Chapter 1

Introduction

When you develop your first websites, you usually do not have any idea of the existing vulnerabilities in the world of the web. This small project aims to fill this gap: you will become aware of these vulnerabilities by doing an audit of a simple website. This site has flaws still regularly present on sites that you visit every day. Here is a big introduction to the general vulnerabilities found in the world of the web.

Chapter 2

Objectives

This project aims to introduce you to computer security in the field of the web. You will be able to discover OWASP, which is, neither more nor less, the biggest project of web security to date. You will also understand what many frameworks do completely transparent for you.

Chapter 3

General Instructions

- This project will only be corrected by humans.
- During your defense, you may be required to prove your results. You must prepare for it.
- You need to use virtual machine (i386) to validate this project. Once your machine launched with the ISO provided with the subject, if everything is well configured, you will have a simple prompt with an IP

```
 ____                  _______    _____
|  _ \                |__   __|  / ____|
| |_) | ___  _ __ _ __ | | ___| (___   ___  ___
|  _ < / _ \| '__| '_ \| |/ _ \\___ \ / _ \/ __|
| |_) | (_) | |  | | | | | (_) |___) |  __/ (__
|____/ \___/|_|  |_| |_|_|\___/_____/ \___|\___|
                  WEB SECTION
              Good luck & Have fun
To start the challenges, open your web browser (:80) and go to:
                 172.16.60.128
BornToSecWeb login: _
```

- You only need to connect with your browser to ip address displayed.
- Please inform the pedagogical team if you find a bug!
- You can ask your questions on the forum, on jabber, IRC, slack ...

Chapter 4

Mandatory Part

- Your turn-in folder should only contain the things that allowed you to solve each exploited flaw.
- Yout turn-in folder should have the following structure:

```
$> ls -al
[..]
drwxr-xr-x  2 root root 4096 Dec  3 XX:XX {Nom de faille}
[..]
$> ls -alR {Nom de faille}
{Nom de faille}:
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
{Nom de faille}/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
$> cat {Nom de faille}/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$>
```

Where `Nom de faille` is name of the fault

- In the Resources folder you will put everything you need for prove your resolution in defense

  ATTENTION Everything in this folder must be able to be explained clearly without any hesitation. NO binary should be present in this

file.

- If you need to use a specific file present on the ISO of the project, you must download it in defense. You must not under any circumstances put this one in your repository.
- In the case of using specific external software, you must prepare a specific environment (VM, docker, Vagrant).
- As mandatory part, you must exploit 14 different faults.
- During your defense, in some cases, you will be asked for possible fix for the flaws you exploited. It is strongly advised to understand everything you operate.
- Knowing how to explain is often more important than exploitation itself: take the time to understand, and especially to make sure you can be understood clearly.

  For the clever (or not) ... Of course you do not have the right to use scripts like sqlmap in order to make the exploitation trivial. You must in any case clearly explain your approach during your defense.

Chapter 5

Bonus Part

> Bonuses will only be counted if your mandatory part is PERFECT. By PERFECT, we obviously mean that it is fully realized, and it is not possible to alter its behavior in default, even in case of error, misuse, etc ... Concretely, this means that if your mandatory part is not validated, your bonuses will be fully IGNORED.

As bonus part, you simply need to provide advanced explanations for the most recognized flaws that you have encountered.

Chapter 6

Correction and peer-evaluation

Make your work on your GiT repository as usual. Only the present work on your repository will be assessed in defense.