube (block special chars.. escape... parameters... auth and validate..)**

# References: