Web Security and Malware Analysis

Assignment 5 – 17/12/2020

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 5**). The file should be named as follows: **"websec_report_5_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 – Reflected XSS

You have to solve the Reflected XSS tasks of the DVWA at the low, medium, and high difficulty levels. The final goal is stealing your own session cookie and intercepting it using a Webhook. As a webhook, you can use this service: https://requestcatcher.com

To bypass filters, you can check these payloads:

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection#xss-in-htmlapplications

For the high level, the payload will be a bit different. You will need the concept of the **document.location** property (google it).

Task 2 – Stored XSS

You have to solve the Stored XSS tasks of the DVWA at the low, medium, and high difficulty levels. The final goal is to redirect the user to the page https://www.unica.it. Solve this task after Reflected XSS, use all you learned. Once you complete every difficulty level, remember to reset the VM.

Bonus Task – What did you learn?

Consider the same web application proposed in the first assignment: http://zero.webappsecurity.com/

This time, your goal is to perform a complete analysis of the web app and find all possible vulnerabilities, according to what you learned during the course. Can you exploit at least one of these vulnerabilities?

You can use these credentials to log in as a generic user:

user: **username**

password: **password**