LAB EXERCISE

6

COMP3134

Introduction to Cyber Security

Week: 10

Objective(s):
Attacking the web applications and applying mitigation techniques

Learning Outcome(s):
Implement various tactics to attack a network or application
Critique and execute mitigation techniques

Table of Contents

Contents

Summary

Goal: Attacking the web applications and applying mitigation techniques

In Effort To: Implement various tactics to attack a network or application, as well as to critique and execute mitigation techniques

A. Clone GitHub Repo

Clone course GitHub repo to any location on your local machine
Navigate to the location above and create a folder named **wk10**
Use this local folder created above to create all the files necessary for this Lab Exercise

B. Connect to Droplet Server

Using GitBash (on Windows) or the Terminal (on Mac), connect to your droplet server by executing the following command

```
ssh droplet_username@droplet_ip_address
```

When prompted, user your droplet password

Navigate to your web root of your droplet

```
cd /var/www/html
```

You will create scripts in the steps below in the web root

C. HPING3

hping is a free packet generator and analyzer for the TCP/IP protocol.

Install

To install hping3, type the command

```
apt install hping3
```

Navigate to the help manual of hping3 by typing the command

```
hping3 -h or hping3 –help
```

Usage

Using the help as a guide, send the following packets to the prof IP Address

1) 10,000 TCP packets all at once from random source IP Addresses
2) 9,000 UDP packets in a span of 90 seconds from a spoofed source address
3) 11,000 ICMP packets with a data size of 1KB at an interval of 75 packets per second

Create a file named **hping.txt** that shows the commands needed for the tasks above.

D. Directory Traversal Page Version 1

Script Creation

Create PHP page named **directory_traversal_part1.php** in your droplet web root
This PHP page will display all files and folders of path that will be given to it via a query string parameter without any validation checking
Insert the following content for the php page

```
<?php

ini_set('display_errors', 1);

ini_set('display_startup_errors', 1);

error_reporting(E_ALL);

$path=isset($_GET['q']) ? $_GET['q'] : '.';

print "<pre>";

print_r(scandir($path));

print "</pre>";

?>
```

Running Script

Open any browser.
Open the URL: {Your droplet IP}/ directory_traversal_part1.php
Take a screenshot of your browser. Name the screenshot **step_d-1.png**

Using the Query String

Open the URL: {Your droplet IP}/ directory_traversal_part1.php?q=./
Take a screenshot of your browser. Name the screenshot **step_d-2.png**

Mystery Task 1

Open the URL
{Your droplet IP}/ directory_traversal_part1.php?q=hello
Take a screenshot of your browser. Name the screenshot **step_d-3.png**
Create a text file named **step_d.txt** and describe

- What you see on the browser (the issue)
- What sensitive information is given by this page

Directory Traversal 1

Open the URL: {Your droplet IP}/ directory_traversal_part1.php?q=../../
Take a screenshot of your browser. Name the screenshot **step_d-4.png**
Create a text file named **step_d-4.txt** and describe

- What you see on the browser (the issue)
- What sensitive information is given by this page

Directory Traversal 2

Open the URL: {Your droplet IP}/ directory_traversal_part1.php?q=%2e%2e%2f
Take a screenshot of your browser. Name the screenshot **step_d-5.png**
Create a text file named **step_d-5.txt** and describe

- What you see on the browser (the issue)
- What sensitive information is given by this page

E. Directory Traversal Page Version 2

Create a PHP script named **directory_traversal_part2.php**. Copy the contents of **directory_traversal_part1.php** as your starting point.
Apply the necessary changes to mitigate the issues stated in Step D
Hint: There are two issues to mitigate

- Should not be able to view files and folders before html directory
  - *HINT,* Use basename()
- Should not attempt to look at folders that do not exists
  - *HINT,* File_exists()
- BONUS, do not allow user to pass a filename
  - Look for dot in parameter

Create a text file named **step_e.txt** and state how you will mitigate these two problems.
Take a screenshot of your source code, demonstrating the updated changes of the **directory_traversal_part1.php** script. Name the screenshot **step_e.png**

F. Login Page Version 1

Create a PHP script named **login_part1.php**
This page will display a login form with a password field and a submit button

```
<h1>Weak Password</h1>

<form method="post">

   <label>Password</label>

   <input type="password" name="password">

   <br/>

   <input type="submit">

</form>
```

Using the following url:
https://www.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

Make the modifications to the script so that:

- if the user types in any of the ten passwords
    - Display a success message instead of the form
        - "Successfully authenticated"

Take a screenshot of your source code, demonstrating the updated changes of the script.
Name the screenshot **step_f.png**

G. Comments in Source Code Version 1

Create an HTML script named **comments_in_source_code_part1.html**
Create an html page that will display h1-h6 tags and a descriptive comment tag
Below is a sample for h1

```
<h1>This is an example of an H1 header tag</h1>

<!--Created by John Smith with employee id: 123456-->
```

Create 5 more examples (h2-h6)
Take a screenshot of your html source code. Name the screenshot **step_g.png**

H. Comments in Source Code Version 2

Create a PHP script named **comments_in_source_code_part2.php.** Copy the contents of **comments_in_source_code_part1.html** as your starting point.
Apply the necessary changes to mitigate the issues stated in Step G
Create a text file named **step_g.txt** and state how you will mitigate the problem.
Take a screenshot of your source code, demonstrating the changes.
Name the screenshot **step_g.png**

Hint: Convert all HTML comments to PHP comments, which are not seen by browser

I. Login Page Version 2

Create a PHP script named **login_part2.php**. Copy the contents of **login_part1.php** as your starting point.
Make the following alterations:

- Add a hidden field with a username (be creative)
- Once user correctly guesses password
    - Display a welcome message instead of the form
        - "Welcome {username} to Your Portal"

Take a screenshot of your source code, demonstrating the changes.
Name the screenshot **step_i.png**

J. Commit and Upload Changes to GitHub repo

Commit the changes to your repo by:

1. Opening a GitBash window and ensure that it is connected to your local machine
2. Navigate to local repository directory location
3. Add all the files completed in this Lab Exercise
4. Commit the changes
5. Push the changes to your GitHub course repo

Please refer to the instructions in the last section of Lab Exercise 1