|  |  |
| --- | --- |
| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | 5 Stars |
| Practical |
| Supply Chain Attack | |

**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* OWASP vulnerability: Using Components with Known Vulnerabilities, Vulnerable and Outdated Components (A09:2017) (A06:2021)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**

* Install Leafpad on your kali

**Challenge – Supply Chain Attack**

* Informing the development team about a danger to some of their credentials
* Supply Chain Attack - Difficulty: 5/6 stars

To first start off this challenge, we would need to install the leafpad in your kali machine.

**Step 1**

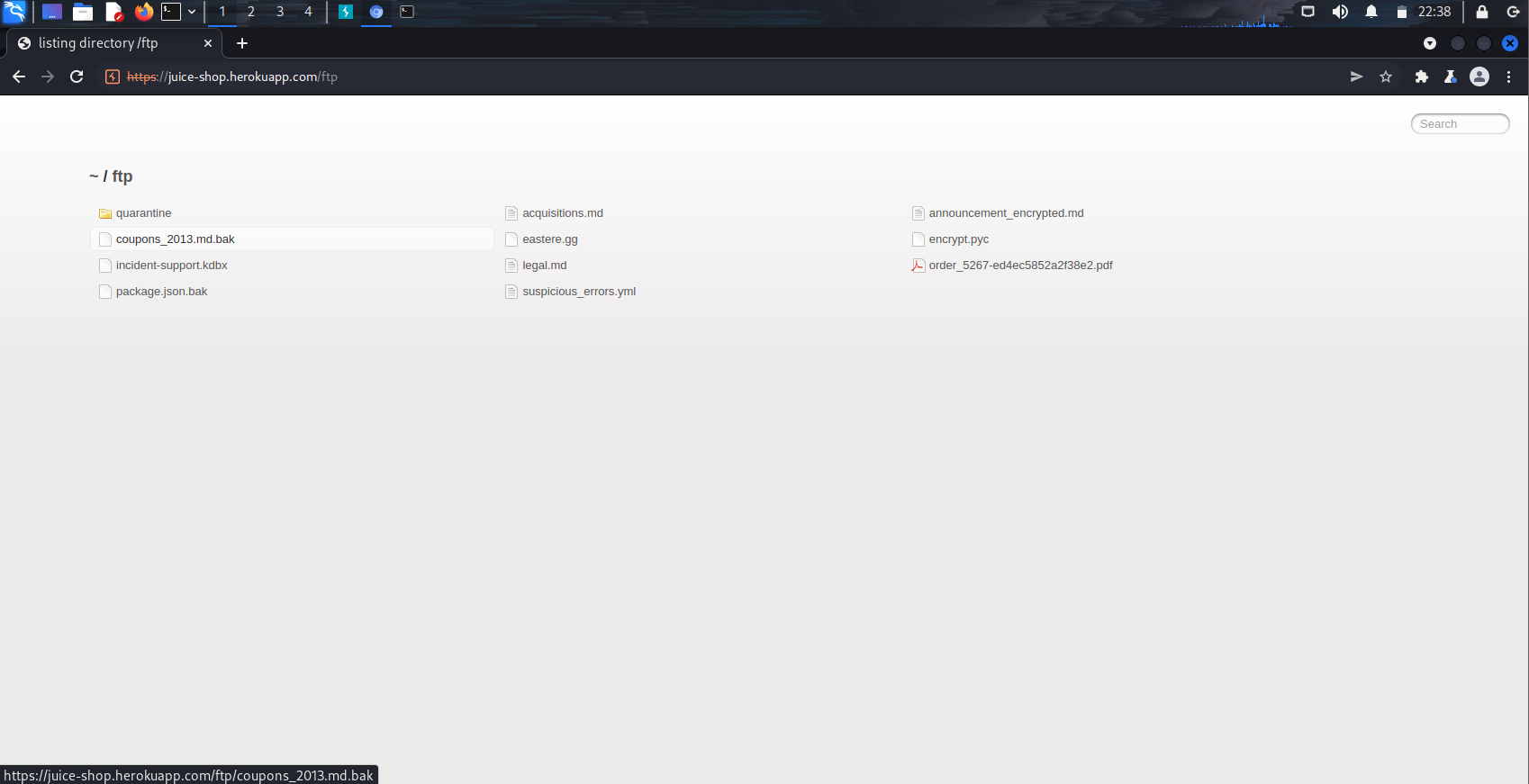
Use this command apt-get install Leafpad

Text

Description automatically generated

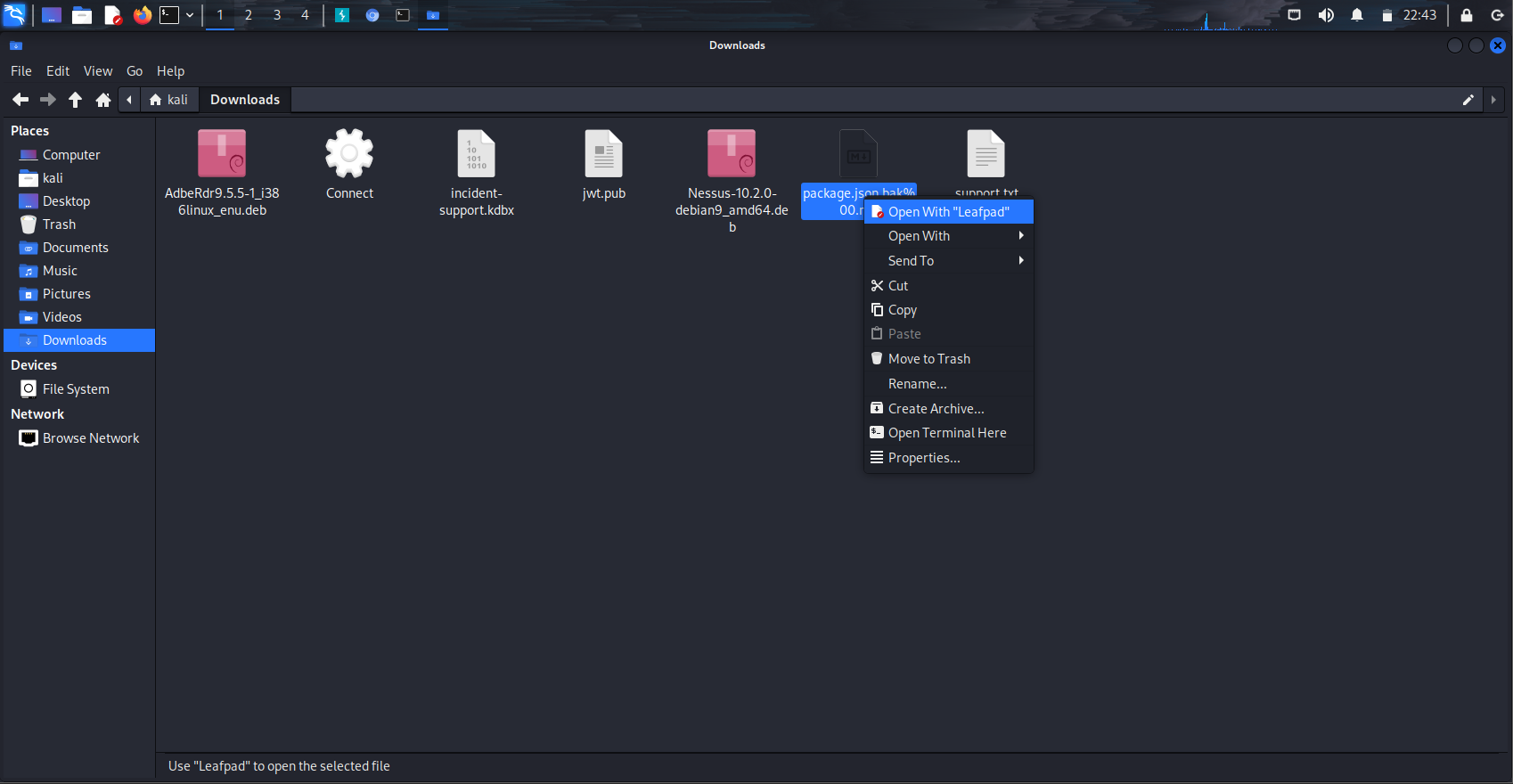
**Step 2**

Go to the ftp page on juiceshop and download the package.json.bak file by adding ‘%2500.md’ to the back of the URL.



**Step 3**

Open the file using leafpad in the file explorer.

****

**Step 4**

Open the search using Crtl + f and type in eslint and this should appear.

Text

Description automatically generated

Eslint-scope 3.7.2 contained an exploit which sends a .npmrc file to a third party and may possibly steam the NPM credentials. This is a huge vulnerability for juice shop and should be reported immediately.

However, before we can do that, we need to find a link to the problem on github and by searching for Eslint-scope 3.7.2 this search result would appear.

Copy the link of the github

Text

Description automatically generated

**Step 5**

Paste the github link in the comment section and answer the captcha before submitting the customer feedback

Graphical user interface, application

Description automatically generated

**Step 6**

Upon submission, a notification would appear informing you that you have successfully solved this challenge.

A screenshot of a computer

Description automatically generated with medium confidence

**~ End of Challenge ~**