Web Security and Malware Analysis

Assignment 2 – 28/11/2019

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. 10th,2019

What to do: Send the report in the PDF format to davide.maiorca@unica.it with the subject "[WEBSEC] - Report For Assignment 2 – NAME SURNAME" and name the file "websec_report_2_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-Brute-Force #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 – Brute-Force

Attack the Brute-Force section of the web application at each difficulty level (except for impossible).

For each level, you have to retrieve the passwords for the following users:

pablo

admin

1337

gordonb

smithy

The task is divided into two subtasks:

1. **Easy and Medium levels:**

You have to complete the tasks at each difficulty by using **BURP Turbo Intruder** (download it from Burp Extender) **and** one of the tools between **WFUZZ** and **Hydra** (you can choose). Besides completing the task, discuss the server-side actions of the PHP code.

For a tutorial on Turbo Intruder, check:

https://portswigger.net/research/turbo-intruder-embracing-the-billion-request-attack

For good password sets, check:

https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

2. **High level:**

To solve the task, carefully read this tutorial:

https://blog.g0tmi1k.com/dvwa/bruteforce-high/

The best way possible to solve the task is by using the **patator** tool: https://github.com/lanjelot/patator. However, the tool would require Linux to work at its best. A Windows version is also available at https://github.com/maaaaz/patator-windows, but it seems to create some problems.

By following the previous tutorial, you can also use **BURP+Intruder (careful: Turbo Intruder will not work)**. However, the tool is significantly slower.

Hence:

A. If you use Linux+Patator, provide the passwords **for all the users.**
B. If you use Burp+Intruder, provide the passwords for the users **admin, smithy, and pablo**.

Additionally, briefly answer the following questions:

- What are the main actions of the code?
- What makes the High level significantly more complicated than the previous two?
- What is, in your opinion, the major weakness of this defense system? How would you improve it?

Task 2 – Attacks against Sessions

Complete the “Weak Session IDs” tasks at low, medium, and high difficulty. The goal of these tasks is understanding how the *dvwaSession* cookie is generated in the server response. You are required to answer the following questions:

- Try to solve each task *without looking at the PHP source code*. What can be inferred by only observing the server response to the generated requests? How is the cookie created? **Hint**: Use BURP repeater.

- Use BURP Sequencer (tutorial: https://portswigger.net/burp/documentation/desktop/tools/sequencer) to launch multiple requests at medium and high difficulty. What can we say in terms of the predictability of the cookie? How are the plots related to the characteristics of the cookie?

Task 3 – More PHP

Note: especially for question number 3, there is not only one “right” answer. Try to use your creativity.

Given the following PHP code, answer the following questions:

1. What does the PHP code do?
2. Is this code vulnerable? If yes, describe how you would crack it.
3. How would you enforce the security of the code?

```
<?php

    $user = mysql_real_escape_string($user);

    $query = "SELECT hash FROM users WHERE username='$user';";

    $result = mysql_query($query) or die('Query failed: ' .
mysql_error());

    $line = mysql_fetch_row($result, MYSQL_ASSOC);

    $hash = $line['hash'];


    if (strlen($pass) != strlen($hash))

        return False;


    $index = 0;

    while($hash[$index]){

        if ($pass[$index] != $hash[$index])
```

```
            return false;
        usleep(300000);
        $index+=1;
    }
    return true;
?>
```