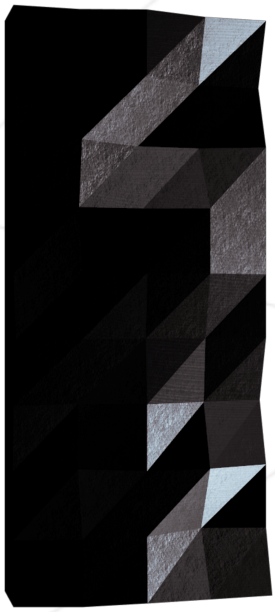

Project SECURITY

Darkly

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

Contents

Chapter I

Preamble

There is something wrong...

Chapter II

Introduction

When you develop your first websites, you will have absolutely no clue regarding the risks they will be exposed to in 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 shows breaches, some of which still show on well established websites you visit on a daily basis.

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

Chapter III

Objectives

This project aims to make you discover cyber security in the field of the WWW.

You will discover OWASP, which simply is the largest cyber security project to this day.

You will also find out 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 have launched your machine with the ISO you were provided with the subject, you will get a simple prompt with an IP:

- You just need to choose your web browser to launch the displayed IP address.
- Please, warn the educational team if you find a bug !
- You can post you questions on the forum, Jabber, IRC, Slack...

Chapter V

Mandatory part

- Your turn-in folder will only include the things 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 Ressources

{Breach name}/Ressources:
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.wahtever
$> cat {Breach name}/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$>
```

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

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

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

- If you're using a specific external software, you will have to set the specific 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 often is more important than the exploitation itself. Take 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 you explain your approach during evaluation.

Chapter VI

Bonus part

Bonus will be taken into account only if the mandatory part is PERFECT. PERFECT meaning it is completed, that its behavior cannot be faulted, even because of the slightest mistake, improper use, etc... Practically, it means that if the mandatory part is not validated, none of the bonus will be taken in consideration.

For that bonus part, you will only have to give advanced explanations for the most recognized breaches you will have found.

Chapter VII

Turn-in and peer evaluation

As usual, turn-in your work on your `GiT` repository. Only the work on your repository will be reviewed during the evaluation.