Careers in Web app Testing

~ Lalithya Malyala

Myself

- Completed my master's degree in Cybersecurity (May 2020).
- Worked as a graduate teaching assistant in Data Center Security in teaching, grading, and working under university standards.
- Also a member of OWASP local Chapter from January 2020 with a keen interest in practicing Web App sec testing through various platforms.
- Possess two years of work experience in Quality Assurance (QA)/Software testing.

Agenda

- The main agenda of this presentation is to Introduce you to our Webgoat
- If you are a beginner – Well, just like me you will love webgoat once you start
- If you are an Industry Professional – Explore!! Webgoat is challenging you to have fun hacking.

This program is a demonstration of common server-side application flaws. The exercises are intended to be used by people to learn about application security and penetration testing techniques.

Introducing Webgoat

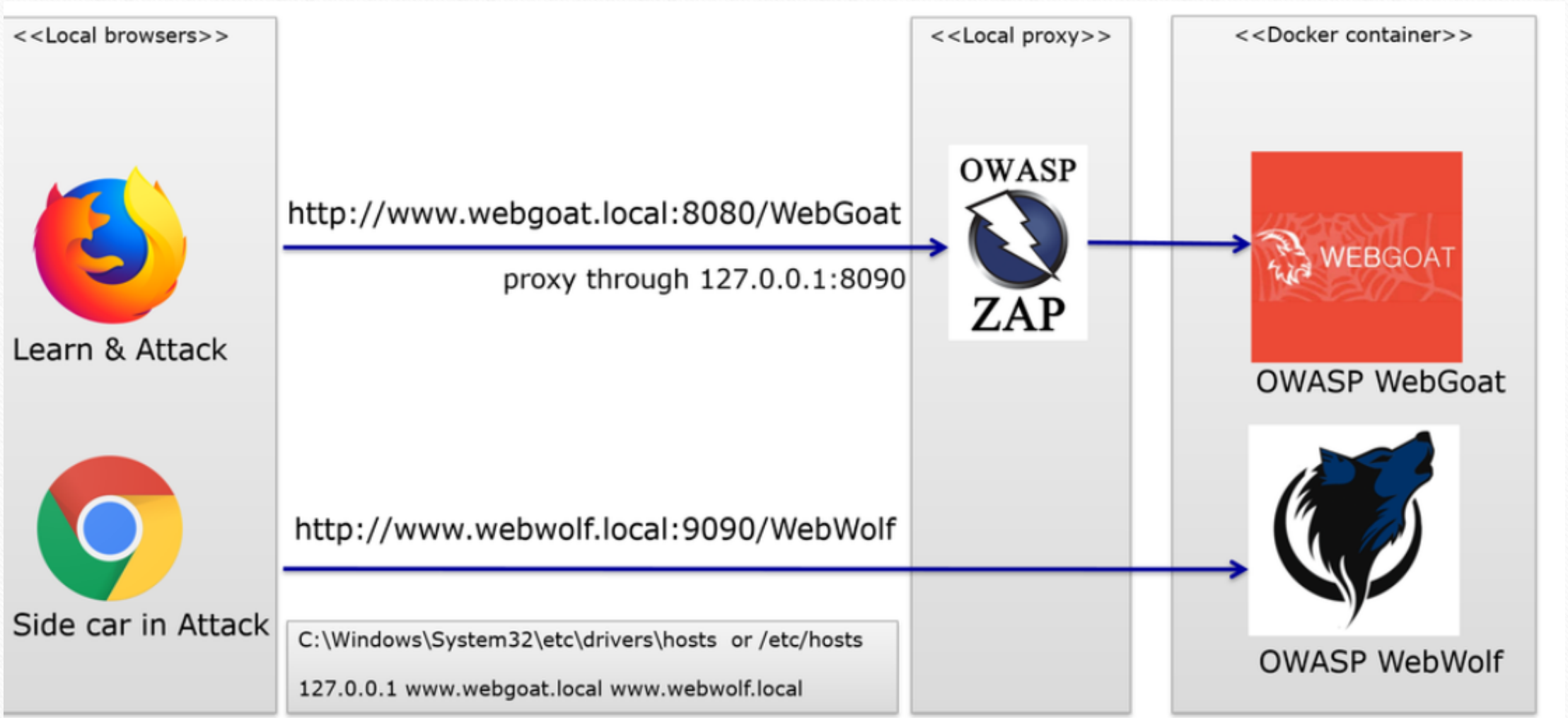
- It's a deliberately insecure web application designed for teaching/learning about web application security.
- Developed and Maintained by OWASP to learn and practice web security concepts of OWASP Top 10 Vulnerabilities.
- I found Web Security to be a topic where many people struggle.

What you need?

- Webgoat is a J2EE web application runs as a web application on the Apache Tomcat web server in the background – Download the jar from Github.
- So you need to have Java on your side.
- And a Proxy – OWASP ZAP, Burpsuite etc.
- WebWolf is an other web application that depends on WebGoat and requires that WebGoat is started first (Hosting a file, Receiving email, Landing page for incoming requests).

Don’ts!!

- Do not operate webgoat on an externally visible IP, it is vulnerable to attack.
- Do not even operate WebGoat on a reserved IP Subnet, always use local host.
- While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.


<<Local browsers>>
Learn & Attack
Side car in Attack
http://www.webgoat.local:8080/WebGoat
proxy through 127.0.0.1:8090
http://www.webwolf.local:9090/WebWolf
C:\Windows\System32\etc\drivers\hosts or /etc/hosts
127.0.0.1 www.webgoat.local www.webwolf.local
<<Local proxy>>
OWASP
ZAP
<<Docker container>>
WEBGOAT
OWASP WebGoat
OWASP WebWolf

Let’s have a quick look

Summary

- Explore as many vulnerabilities as you can and keep practising.
- I hope that you practise web app testing through these available platforms like webgoat and also through OWASP Juice.

Thank you!!