Web Security and Malware Analysis

Assignment 2 – 12/11/2020

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. Remember that solving the Bonus task is not compulsory (it is proposed only for those who are interested).

What to do: Save the Assignment as PDF and submit it to the E-Learning platform (**Section: Assignment 2**). The file should be named as follows: **"websec_report_2_name_surname.pdf".** Remember to include your name, surname and matriculation number in your report.

Task 1 – PHP Reading

Consider the PHP code contained in the file **task_1.php** and answer the following questions:

1. What does the code do? Explain it with precision by referring to code lines. You can use groups of code lines to represent similar instructions. E.g., "lines 7-11 do X, lines 13-21 do Y", etc.
2. What is the role of superglobal variables in the code?
3. **preg_match** is a very important function in PHP. Can you explain what the regular expressions in lines 37-39 do?

As a side note, you will find some instructions and commands that are not contained in the slides. This is done on purpose to make you navigate the PHP documentation. Feel also free to test the code on a sandbox to see how it works.

Task 2 – More NATAS

Solve **NATAS levels 6-8 (included)**. To do so, you must first complete levels 1-5 in Assignment 1.

Focus in particular on describing the actions performed by the PHP code in level 8.

For level 7, check this out: https://owasp.org/www-community/attacks/Path_Traversal

Task 3 – HTTP Requests and Sessions

Find the flag (i.e., manage to authenticate) on this page:

https://exercise-2.0x00sec.dev/

Use BURP to solve the task. This link may also be useful:

https://base64.guru/learn/what-is-base64

After solving the challenge, explain in your answer what is the vulnerability here and why the session insecure.

Bonus Task – Requests/Responses with Python

While Burp is an excellent tool for intercepting requests and responses, Python can be really useful to easily manipulate requests and responses, thus providing similar functionalities to BURP Repeater.

Your goal is solving task 3 of Assignments 1 and 2 by employing only Python 3 to generate requests and to visualize responses (you can try using **urllib3**). Provide a code snippet (directly on the assignment PDF, a screenshot is also fine) of your solutions.