M.A.C.K.
Memory Leak
Sprint 3 Security Evaluation

Prepared by Andrew Palmer

Capstone Project: Spring 2022

The University of West Florida

Last Modified:

24 April 2022

CIS4595: Capstone Project

Dr. Bernd Owsnicki Klewe

Table of Contents

1. Introduction

All tests were performed on the application that was being hosted by Firebase. All attempted exploits and attacks were performed in such a way that a success would not impact the status of the server or database in any negative or irreversible way. For this evaluation, there were few applicable attacks that I was able to execute due to the application not having all functionalities implemented. In future evaluations, it is likely that more potential exploits and vulnerabilities will be included since there will be more functionality to evaluate.

2. Attempted Exploits/Attacks

a. Cross-site Scripting - *failed*

i. In addition to repeating the same tests from the previous evaluation, I attempted to execute a XSS attack through the search page, but this still did not work as was the case in the previous evaluation.

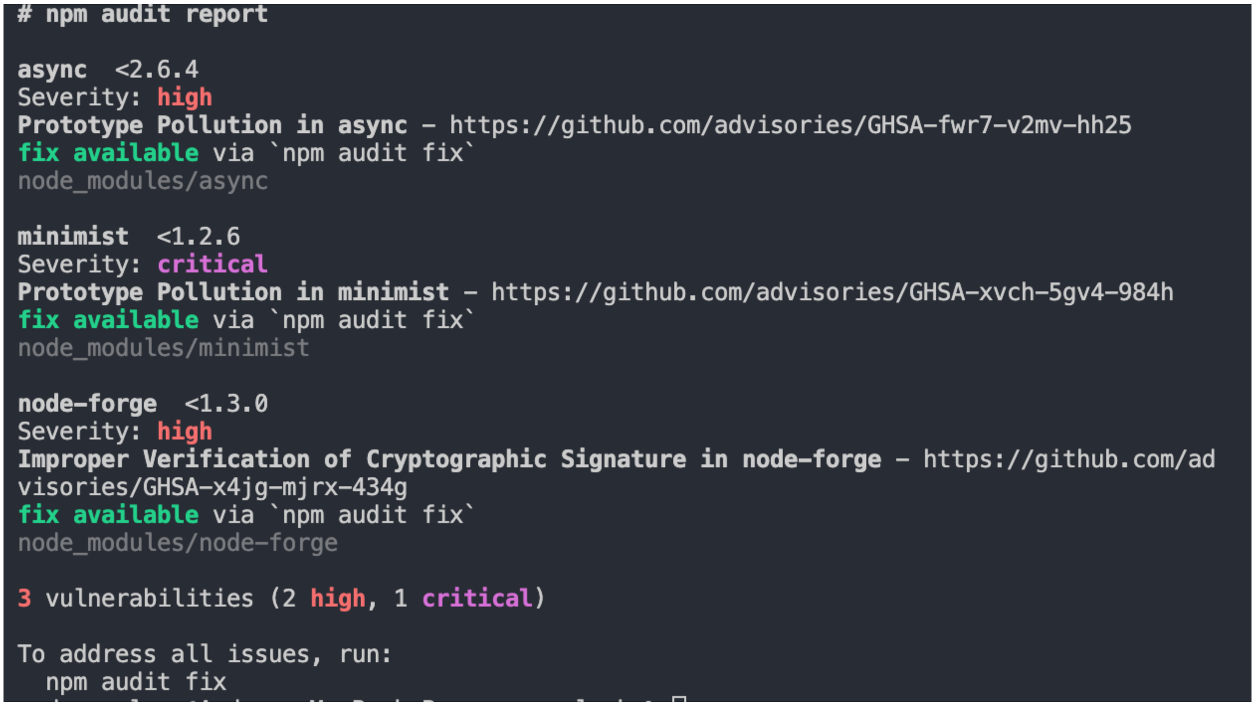
b. DOM-based XSS - *failed*

i. I repeated the same test from the previous evaluation, and it yielded the same results.

3. Codebase Vulnerabilities

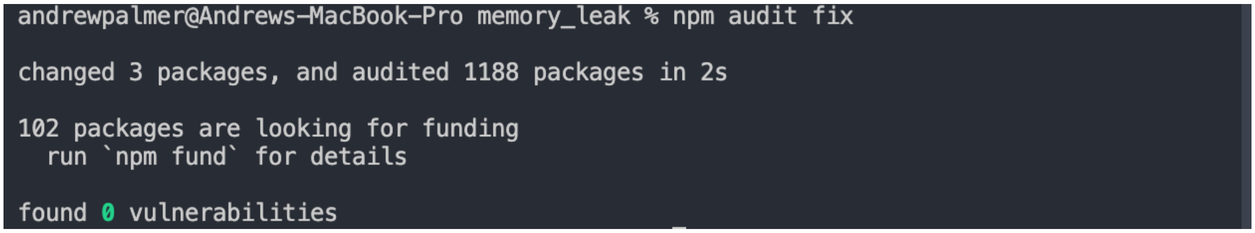
a. Potential Vulnerability: npm Packages

When running an npm *audit* command on the dev branch of our GitHub repository, I was presented with the following vulnerabilities.



```
# npm audit report

async  <2.6.4
Severity: high
Prototype Pollution in async - https://github.com/advisories/GHSA-fwr7-v2mv-hh25
fix available via `npm audit fix`
node_modules/async

minimist  <1.2.6
Severity: critical
Prototype Pollution in minimist - https://github.com/advisories/GHSA-xvch-5gv4-984h
fix available via `npm audit fix`
node_modules/minimist

node-forge  <1.3.0
Severity: high
Improper Verification of Cryptographic Signature in node-forge - https://github.com/ad
visories/GHSA-x4jg-mjrx-434g
fix available via `npm audit fix`
node_modules/node-forge

3 vulnerabilities (2 high, 1 critical)

To address all issues, run:
  npm audit fix
```

As recommended by npm, I ran an *npm audit fix* command which remediated the three vulnerabilities that were present in our codebase.



```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm audit fix

changed 3 packages, and audited 1188 packages in 2s

102 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```