Assignment 3: Due 16 May 2023 (23:59)
Web security

Universiteit Leiden
The Netherlands

Security

Motivation

In this assignment you get to exploit websites in order to obtain hidden secrets (flags).

Task

You are provided with 10 challenges. Complete as many of these challenges as you can by **finding** and **submitting** the flag for each challenge. Creative thinking and trial & error are your friends for this assignment.

Tip: Given you will have to submit a pdf containing for each challenge, the flag you obtained and how you solved it, we suggest you document your steps each time you manage to hack a challenge.

Connection instructions

1. Before connecting, enrol in a **group** (WebSec) on Brightspace. You may either solve this assignment individually or in pairs.
2. In order to connect to the environment of this assignment you need to set-up a proxy over `ssh` with the LIACS gateway. To do this, run:

   ```
   ssh -D port studentid@ssh.liacs.nl
   ```

   In the above command replace `port` and `studentid` with a port of your choice in the range $1024 - 65535$, respectively with your student id.
3. In `Firefox`:
   (a) Go to *Settings*.
   (b) Search *Network settings*.
   (c) In the Network settings choose *manual proxy configuration*.
   (d) In the manual proxy configuration choose *localhost* as *SOCKS host*.
   (e) In the *port* choose the `port` you picked when creating the proxy over `ssh`.
4. To access the environment, go to: `http://132.229.44.138:8000/`
   Once there, you can successfully enter the website of the final assignment:
   (a) Create an account, using your student email.
   Attention! For the password field, **do not** use a password you commonly use or use for a different service, and make sure to remember it because once lost it cannot be recovered.
   (b) Create (or join) a team, where the name of the team is the same as the name of your **group** in Brightspace.

Submission

You need to submit a single **pdf** report that describes for each challenge: the challenge number, how you have hacked the challenge and the flag you obtained.

Requirements for your assignment submission (use it as a checklist):

- ☐ Submission is a **pdf** file titled with your group number (e.g., `groupY.pdf`).
- ☐ Report is in English.
- ☐ Report includes your name(s) and your student ID(s).
- ☐ We prefer you are brief yet still describe all necessary steps.

Policy

- Only access servers over HTTP on the port we provide.
- Do not overload the machine.
- Do not use automated tools and/or vulnerability scanners that can cause heavy network loads e.g., nmap, sqlmap.
- Do not share your solutions with others in any way.
- We may permanently disable your account and change your final grade (up to issuing no grade for this assignment) in case of deliberate offences, especially if they hinder work of other students.
- Deliberate attacks to anything but the provided websites will be reported to the Examination Board and may result into punishments much more serious than a missing course grade.

Evaluation criteria

This project will be evaluated on the following components:

- Concise, typo-free and clear report.
- The number of levels beaten fairly.

The grading system can be revised, based on the average performance of the class.