

## Abstraction/Executive Summary

This assignment was all about how to break into the vulnerable web applications using a Web Goat from OWASP.

In order to break the sites we need three things.

1. Docker
2. OWASPZAP
3. WebGoat vulnerable site via Firefox.

**Steps I took:** hence I don't have all of the above in my machine I have to install all of them.

**First** I installed docker in my machine using Homebrew.

```
To have launchd start docker-machine now and restart at login:
brew services start docker-machine
Or, if you don't want/need a background service you can just run:
docker-machine start
```

==> Summary

```
🍺 /usr/local/Cellar/docker-machine/0.15.0: 11 files, 32.2MB
```

In order to verify whether Docker is installed in your machine you can run the ff commands

```
Abinets-MacBook-Pro:~ abiken$ docker --version
```

```
Docker version 18.03.0-ce, build 0520e24
```

```
Abinets-MacBook-Pro:~ abiken$ docker-compose --version
```

```
docker-compose version 1.20.1, build 5d8c71b
```

```
Abinets-MacBook-Pro:~ abiken$ docker-machine --version
```

```
docker-machine version 0.15.0, build b48dc28
```

```
Abinets-MacBook-Pro:~ abiken$
```

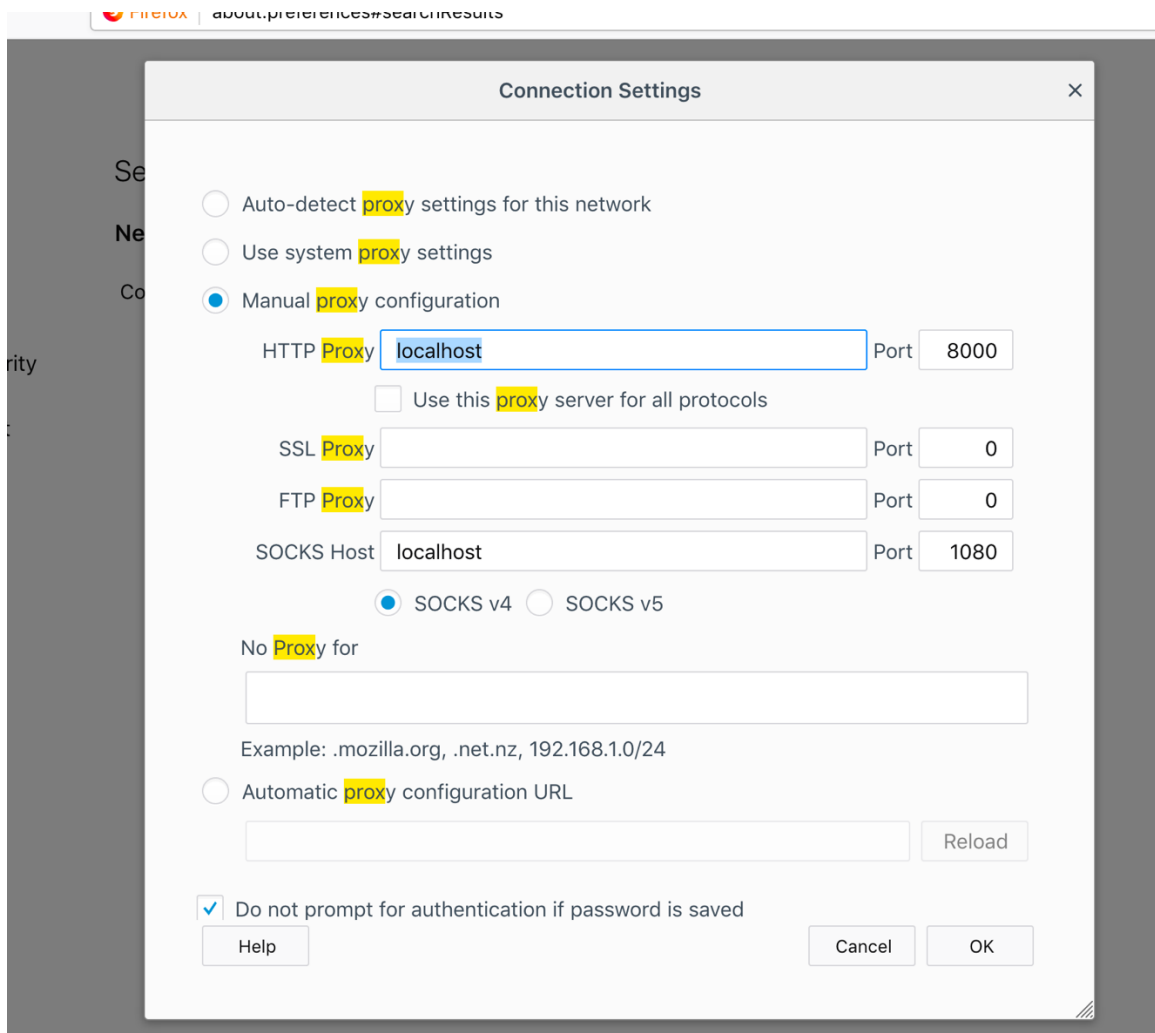
**Second** I installed OWASP ZAP the OWASP Zed Attack Proxy Project website and I followed the download instruction. I also downloaded Firefox as well.

## Method

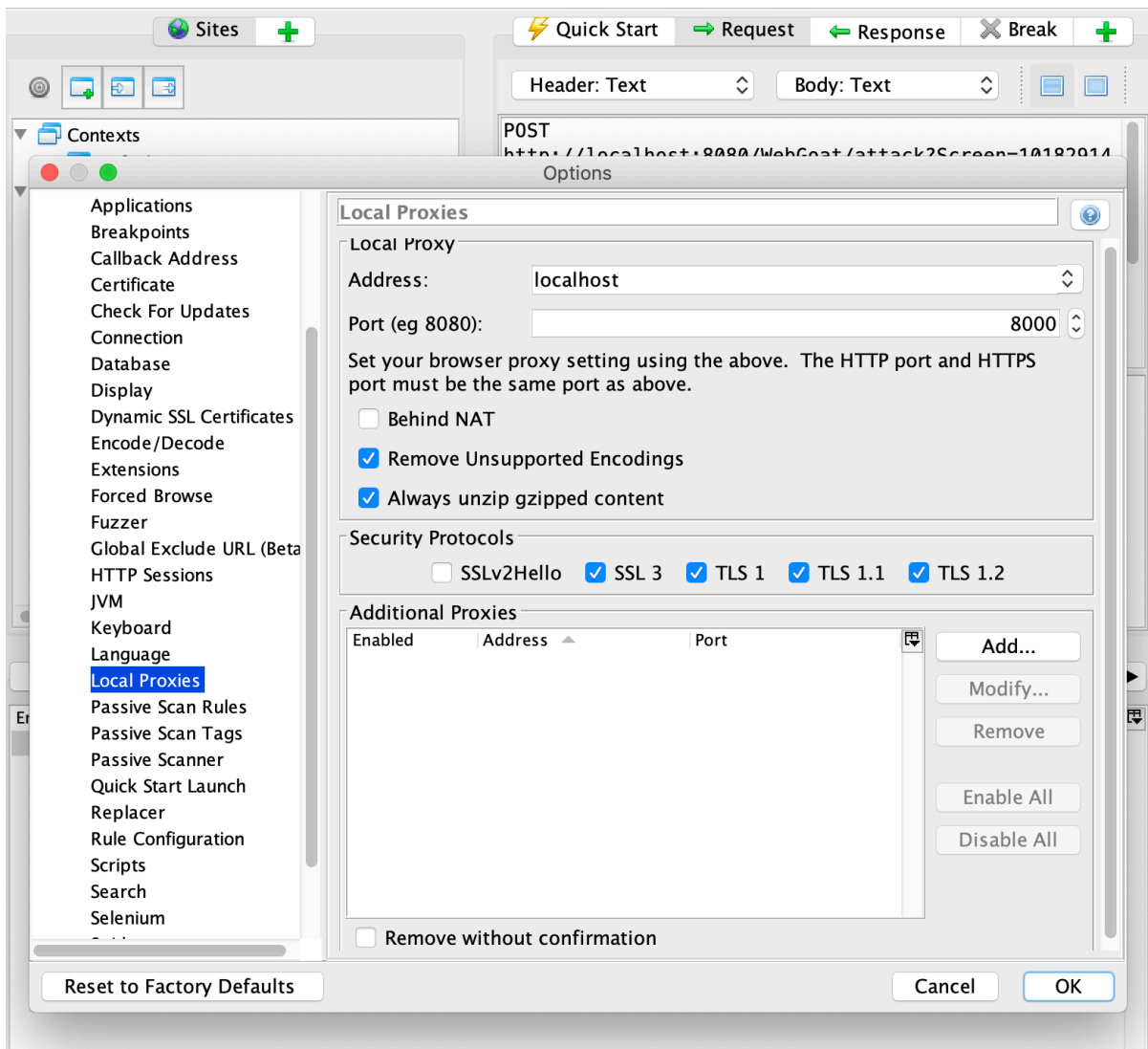
To run webgoat, I needed a container in which it would be put and thus why docker was needed to be installed first. Then

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

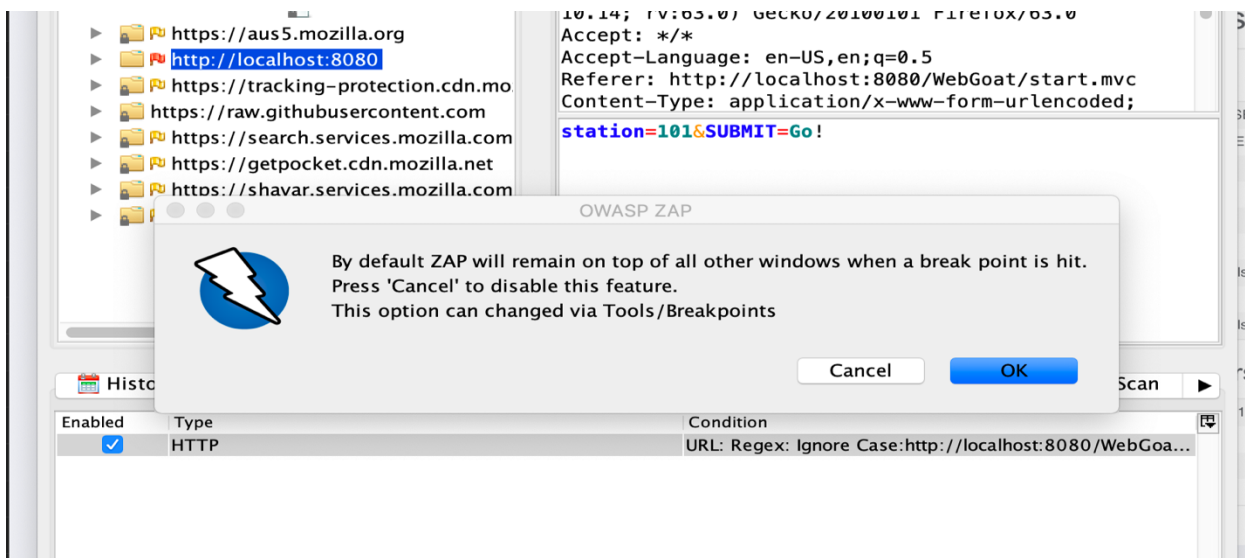
Then after I opened up fire fox configured the proxy as instructed in the PowerPoint from class Lecture



After I configured up the proxy, I fired up zap configured the proxies too. The following screenshot shows what it looks like when you fire up zap.



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



## Result

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

The screenshot shows the WebGoat application interface. On the left is a navigation menu with various security topics. The main content area displays a lesson titled "Congratulations. You have successfully completed this lesson." It explains SQL injection attacks and provides a "General Goal(s)" section. Below this, there is a form to select a local weather station (currently set to "Columbia") and a "Go!" button. A text input field contains the SQL command: `SELECT * FROM weather_data WHERE station = 101 OR 1 = 1`. Below the input field, a table displays the resulting weather data:

STATION	NAME	STATE	MIN_TEMP	MAX_TEMP
101	Columbia	MD	-10	102
102	Seattle	WA	-15	90
103	New York	NY	-10	110
104	Houston	TX	20	120
10001	Camp David	MD	-10	100
11001	Ice Station Zebra	NA	-60	30

On the right side of the interface, there is a "Cookies / Parameters" panel. It shows a single cookie named "JSESSIONID" with a value of "BE69BC718440C3E0CD623997D813A26A". Below the cookies, there is a "Parameters" section with fields for "scr" (101829144), "menu" (1100), "stage", and "num".

The take away from this Homework for me is that how to get around to mess around with the vulnerable sites using necessary tools.

## My concern:

If this how easy it is to break into a web sites in realty, then I have to learn a lot as computer programmers in order to keep the sites not breakable easily or the other way around. More needs to be Done to make the world Better.

## References

### Online

<https://docs.docker.com/docker-for-mac/#proxies>

[https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)

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

[Dr Beaty's PowerPoints.](#)