# HERA LAB

## LAB 2: CSRF LABS

### LAB 2 <#CODENAME: PAWN OWN SHOP!>

WAPTX

eLearn Security
AN INE COMPANY

# CSRF Labs will contain 5 challenging labs:

1. **Warm-up:** CSRF level 1
2. **Easy**: CSRF level 2
3. **Easy**: CSRF level 3
4. **Medium:** CSRF level 4
5. **Hard:** CSRF level 5

# 1. DESCRIPTION

You are a *soft-administrator* of the ***Pawn Own Shop!*** and have decided to add your friend Malice to the administrator list.

However, you cannot do this because only Mrs. Gallegos can do it.

You must find a way to add your friend.

| | |
|---|---|
| **Name** | Malice |
| **Surname** | Smith |
| **Email** | malice@hacker.site |
| **Role** | ADMIN |

**FYI:** each level in Pawn Own Shop! is vulnerable to Cross-Site Request Forgery. Here is some other useful information:

To study the web application here is your login:

**username**: *Padawan*
**password**: *TheLittlePadawan*

**NOTE**: Mrs. Gallegos is always visiting your site: `hacker.site`. In case you don't remember the IP address of your box, it is: 10.100.13.33 and your SSH login is:

**username**: *r00t*
**password**: *Don't worry be happy*

The solutions you will see are just a few of the many you can have. As a suggestion, once you will finish these labs, you can try to solve them again using your way and alternative techniques.

All the solution files are located here:
`http://info.csrf.labs/solutions/`

# 2. Goal

The main goal of these labs is to create valid PoC to exploit CSRF flaws.

You'll initially need simple techniques; later, you will need advanced techniques that require you to code something that automates the brute-force of Anti-CSRF tokens.

# 3. Tool

The best tool is, as usual, your **brain**. You may also need:

- Web Browser
- HTTP Proxy
- The `hacker.site` server web

# 4. SOLUTIONS

The techniques used during this lab are better explained in the study material. You should refer to it for further details.

***NOTE: This is also a video-lab, so you can also watch the video for a complete explanation of what to do! To view, go to the course in your Members Area, find Module 5 and select the video from the resources drop-down menu.***

The solution files are available at http://info.csrf.labs/solutions/. These solutions are provided here only to verify the correctness.