Web Security and Malware Analysis

Assignment 4 – 10/12/2020

Goal: Solve each task by providing a brief explanation of the solution that you adopted. Answers 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 interested people).

What to do: Save the Assignment as a PDF and submit it to the E-Learning platform (**Section: Assignment 4**). The file should be named as follows: **"websec_report_4_name_surname.pdf".** Remember to include your name, surname, and matriculation number in your report.

Starting Notes: Most of this assignment's tasks will concern attacking the Damn Vulnerable Web Application (DVWA).

You can download the Virtual Machine of the course to execute DVWA - https://hub.docker.com/r/vulnerables/web-dvwa (or you can download it directly from Docker).

To run the DVWA:

docker run --rm -it -p 80:80 vulnerables/web-dvwa

Then open the browser and give localhost:80 in the URL bar.

You will be asked to solve tasks by changing their difficulty progressively. To change it, go to DVWA and select the difficulty by clicking on DVWA Security on the menu (you will be asked to solve tasks from low to high).

Task 1 – SQL Injection

Solve the **SQL Injection** tasks of the DVWA at the low, medium, and high difficulties. The final goal is retrieving **and decrypting** all the credentials belonging to the users. In particular, you also have to report the following aspects:

1. The names of the databases;
2. The names of the tables for the database related to the vulnerable web application;
3. The names of the fields for the table related to the user's credentials;
4. The technique you used to decrypt the credentials (hint: check the previous slides about authentication).

Task 2 – Command Injection

The task is composed of two parts:

1. Complete the **Command Injection** tasks of the DVWA at low, medium, and high difficulty. The goal is printing the /etc/passwd file stored in the server (with the command **cat /etc/passwd**).

2. Solve NATAS levels 9 and 10. Use the credentials obtained from the last level solved in the first assignment to access http://natas9.natas.labs.overthewire.org

Remember that the password for the next levels are stored in:
/etc/natas_webpass/natas10 (for level 9)
/etc/natas_webpass/natas11 (for level 10)

Task 3 – PHP and Cookie Encryption

Consider the PHP code of Natas level 11 (solve task 2 first to obtain the credentials).

You are required to describe the following accurately:

1. The functionality of each function of the code.
2. How the cookie is encrypted.
3. Why the employed encryption is weak and how you can crack it. What kind of decryption function is required?

Finally, try to solve Natas 11 and provide the password for the next level.

Bonus Task – Server-Side Template Injection (SSTI)

Another injection vulnerability affects templates, i.e., basic web app structures that can be easily modified with the user's input. You can exploit this vulnerability to trigger remote code execution. You can read the basics about SSTI from here:

https://portswigger.net/web-security/server-side-template-injection

Your task is solving the challenge at this link:

https://2019shell1.picoctf.com/problem/32252/

The flag format is picoCTF{…}