Graphical user interface, text

Description automatically generated

For this assignment, I decided to run ZAP using Kali Linux via Oracle VirtualBox. Here are the vulnerabilities that I was able to find:

Without even utilizing zap, I found this vulnerability. Email addresses of those who leave reviews should not be displayed publicly.

Graphical user interface, application, chat or text message

Description automatically generated

And, it seems there should be more validation when it comes to review text. This looks like an attempt and a JavaScript injection.

Text

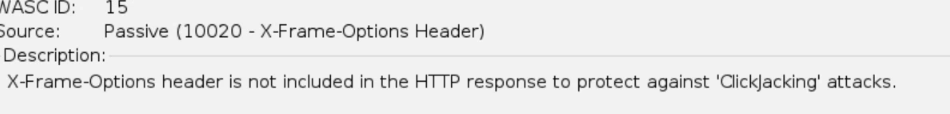
Description automatically generated

Graphical user interface, text, application

Description automatically generated

The version of jquery is outdated, leaving it susceptible to known vulnerabilities.

I don’t fully understand ‘Clickjacking’, or ‘cross domain configuration’, but I found these vulnerabilities as well.



Graphical user interface, text, application, email

Description automatically generated

Merely how quickly ZAP was able to point out vulnerabilities was impressive, and somewhat terrifying.