|  |  |
| --- | --- |
| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | 5 Stars |
| Practical |
| Retrieve Blueprint | |

**OBJECTIVES**

* Understand how attackers can take advantage of the vulnerabilities
* OWASP vulnerability: Using Components with Known Vulnerabilities, Vulnerable and Outdated Components (A09:2017) (A06:2021)

**Prerequisite**

* HTTP Header Live
* Browser Developer Tools

**Challenge – Retrieve Blueprint**

* Deprive the shop of earnings by downloading the blueprint of one of its products.
* Retrieve Blueprint - Difficulty: 5/6 stars

**Step 1**

To go about this challenge, we must perform some reconnaissance. Given some analyzing of the packets, we would notice application-configuration.json in one of the packets, as shown below.

A screenshot of a computer

Description automatically generated

**Step 2**

Opening this file may give some insight to the possible location of the blueprint, or at the very least, some application configurations that could be exploited to find the location. Upon clicking on the application-configuration file, and some analysis, you would stumble upon the obvious field that says fileForRetrieveBlueprintChallenge, and that value is equal to “JuiceShop.stl”.

Graphical user interface, text, application, email

Description automatically generated

**Step 3**

STL is a file format native to the stereolithography CAD software created by 3D Systems, hence it would make sense that this file is related to the OWASP Juice Shop Logo (3D-Printed). We would then proceed to visit the location of where the OWASP Juice Shop Logo (3D-Printed) in the home page. By inspecting the element and locating to where the image is in the HTML, we would see this.

A screenshot of a computer

Description automatically generated with medium confidence

**Step 4**

You would see the directory that leads to the image of the 3D keychain. Let’s try to download the file by changing the directory of /assets/public/images/products/3d\_keychain.jpg to /assets/public/images/products/JuiceShop.stl instead, as shown below.

A picture containing graphical user interface

Description automatically generated

**Step 5**

It would make sense logically, because in the field for OWASP Juice Shop Logo (3D-Printed), you notice that the file location for the Blueprint is in there. It would make sense that the .stl file is in the same directory as the Juice Shop Logo image. Upon changing the directory of the image to the .stl file, the challenge will be completed according to Juice Shop. For the sake of downloading the .stl file, it can be done by hovering over where the image was, and opening it in a new tab, which will lead us to the download prompt, as shown below.

Graphical user interface

Description automatically generated

**~ End of Challenge ~**