Attacks and defenses on web applications lab

# Preparation

### TOOLs

1. Each trainee should install and examine the OWASP Juice Shop tool (<https://www.owasp.org/index.php/OWASP_Juice_Shop_Project>).
2. Additional tools:
   1. Burp Suite (<https://portswigger.net/burp>)
   2. Cyber Chef (<https://cyberchef.org/>)
   3. Dirsearch (<https://github.com/maurosoria/dirsearch>)

# Introduction

Vulnerable software packages, like the OWASP Juice Shop, represent applications that contain vulnerabilities and security challenges, where trainees need to conduct attacks to complete a challenge. Once the attack is understood and successfully conducted, the defender perspective is examined by discussing the vulnerabilities and countermeasures that need to be put in place to prevent the attack from succeeding.

Vulnerable software packages vary in their maturity, from basic examples demonstrating a few attacks and vulnerabilities, to sophisticated systems containing a vast plethora of teaching assignments. Furthermore, they differ on the security concepts that they cover, as well as the underlying technology on which they are built. Out of all the available options, we selected the OWASP Juice Shop Project due to the following reasons:

* It is mature, categorized as a Flagship project by the OWASP organization, signifying its value to the field of application security. Furthermore, it has previously been utilized in the classroom, as a tool for testing the efficiency of a hacking tool and a security defense.
* It is rich with content, covering a wide array of attacks and defenses and containing more than 100 challenges as of version 16.0.
* It is easy to use, offering detailed documentation, presentation, and video material to aid with its use and a companion guide which details each challenge and its solution.
* It is built on a modern and recognized technological stack (Angular, Node.js, SQLite).
* It is a fully functioning web shop, offering browsing and shopping functionalities similar to applications which most trainees build in introductory software engineering courses.

# Assignments

The OWASP Juice Shop has a companion guide ([online version](https://pwning.owasp-juice.shop/companion-guide/latest/), [free book](https://leanpub.com/juice-shop)) which details each of the challenges, providing both hints and solutions to the challenge. To select the appropriate subset of the challenges, a few things should be kept in mind:

* How familiar the trainees are with specific classes of attacks and defenses, to avoid assigning challenges which are too easy or too foreign.
* The difficulty of the challenges, which ranges from 1 to 6, where a single level 6 challenge can take up to an hour or two, while all level 1 challenges can be solved within an hour.
* The significance of the exploit, in relation to new real-world attacks.

## Defense Analysis

As the OWASP Juice Shop offers a platform for conducting attacks and does not offer much in terms of defenses, the trainees need to note and discuss the following points for each class of attacks:

* Explain the class of attacks;
* What is the greatest impact of a successful exploit of the given class;
* Which vulnerabilities in the software allowed the attack to succeed;
* What are the appropriate countermeasures (the more details the better) to prevent the attack.

Three of the challenges are mandatory for every team to solve (all the challenges are enumerated here: [localhost:3000/#/score-board](http://localhost:3000/#/score-board)):

* Find out what the password for the admin account is
* Bypass the CAPTCHA automation protection
* Find the easter egg and download it

Every student from the team should choose five additional challenges from different attack classes.