STI 2021/2022

Practical Assignment #3

1. Goals

- Explore the WSTG (Web Security Testing Guide) web security testing guidelines
- Configure and explore the usage of ModSecurity reverse proxy as a WAF (Web Application Firewall)

2. General description

The main goals of this assignment are to explore **web application security** and to implement a **web application firewall** to secure a web application against application-layer attacks. The web application to be used in this assignment is the OWASP JuiceShop[1] [2]. This assignment is split in two phases: the first phase is dedicated to exploring the JuiceShop security, and the second phase aims at monitor, filter and block HTTP traffic to the JuiceShop through the implementation of a ModSecurity WAF, with the aim to address the security issues identified in the first phase. Figure 1 illustrates the two phases of the assignment, depicting the JuiceShop web server, the penetration testing client and the WAF.

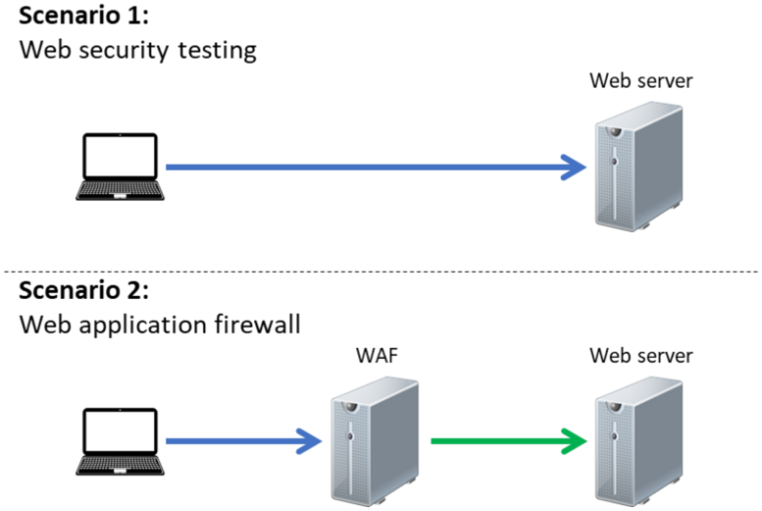

Figure 1 – Security testing and WAF phases of the Assignment

[1] OWASP JuiceShop: https://owasp.org/www-project-juice-shop/

[2] For this assignment, it is recommended to use the most recent version of the JuiceShop. At the time of writing this document it is v13.3.0

3. Phase 1 - Web application security testing

In this phase the goal is to explore web application security using the JuiceShop website following the relevant and applicable WSTG web security testing guidelines, and for this purpose the Kali Linux and OWASP ZAP tools can be used. This web security testing phase is described in Figure 1, where the client has direct communications to the web server. As part of your tests, the OWASP ZAP penetration tests must, at least:

a. Perform an automated scan to the website.
b. Perform an active scan to the website (explore the most effective policies).
c. Manage add-on required to improve the test and maximize threats identification.
d. Perform a Fuzz attack to the login form.
e. Perform a manual penetration test to explore logged in threats.
f. Configure OWASP ZAP active scan to explore authenticated area.

The installation of JuiceShop is left to the decision of the student:

- can be installed through source code in one of the virtual machines
- using docker approach (requires Docker Desktop)

As a result of your tests, you should create a web application security report considering the WSTG guidelines. The report must document the identified vulnerabilities and on how these can be exploited (e.g., weak passwords).

4. Phase 2 - Web application firewall

Based on the web application security report produced in the first phase of the assignment, deploy an WAF between the client and the web server, as depicted in Figure 1. The goals of this WAF are to monitor, filter, and block HTTP traffic to the Juice Shop. This WAF server should be composed of an Apache 2 service with ModSecurity, and the WAF configuration should be optimized to prevent all possible attacks.

As a result of this phase of the Assignment, you should repeat all penetration tests performed in the previous task, assess the WAF performance and update the web application security report accordingly, by including the configurations, description of the tests and performance results in a separate section.

5. Delivery of the Practical Assignment

For the delivery of the assignment, you should include all the reports elaborated in both phases. The deadline for the delivery of the assignment (configuration files and report, via Inforestudante) is **May 30 2021**.