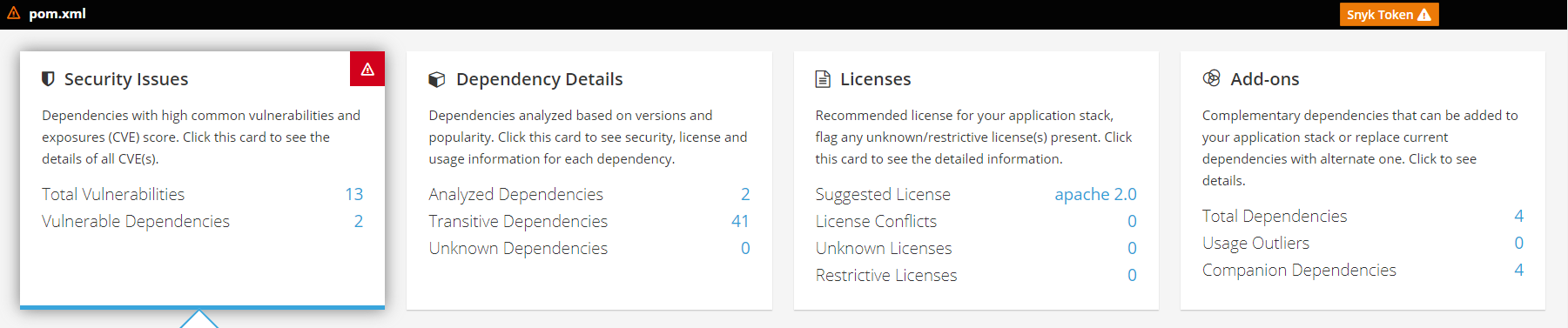
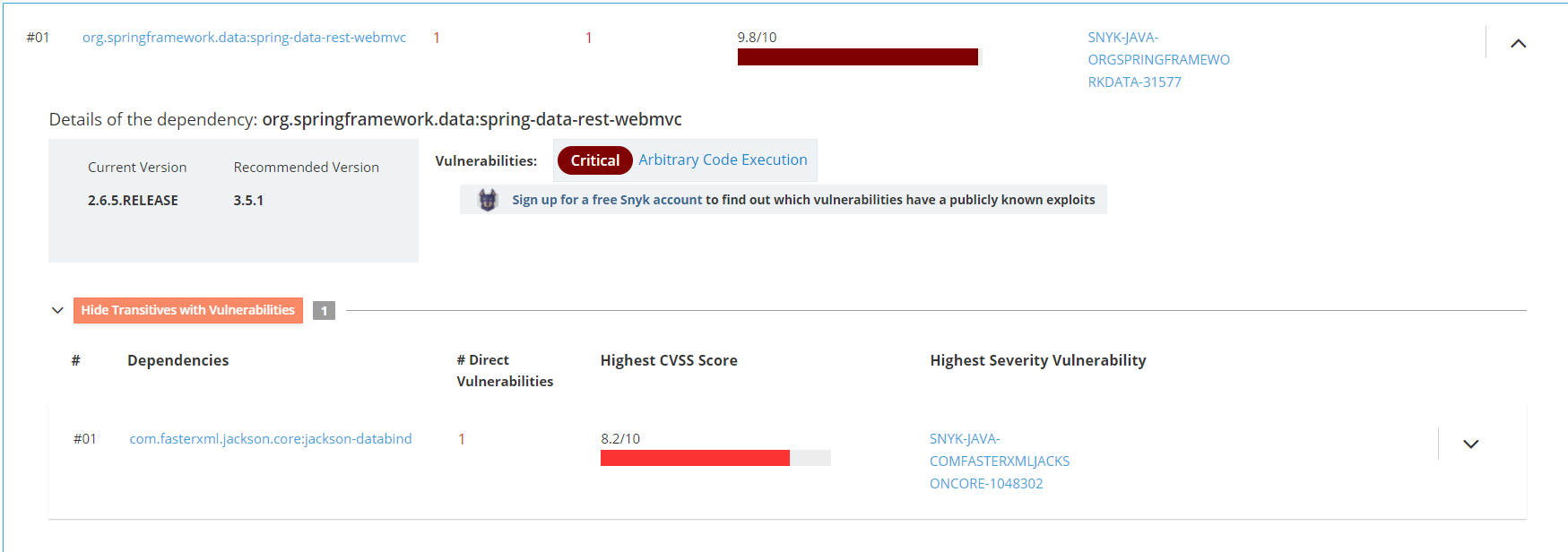
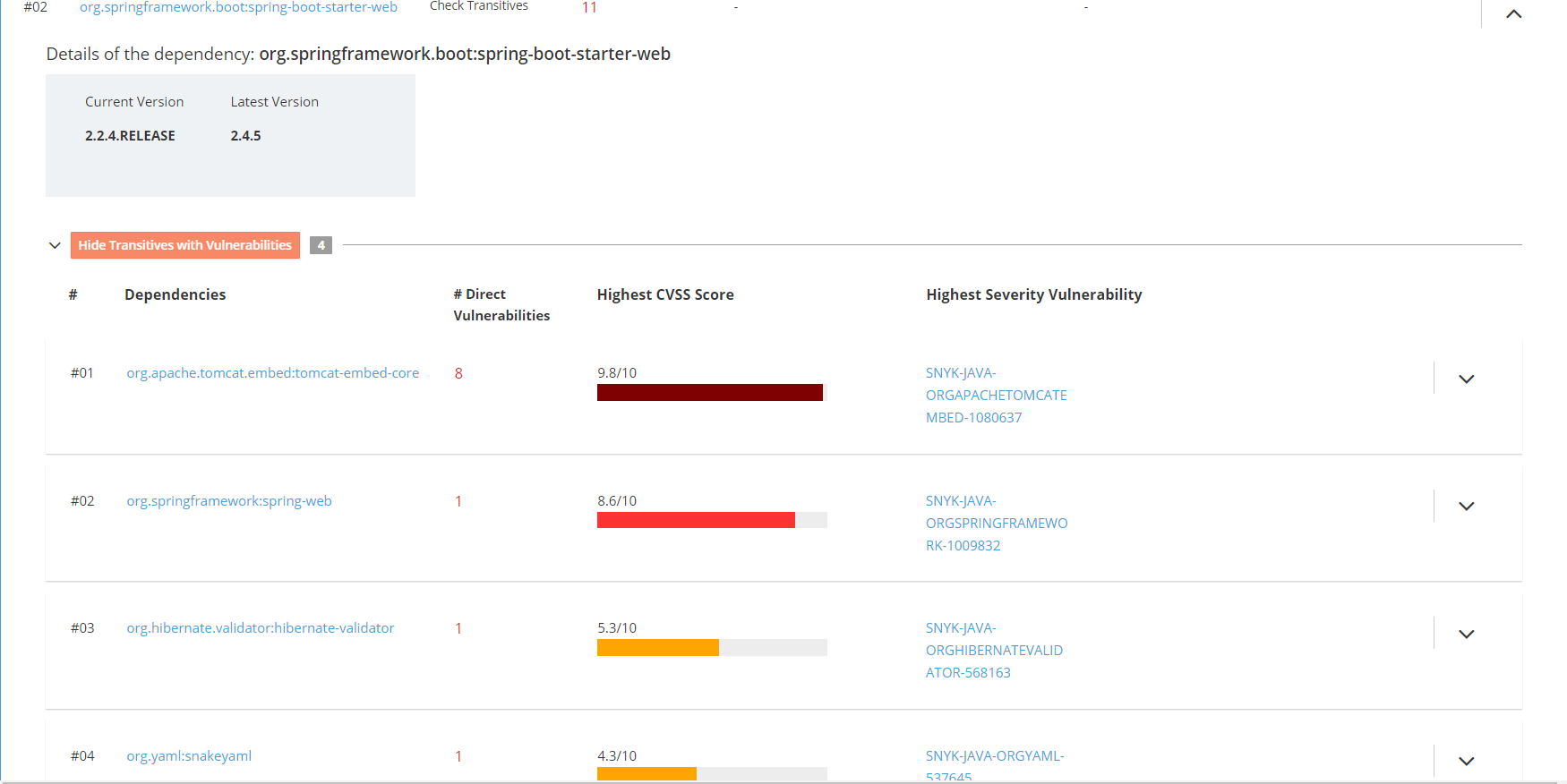
# CS 305 Module Two Static Testing Summary Template

## Instructions

Replace the bracketed text with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

### Run Dependency Check

* 
* 
* 

### Document Results

* [org.springframework.data:spring-data-rest-webmvc](https://snyk.io/vuln/maven:org.springframework.data%3Aspring-data-rest-webmvc?utm_medium=Partner&utm_source=RedHat&utm_campaign=Code-Ready-Analytics-2020&utm_content=vuln/maven:org.springframework.data%3Aspring-data-rest-webmvc)
* [org.springframework.data:spring-data-rest-webmvc](https://snyk.io/vuln/maven:org.springframework.data%3Aspring-data-rest-webmvc?utm_medium=Partner&utm_source=RedHat&utm_campaign=Code-Ready-Analytics-2020&utm_content=vuln/maven:org.springframework.data%3Aspring-data-rest-webmvc)
  + [CVE-2017-8046](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8046) – (Direct) Allows arbitrary Java code to be executed due to how spring uses its own expression language
    - [CVE-2020-25649](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25649) – (Transitive) Jackson Data Processor is a library that is vulnerable to an XXE injection attack that can give an attacker access to internal data or files
* [org.springframework.boot:spring-boot-starter-web](https://snyk.io/vuln/maven:org.springframework.boot%3Aspring-boot-starter-web?utm_medium=Partner&utm_source=RedHat&utm_campaign=Code-Ready-Analytics-2020&utm_content=vuln/maven:org.springframework.boot%3Aspring-boot-starter-web)
  + No direct vulnerabilities
    - [CVE-2021-25329](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25329) – (Transitive) Gives an attacker access to file contents and name under certain configurations
    - [CVE-2020-5421](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5421) – (Transitive) Can bypass certain file protections previously patched via a jsessionid parameter
    - [CVE-2020-10693](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10693) – (Transitive) Attackers can utilize flaw in hibernate-validator library to bypass input validation
    - [CVE-2017-18640](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18640) – (Transitive) YAML parser and emitter for java open to DoS attacks

### Interpret Results

* This dependency check shows the importance of keeping our dependencies updated. This is the first line of defense against vulnerabilities. Most of the dependencies in this project are very outdated and these problems have already been addressed in later releases. This is not always the solution, however. For example, CVE-2017-18640 mentions that the maintainer acknowledges the vulnerability but does not believe that it should be addressed by the parser, but instead by addressing the input the parser receives.
* False positives should be filtered from the tool because this tool should be evidence based. Anyone can report an issue with the dependency, but the integrity of this system comes from multiple users reporting the same problem. A system like this needs to have integrity, otherwise it could be manipulated and programs would be left vulnerable.