**Incident Report:** CH-15118-Offensive-Access-Secured-Documents

**Date:** 10-24-2022

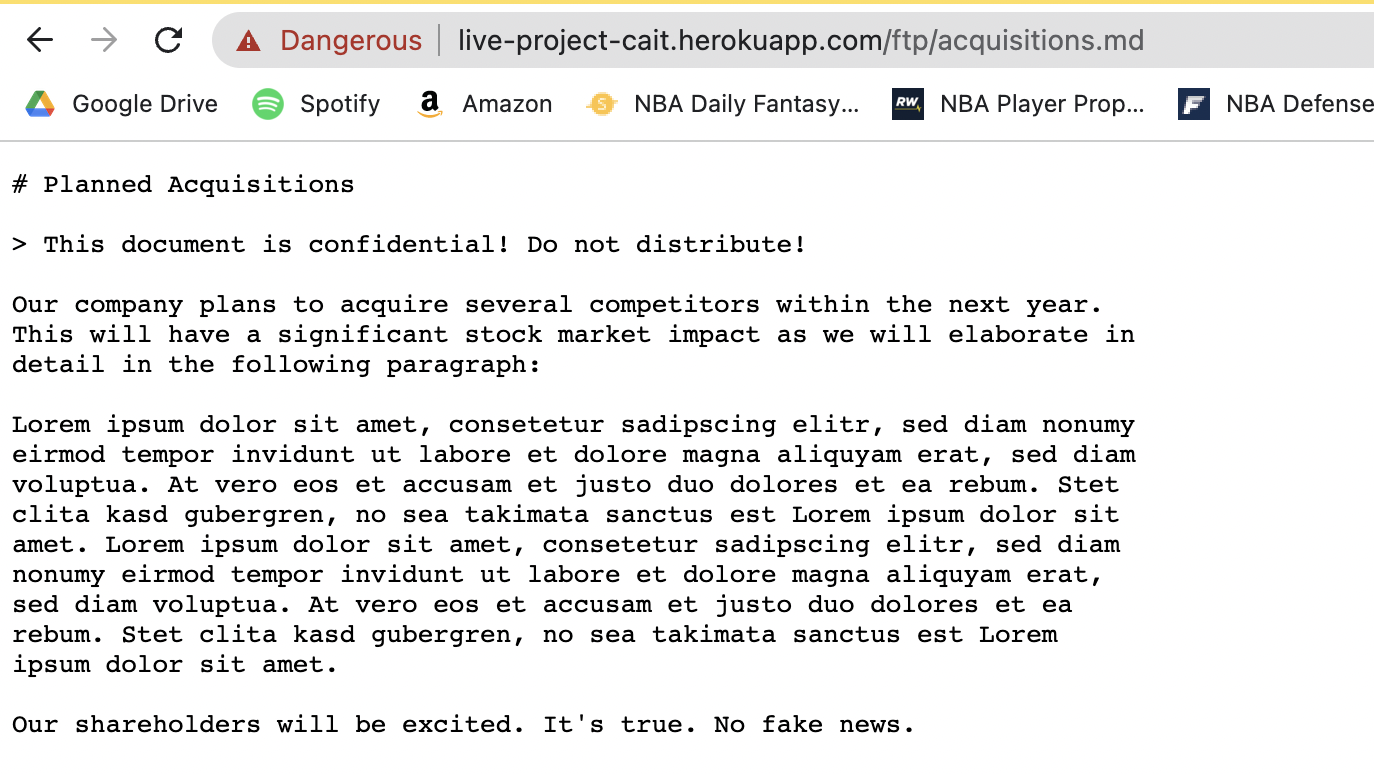
**Executive Summary:**

Test the OWASP Juice Shop application’s security by exploiting its directory listings and accessing confidential documents maintained under FTP without the use of any external pentesting software.

**Action Steps:**

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

1. Opened the OWASP Juice Shop app in browser
2. Navigated to different pages linked to the mainpage of the site
   1. Observed naming conventions used in the URL of each page
3. On the “About Us” page (<https://live-project-cait.herokuapp.com/#/about>):
   1. Linked document in the middle of the page - “Check out our boring terms of use if you are interested in such lame stuff”
   2. Hovering over link revealed the file path to accessing that document: …/ftp/legal.md
   3. FTP = File Transfer Protocol, which is a protocol used to transfer files unencrypted
   4. The file path used with the legal.md document suggested that there existed within the directory of this website a folder called “ftp” that likely had additional documents stored inside and accessible by traversing along the same directory path
   5. Folder name suggested these files were likely unencrypted
4. Hovered mouse over the file link → right-click → Copy Link Address
   1. Pasted copied URL into browser
   2. Edited URL by removing “legal.md” text
      1. Updated URL = <https://live-project-cait.herokuapp.com/ftp/>
      2. Updated address linked to page with multiple files stored in the ftp folder of the Juice Shop’s internal file directory
      3. Located and clicked on file named “acquisitions.md” revealing confidential company information (see below)



**Consequences of Attack:**

This security test revealed the following exploitable vulnerabilities within this web application:

* Sensitive Data Exposure
* Directory Transversal Attack

These vulnerabilities occur when attackers are able to exploit the internal filing structure of a web application and access data that is unencrypted and lacks sufficient access controls.

**Mitigation Strategies:**

Protection against these types of attacks include:

* Encrypting data both at rest and in transit using a secure protocol
  + Example: FTPS = FTP over SSL/TLS - client-server connections and file transfers are encrypted and certified via CA
* Restricting access to certain directories and files with Access Control Lists
* Using a Content Management System