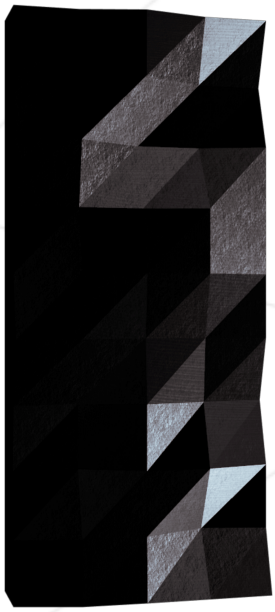


# SECURITY Project

## Darkly

42 Sta ff pedago@staff.42.fr

*Summary: This project is an introduction to computer security in the field from the web.*

# Contents

# Chapter I

# Preamble

There is something wrong ..

# Chapter II

# Introduction

When you develop your first websites, you usually don't have the slightest idea of the vulnerabilities that exist in the web world.

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 that are still regularly present on sites that you visit every day.

So here is a big introduction to general vulnerabilities found in the web world.

# Chapter III

# Objectives

The aim of this project is to introduce you to computer security in the web domain.

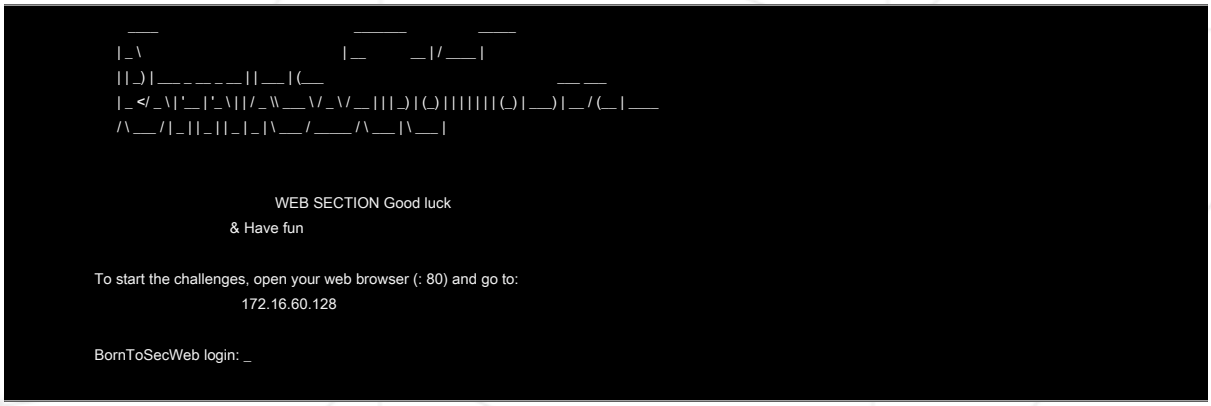
You will be able to discover OWASP, which is, no more and no less, the biggest web security project to date.

You will also understand what a lot of frameworks do in an automatic and completely transparent way for you.

# Chapter IV

# General guidelines

- This project will only be corrected by humans.
- You may be required, during your defense, to prove your results. You have to prepare for it.
- You will need to use a virtual machine (i386) to validate this project. Once your machine is started with the ISO supplied with the subject, if everything is well con fi gured, you will have a simple prompt with an IP:



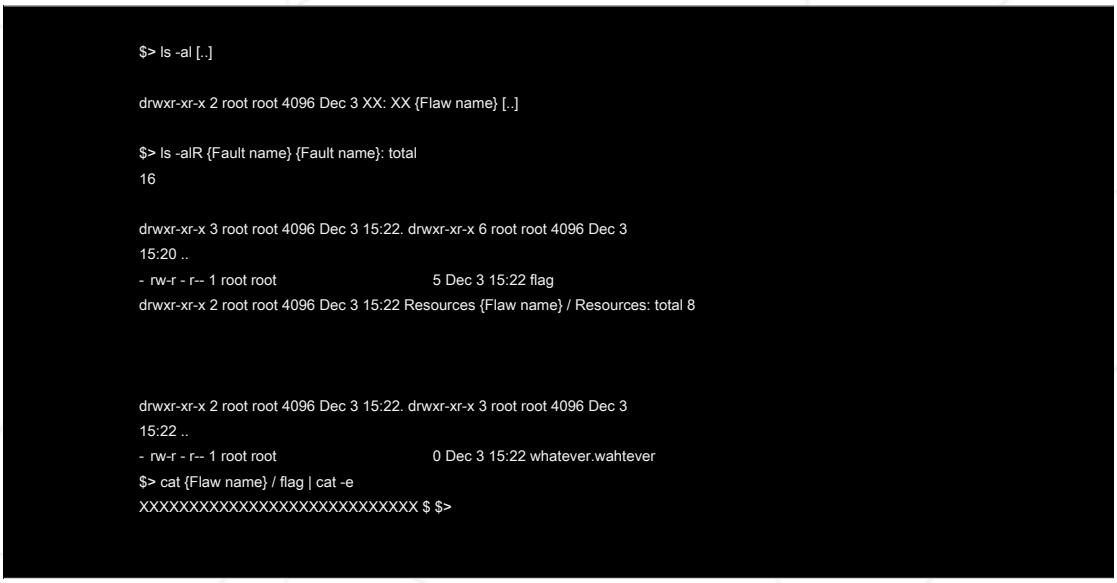

- You only need to choose your browser to launch the displayed ip address.
- Please let the pedago know if you find a bug!
- You can ask your questions on the forum, on jabber, IRC, slack ...

# Chapter V

# Mandatory part

- Your render folder should only contain the things that allowed you to resolve each of the exploited flaws.

- Your rendering will look like this:




- In the Resources folder you will place everything you need to prove your resolution in defense.

ATTENTION: Everything that is present in this file must be able to be explained clearly without any hesitation.

NO binary should be present in this folder.

- If you need to use a speci fi c fi le present in the ISO of the project, you must download it in defense. You should not put it in your repository under any circumstances.

- In the case of using specific external software, you must prepare a specific environment (VM, docker, Vagrant).

- As part of your mandatory part, you must complete 14 di ff erent loopholes.
- During your defense, in certain cases, you will be asked for possible fi xes for the loopholes you have exploited. It is therefore strongly advised that you fully understand everything you are exploiting.
- Knowing how to explain is often more important than the operation itself: take the time to understand, and above all to ensure that you can be understood clearly.

For the smart ones (or not) ... Of course you are not allowed to use sqlmap type scripts in order to make exploitation trivial. You will have to clearly explain your approach during your defense anyway.

# Chapter VI

# Bonus part

Bonuses will only be counted if your mandatory part is PERFECT. By PERFECT, we obviously mean that it has been fully implemented, and that it is not possible to fault its behavior, even in the event of an error, however vicious it may be, improper use, etc. Concretely, this means that if your mandatory part is not validated, your bonuses will be completely IGNORED.

As part of your bonus round, all you have to do is provide advanced explanations for the most recognized loopholes that you have encountered.

# Chapter VII

## Rendering and peer-evaluation

Return your work to your repository GiT as usual. Only the work on your deposit will be evaluated in defense.