Web Security and Malware Analysis

Assignment 3 – 05/12/2019

Goal: Solve each task by providing a brief explanation of the solution that you adopted. You must use BURP or one of the indicated tools to solve the tasks (when required). Explanations should mainly include screenshots and some brief comments.

Note: Although you may find the solutions to many of the proposed tasks on the web, *try to solve them on your own and do not immediately give up*. This training will be very useful for the practical question that will be asked during the exam. Also, remember to give **brief written** answers (avoid copy-and-paste from other tutorials and try to write your own answers) and to use screenshots to describe what you do. You are also recommended not to use copy-and-paste texts from tutorials, but to use your own words.

Deadline: Dec. 23th,2019

What to do: Send the report in the PDF format to davide.maiorca@unica.it with the subject "[WEBSEC] - Report For Assignment 3 – NAME SURNAME" and name the file "websec_report_3_name_surname.pdf". Remember to include your name, surname, and matriculation number in your report!

Starting Notes: most of the tasks of this assignment will be done by attacking the Damn Vulnerable Web Application (DVWA). To access the machine, you have to follow these steps:

1. Connect to https://app.cyberranges.com/
2. Create an account
3. Click on "Play," log in with your account
    a. Click on "Library," then "Category," then "Web."

   b. Select DVWA-SQLi (Error) #1, then load the Virtual Machine
   c. Click on VPN and download the related VPN file (it should have a .ovpn extension)
4. You have to open this file with OpenVPN. If you do not have it, download it from https://openvpn.net/community-downloads/ and install it.
5. In Windows, open the command prompt *with administrator privileges* (VERY IMPORTANT, otherwise the VPN will not work).
6. If you installed in the default path, give this command: **"C:\Program Files\OpenVPN\bin\openvpn.exe" "your_ovpn_path"**
7. If the VPN is working, you should get the message "Initialization Sequence Completed."
8. With the VPN working and the virtual machine started in app.cyberranges, connect to http://192.168.125.150/dvwa/, and put as username: "admin" and as a password: "password."

Note that the virtual machine will be reset after 1-2 hours, so you have to reload it again from the Cyberranges web app.

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

You have to solve the SQL Injection tasks at the low, medium and high difficulty of the Damn Vulnerable Web Application. 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).

Use BURP to intercept and send the attacks. Finally, discuss the differences between the server-side codes at the three difficulty levels.

Task 2 – Command Injection

The task is made of two points:

1. Complete the "Command Injection" tasks at low, medium, and high difficulty. The goal is printing the /etc/passwd file stored in the server (with the command **cat /etc/passwd**). Additionally, explain how the blacklisted characters evolved.

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) and /etc/natas_webpass/natas11 (for level 10)

Task 3 –PHP Analysis

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.

Note: you can very easily solve this task by checking its solution online. However, remember that this is not the goal of the task. You should spend quite some time thinking about the structure of the code and about the related security issues. Remember that the practical question of the final exam will be similar, in terms of structure, to this one.