Cyber Security Assessment and Management
Bruno Sousa, bmsousa@dei.uc.pt
2024/2025

Worksheet #3 – Security Assessment

Practical Lecture #5

OBJECTIVE:

Understand the process of discovering, analyzing the attack surface in web applications and on the environment where they run. The process can be automated through the utilization of tools like OWASP Attack Surface Detector[1] (ASD) that have several steps pre-prepared for use in attack surface detection.

CONTEXT:

WebGoat[2] is an OWASP project which comprises a deliberately insecure web application, designed to teach web application security lessons. In each lesson, users must demonstrate their understanding of security issues by exploiting a real vulnerability in the WebGoat application.
JuiceShop[3] is an OWASP project that is labelled as the "most modern and sophisticated insecure web application!", which can be used for security, trainings, awareness and others.

SETUP:

WebGoat and JuiceShop can be installed using Docker **OR** using standalone versions which are available for download on the respective websites.

ZAP

Install Zed Attack Proxy (ZAP) on your virtual machine, where you will install the WebGoat and JuiceShop.
The OWASP Attack Surface Detector should be installed on ZAP, check the installation instructions that are available in the official repository[4]. It can be installed using the Add-Ons options in ZAP.

Docker

First install Docker following the steps available at: https://dockr.ly/3DuDnf4. After configuring it, run the following command to start the container and the image will automatically download, if not present.

WebGoat

[1] https://owasp.org/www-project-attack-surface-detector/
[2] https://owasp.org/www-project-webgoat
[3] https://owasp.org/www-project-juice-shop/
[4] https://github.com/secdec/attack-surface-detector-zap

```
$ docker run -p 8080:8080 -p 9090:9090 -p 80:8888 -e
TZ=Europe/Amsterdam webgoat/goatandwolf:latest
```

After the setup process is complete, WebGoat should be available at http://localhost:8080/WebGoat.

Download the source code of webGoat, as it will be required for Attack Surface Detector, the source code is available in the official repository[5].

JuiceShop (optional)

```
$ docker pull bkimminich/juice-shop
$ docker run --rm -p 3000:3000 bkimminich/juice-shop
```

After the setup process is complete, JuiceShop should be available at http://localhost:3000/.

EXERCISES:

1. Download WebGoat source code

Download the source code of webGoat, as it will be required for Attack Surface Detector, the source code is available in the official repository[6] and decompress it to a folder.

At the same time install Attack Surface Detector, which is a tool to analyse source code regarding Attack Surface (possible endpoints of an application).

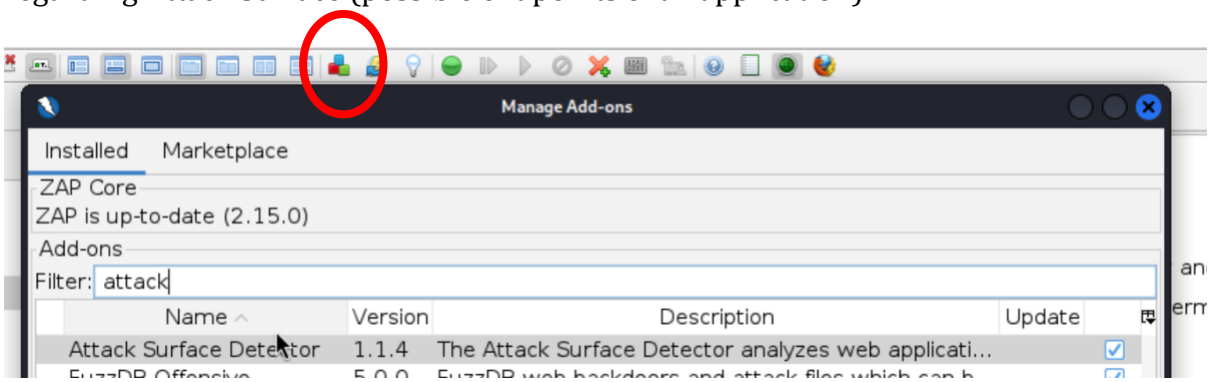

Figure 1 - Installation of Attack Surface Detector

2. Identify the ATTACK SURFACE in WebGoat using ASD

Running ZAP with OWASP Attack Surface Detector plugin. Document the number of endpoints, HTTP methods that can be used in each of the endpoints.

Note you need to activate this functionality in the bar of ZAP.

[5] https://github.com/WebGoat/WebGoat
[6] https://github.com/WebGoat/WebGoat

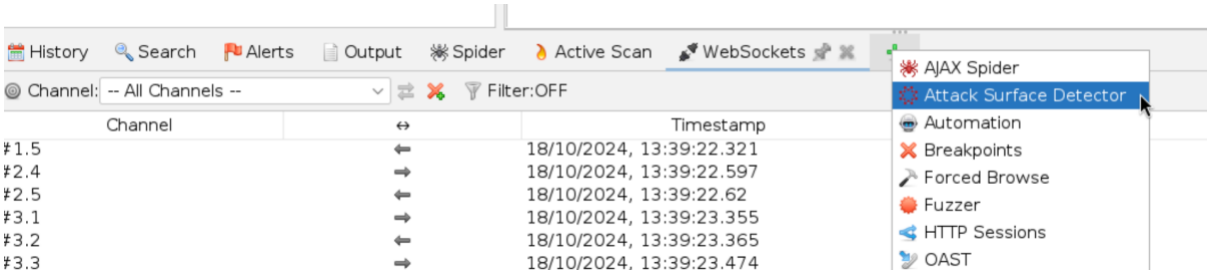

Figure 2 - Activating the Attack Surface Detector

To perform the analysis, choose the "Import Endpoints from Source".

Documentation in Report
Include in the report the number of detected endpoints

2. Identify the ATTACK SURFACE in WebGoat with a Scan from ZAP

Run ZAP an automated scan to identify the endpoints and urls, use the mode ATTACKER MODE. Compare the results with the first step. Are there any differences?

The Attacker mode is available at the top of the ZAP program.

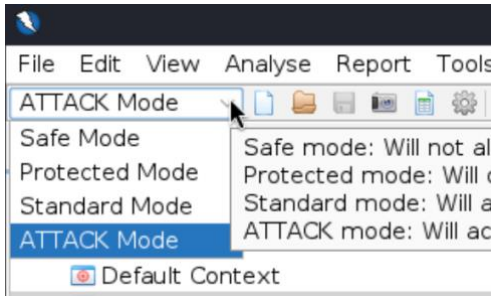

Figure 3 - Availability of ATTACK MODE in ZAP

Documentation in Report
Include the number of endpoints and urls found by the ZAP scan

Answer the following questions:

1. What is the most reliable source for determining the attack surface ? Justify your answer.
2. Which approach would you use to determine the most accurate attack surface ? Justify your answer

3. Identify the ATTACK SURFACE in Environment where the applications run

Use the nmap tool[7] to find the (TCP, UCP) ports that are open in the system, where the applications are running. If you need a GUI tool you can consider in using the Zenmap tool which is included in Kali distribution.

[7] https://nmap.org/

Documentation in Report
Include the number of additional endpoints identified by nmap/Zenmap.
Document the type of test you have used to run the nmap test.

4. ANALYSE THE RESULTS

Documentation in Report
Analyse the results that were identified in the previous steps.
What could you do to reduce the overall attack surface?

You can repeat the steps for the Juice-Shop, but be aware that ASD is not able to analyse the source code of the Juice-Shop.

READINGS:

- OWASP, *"Top 10 Web Application Security Risks"* 2017. Available at: https://owasp.org/www-project-top-ten
- Weidman, Georgia. *"Penetration testing: a hands-on introduction to hacking".* No Starch Press, 2014. [Chapter 14: Web Application Testing]
- Gordon "Fyodor" Lyon, Nmap Network Scanning, 2008, Chapter 4, Chapter 5, available at: https://nmap.org/book/toc.html