Darkly

Summary: This project is an introduction to cyber security in the field of the Web

Version: 5.1

Contents

Chapter I

Preamble

Chapter II

Introduction

When you develop your first websites, you will have absolutely no clue about the risks they will be exposed to on the World Wide Web.

This little project is here to teach you the basics: you will learn about these risks and vulnerabilities while auditing a simple website. This website demonstrates breaches, some of which still appear on well-established websites you visit on a daily basis.

Here is a major introduction to general vulnerabilities you will encounter on the World Wide Web.

Chapter III

Objectives

This project aims to introduce you to cybersecurity in the field of the WWW.

You will discover OWASP, which is simply the largest cybersecurity project to date.

You will also learn what many frameworks do for you, automatically and transparently.

Chapter IV

General instructions

- This project will be reviewed by humans.
- You might have to prove your results during your evaluation. Be ready to do so.
- To validate this project, you will have to use a virtual machine (i386). If the configuration is correct, once you launch your machine with the ISO provided in the subject, you will get a simple prompt with an IP:

- You just need to use your web browser to access the displayed IP address.
- Please inform the educational team if you find a bug!

Chapter V

Mandatory part

- Your turn-in folder will only include the files that allowed you to solve each of the exploited breaches.

- Your folder will look like this:

```
$> ls -al
[..]
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX {Breach name}
[..]
$> ls -alR {Breach name}
{Breach name}:
total 16
drwxr-xr-x 3 root root 4096 Dec 3 15:22 .
drwxr-xr-x 6 root root 4096 Dec 3 15:20 ..
-rw-r--r-- 1 root root  5 Dec 3 15:22 flag
drwxr-xr-x 2 root root 4096 Dec 3 15:22 Resources

{Breach name}/Resources:
total 8
drwxr-xr-x 2 root root 4096 Dec 3 15:22 .
drwxr-xr-x 3 root root 4096 Dec 3 15:22 ..
-rw-r--r-- 1 root root  0 Dec 3 15:22 whatever.whatever
$> cat {Breach name}/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$>
```

- You will place everything you need to prove your resolution during the evaluation in your Resources folder.

WARNING: You must be able to perfectly explain everything that is included in this folder. This folder cannot include ANY binaries.

- If you need a specific file included in the project ISO, you will have to download it during the evaluation. You must not put it in your repository under any circumstances.

- If you're using a specific external software, you will have to set up the required environment (VM, Docker, Vagrant).
- For the mandatory part, you will have to complete 14 different breaches.
- During the evaluation, you may be required to fix the breaches you have exploited. Understanding what you exploit is, of course, strongly recommended.
- Explaining what you do is often more important than the exploitation itself. Take the time to understand, and make sure you are understood.

Hey, smarty (or not-so-smarty) pants! You cannot use scripts such as sqlmap to make exploitation look trivial. Anyway, you will have to be very specific when explaining your approach during the evaluation.

Chapter VI

Bonus part

For the bonus part, you will only need to provide advanced explanations for the most recognized breaches you have identified.

The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been fully completed and works without any malfunctions. If you have not met ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter VII

Submission and peer-evaluation

Submit your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double-check the names of your folders and files to ensure they are correct.