# CS 305 Module Two Coding Assignment

Alexander Freeders

## Run Dependency Check

A screenshot of a checklist

AI-generated content may be incorrect.

## Document Results

A screenshot of a computer

AI-generated content may be incorrect.

## Analyze Results

Looking at the results of the dependency check, there are several portions that stand out immediately. There are 9 dependencies that have critical severities, 7 of which have a known exploited vulnerability; all of these come with the highest confidence level. These dependencies are all apache tomcat and spring framework. For example, one of the identified vulnerabilities with the aforement ioned apache tomcat was the following :

A black text on a white background

AI-generated content may be incorrect.

Having these connections potentially available to a malicious actor is not something that developers should take lightly! The recommendation for this issue is to block the vector that permits returning arbitrary files and execution. For this example and simply in general, it is paramount to ensure that remaining up-to-date is a top priority, as patches frequently fix issues which could be catastrophic.

Another example of a known exploited vulnerability from the report is that of the HTTP/2 Rapid Reset Attack. Essentially, there is a known vulnerability with HTTP/2 that allows for a DDoS attack, the recommended action for this vulnerability is apply vendor-specific mitigations. If none exist, cease using this protocol.

It can also be important to turn on a false positive filter in dependency check tool. This allows developers to be able to focus on the real threats and vulnerabilities, while maintaining resource efficiency and stopping and unnecessary changes to the codebase as well. Moreover, it is a morale boost to see a much lower number of *real* threats that can be focused on, rather than being flooded by alarms which are false positives in the first place.