**Incident Report:** CH-15119-Offensive-Download-Secured-Documents

**Date:** 10-26-2022

**Executive Summary:**

Test the OWASP Juice Shop application security by using a null byte injection to download a secured JSON document.

**Action Steps:**

To complete this task successfully, I took the following actions, in order:

1. Reviewed Incident Report for Story #15118 - Accessing Confidential Files - to obtain the URL address that granted access to the directory listings of the Juice Shop web application
2. Navigated to <https://live-project-cait.herokuapp.com/ftp/>
   1. File path to internal folder “ftp” containing confidential files
3. Clicked on file named “package.json.bak”
   1. Returned an Error Message 403 - only .md and .pdf files are allowed
4. Attempted null byte injection:
   1. Modified file path URL to read “<https://live-project-cait.herokuapp.com/ftp/package.json.bak%00.md>”
   2. Returned a Google Search results page with no true matches
5. %00 = terminates a string by ignoring everything after it
   1. Meant that the previous exploit attempt was unsuccessful at bypassing the file type restriction
      1. The “.md” was ignored by the interpreter because it followed the %00
6. Modified the file path URL to read “[https://live-project-cait.herokuapp.com/ftp/package.json.bak%2500.md](https://live-project-cait.herokuapp.com/ftp/package.json.bak%00.md)”
   1. Double-encoding the null byte accomplished two things:
      1. Bypassed the file type restriction
      2. Served as a breakpoint between the actual file extension and the appended one so that the correct file was returned by the server
7. File download completed



