Web Security and Malware Analysis

Assignment 1 – 29/10/2020

Goal: Solve each task by providing a brief explanation of the solution that you adopted. Explanations should mainly include screenshots and some brief comments. Use the provided template to write your assignment. You must use BURP to solve the tasks (when required).

What to do: Save the Assignment as PDF and submit it to the E-Learning platform (**Section: Assignment 1**). The file should be named as follows: **"websec_report_1_name_surname.pdf".** Remember to include your name, surname and matriculation number in your report.

Task 1 - Spidering

Perform a web spidering of the following web application:

http://zero.webappsecurity.com/

To log in, you can use the following credentials:

user: **username**

password: **password**

Report all the useful information that you can find, such as:

- Pages found automatically (you must use BURP);
- Pages not found automatically (if any – specify why it is difficult to find them automatically).

Task 2 – Basic Web Hacking

Complete the levels of the Natas wargame until **Natas 5 (included)** by using BURP to manipulate requests (when needed). By solving each level, you obtain a password to proceed to the next one.

The wargame starts here:
http://natas0.natas.labs.overthewire.org/

User: **natas0**

Pass: **natas0**

To access the next level, just go to the corresponding URL.

For example, for natas1:

http://natas1.natas.labs.overthewire.org/

User: **natas1**

Pass: **PASSWORD_FOUND_IN_NATAS0**

The goal of the task is to briefly describe the solution for each level (some screenshots + brief description of the solution is enough).

Hints that may be useful:

Passwords are hidden in the webserver under the folder /etc/natas_webpass/natas_level (e.g. password for natas1 is stored in /etc/natas_webpass/natas1 - this may be useful for some levels)

Task 3 – Mangling Requests/Responses

Your goal is finding a secret flag (password) by analysing the following Web Application:

https://jupiter.challenges.picoctf.org/problem/28921/

The flag has the format **picoCTF{…}** (with some text between the brackets).

Hints: Use **BURP** to intercept requests and responses. Maybe some manipulation is required…