Tonny Mutumba

HomeWork 4

**Abstraction/Executive Summary**

For this assignment we were required to break into a vulnerable web application. Use WebGoat from OWASP as the vulnerable web application.

**Introduction/Method**

To run webgoat, I needed a container in which it would be put and docker was the container of my choice. Made the necessary downloads and installed them.

<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

<https://store.docker.com/editions/community/docker-ce-desktop-mac>

docker run -p 8080:8080 webgoat/webgoat-7.1

A drawing of a cartoon character

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Then after opened up fire fox configured the proxy as instructed in the powerpoint

A screenshot of a cell phone

Description automatically generated

Fired up zap configured the proxies for that too

A screenshot of a cell phone

Description automatically generated

With all configurations done I ran webgoat server and it listened to <http://localhost:8080/WebGoat> logged in as a guest went to the numeric SQL injection executed the SQL command selecting local weather station as Columbia. Navigated through ZAP got the post broke it and ran it again. And as expected ZAP stopped the submission

A screenshot of a social media post

Description automatically generated

**Result**

As for the result I edited and submitted the SQL command in ZAP and hit play twice, then I got the required results.

A screenshot of a social media post

Description automatically generated

**Conclusion**

If this how easy it is to break into a web application, then we have a lot to do as computer programmers. Hopefully as I advance in this profession, I can get better at noticing this kind of vulnerabilities in my applications.

**Reference**/s:

Class notes