**Cybersecurity 401**

**Module 8 - Web Application Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 38 - Attacking Juice Shop with Burp Suite**

## 

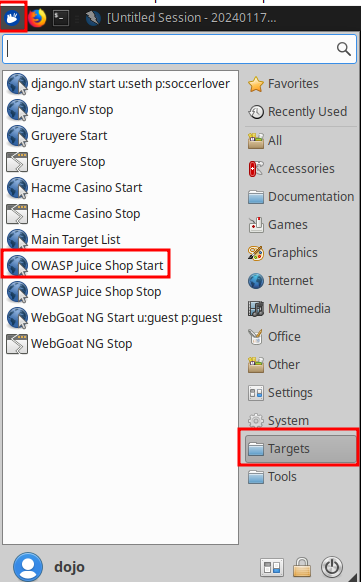
**| Rodrigo Brasil 01/2024 |**

### **Part 1: Staging**

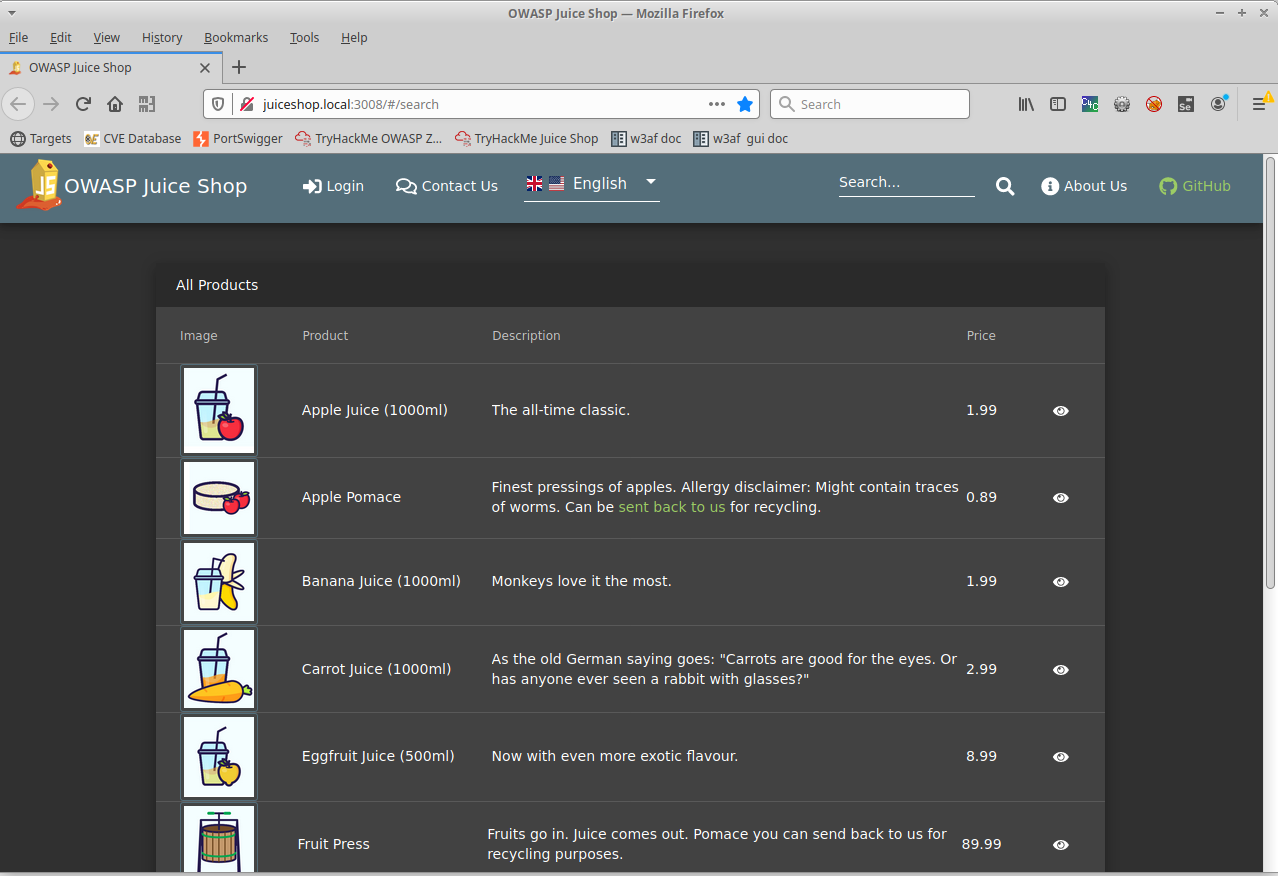
**This lab requires the Web Security Dojo VM.**

****

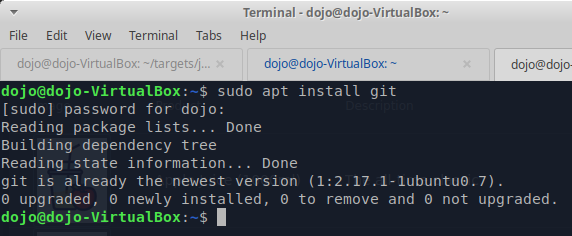
* **Juice Shop is manually launched via shell script from the start menu > targets section.**

****

* **Access the Juice Shop page to verify it is up.**

****

* **Install Git with sudo apt update then sudo apt install git.**

****

* **Git clone** [**SecLists**](https://github.com/danielmiessler/SecLists) **to your Web Security Dojo.**

***If you reboot Web Security Dojo, you’ll need to re-launch Juice Shop manually.***

### 

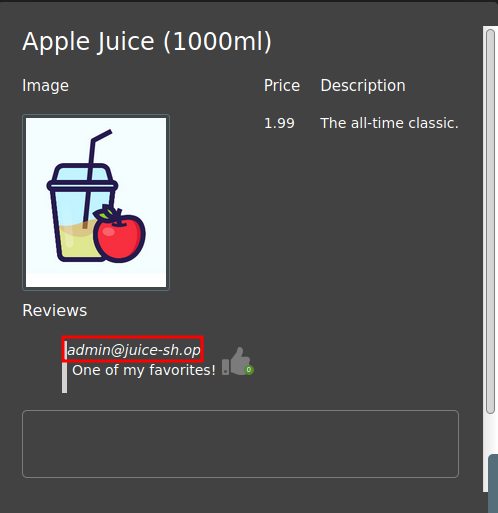
### **Part 2: TryHackMe Burp Suite Lab**

**We’ll be revisiting TryHackMe’s site once again, this time in guiding us on how to use Burp Suite against OWASP Juice Shop.**

* **Complete the lab at** [**TryHackMe OWASP Juice Shop Room**](https://tryhackme.com/room/owaspjuiceshop)**. Respond to any questions/prompts here in your submission instead of on the TryHackMe page.**
  + **Task 1: Open for business!**
    - **Nothing to do here but to review the primer and move forward into Task 2.**
  + **Task 2: Let’s go on an adventure!**

****

* + - **What is the administrator’s email address?**

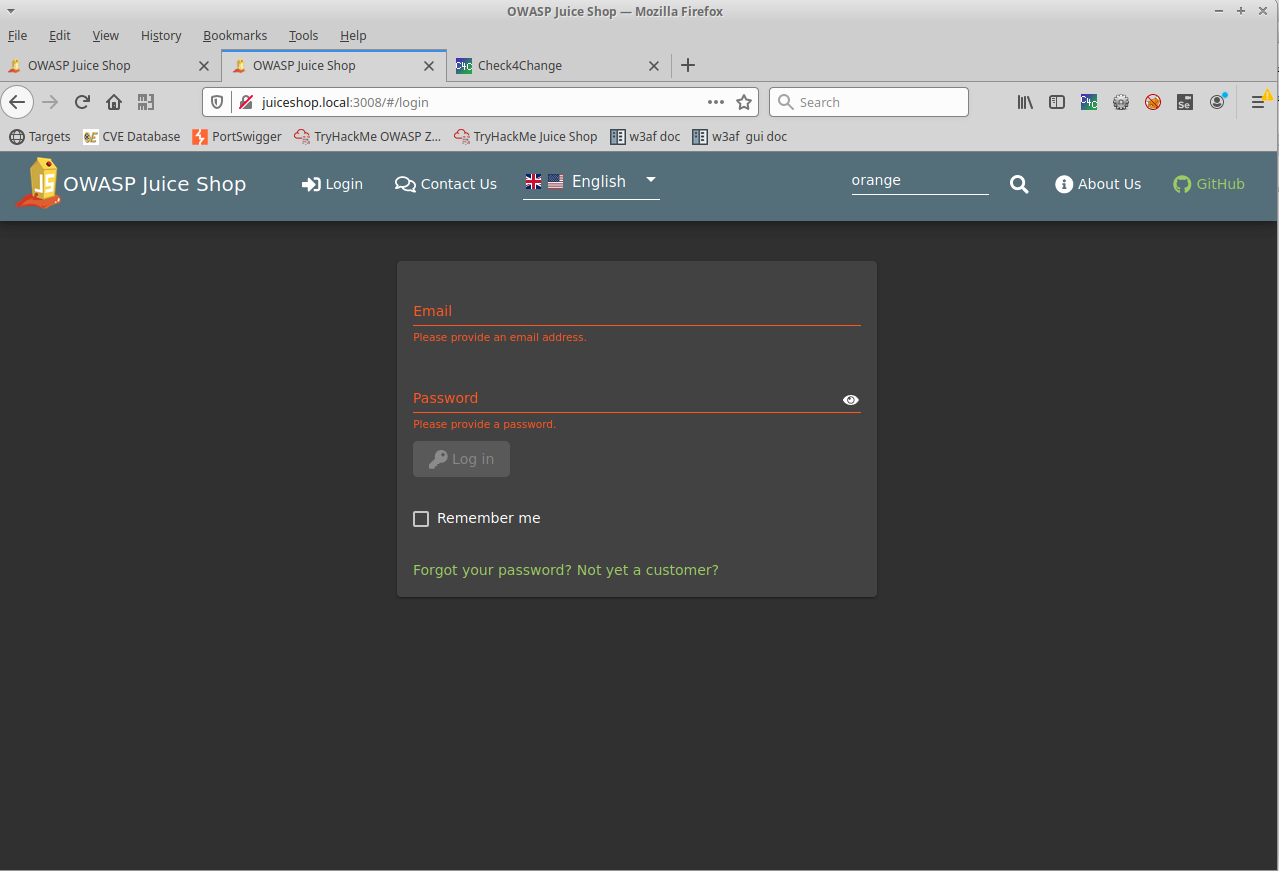
****

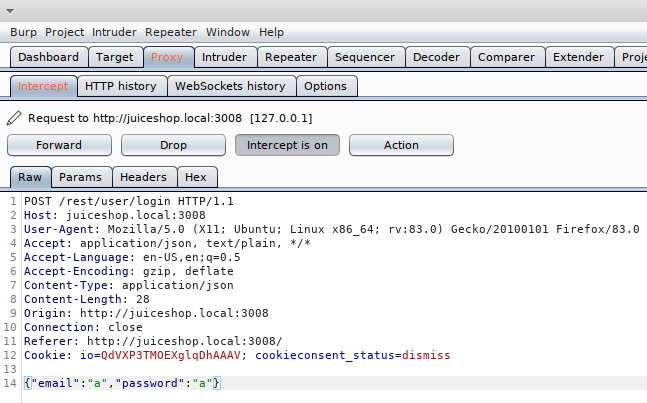
* + - **What parameter is used for searching?**

****

* + - **What show does Jim reference in his review?**
      * **Star Trek**
  + **Task 3: Inject the juice**

****

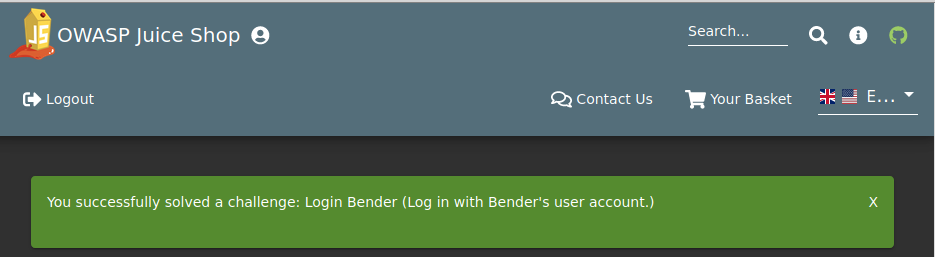
****

****

* + - **How did you log into Bender’s account?**

**On burpsuite with the forwarder on, by changing the email to bender email, was able to successfully Log-in into bender user account**

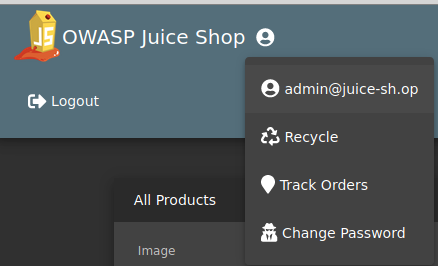
****

****

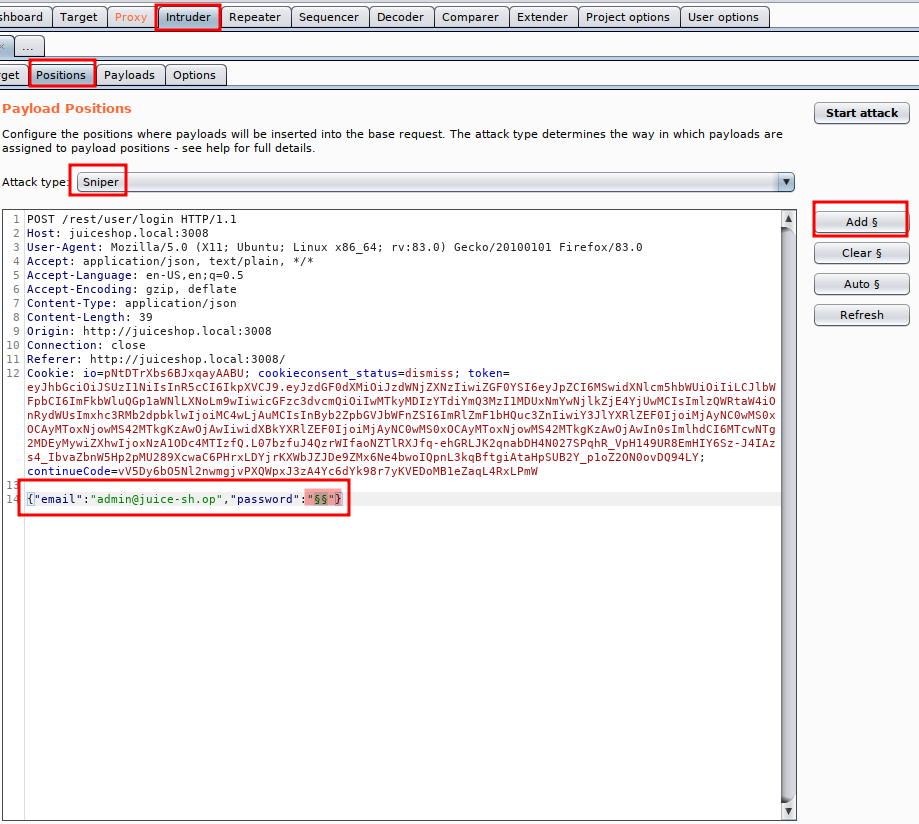
* + - **How did you log into the administrator’s account?**

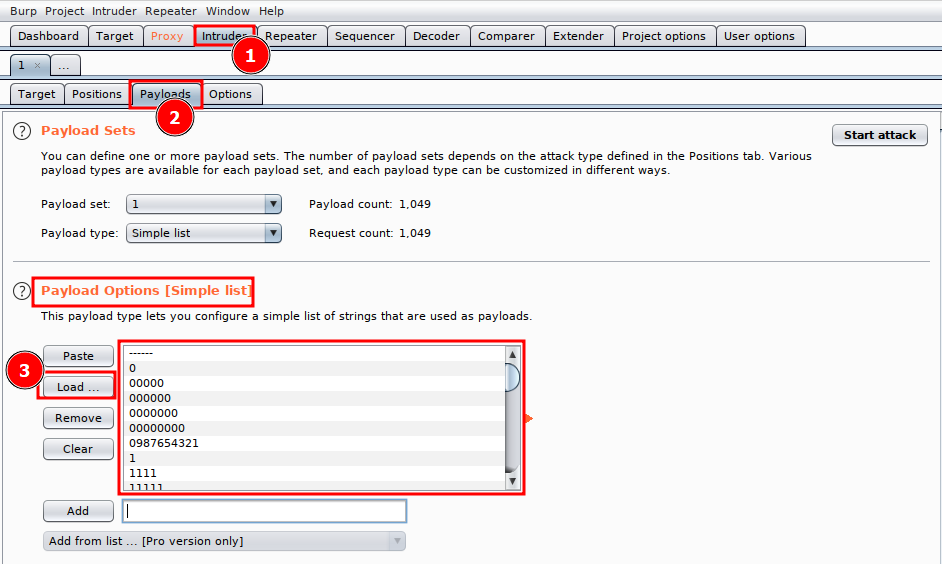
**Changing the query on email to “or 1=1–” so the email is always “correct” and log us into user id 0, which happens to be the administrator account.**

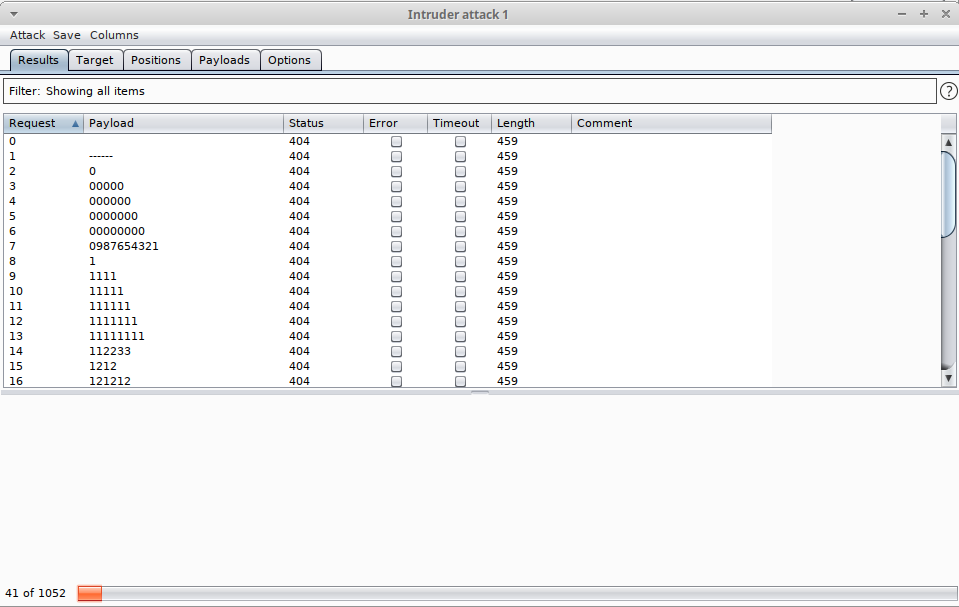
****

****

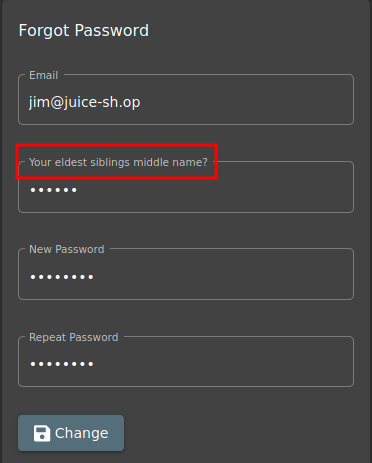
* + **Task 4: Who broke my lock?!**
    - **Brute force the administrator’s password. How did you do it?  
      *Don’t forget, you downloaded SecLists in Part 1.***

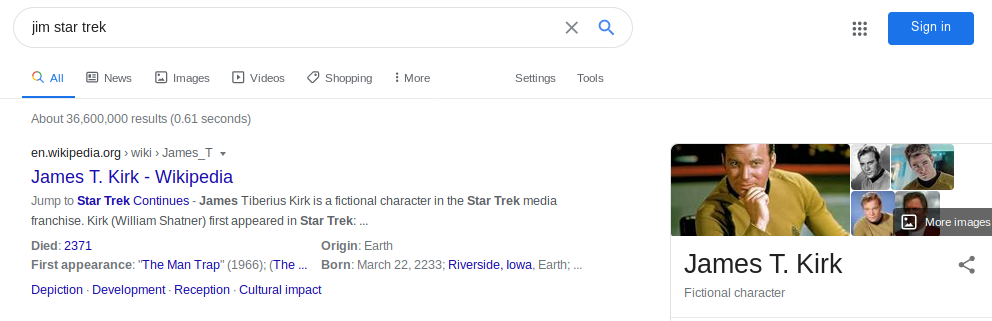
******

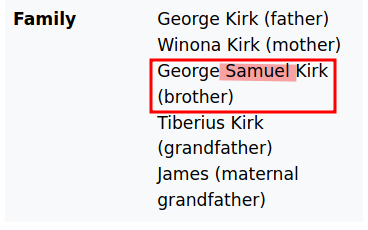
******

******

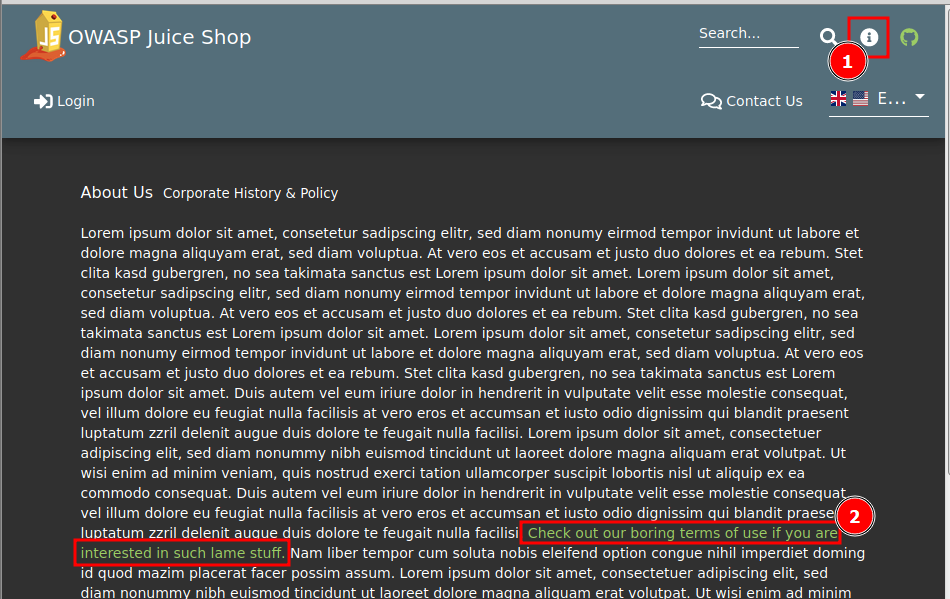
* + - **Reset the password. How did you do it?**

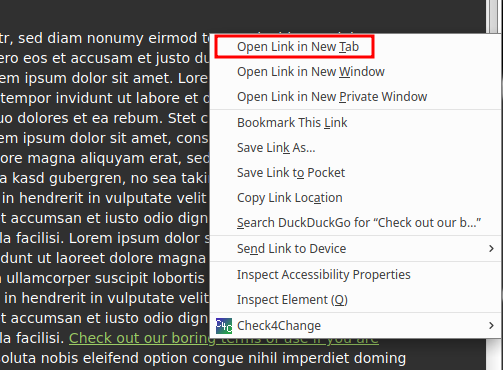
****

****

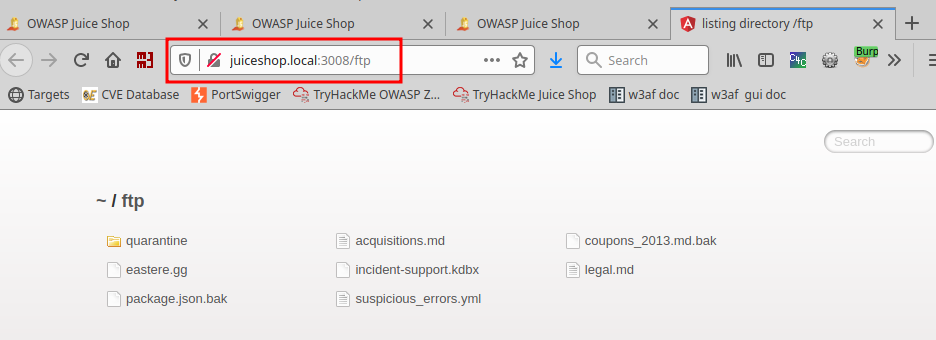
****

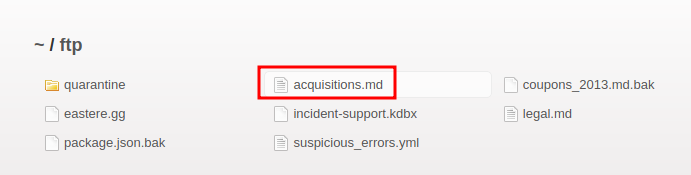
* + **Task 5: AH! Don’t look!**
    - **Access the confidential document. How did you do it?**

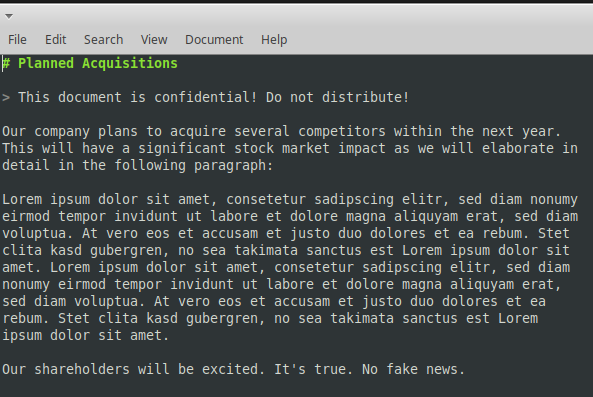
****

****

****

****

****

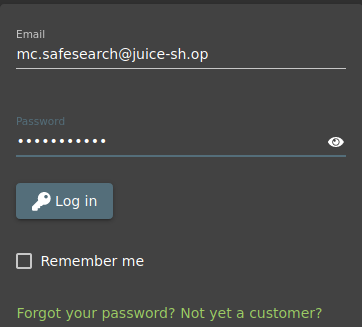
****

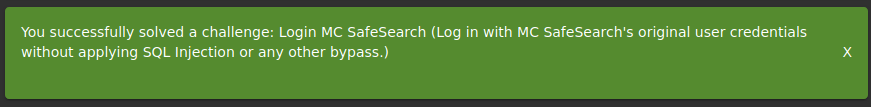
* + - **Log into MC SafeSearch’s account. How did you do it?**

[Rapper Who Is Very Concerned With Password Security](https://youtu.be/v59CX2DiX0Y)

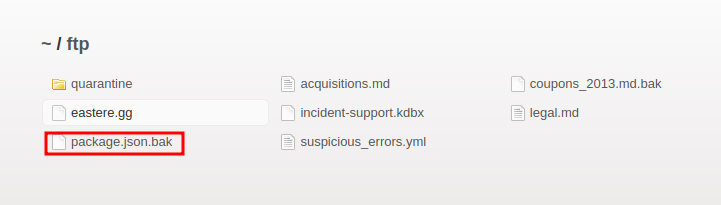
**He notes that his password is "Mr. Noodles" but he has replaced some "vowels into zeros", meaning that he just replaced the o's into 0's.**

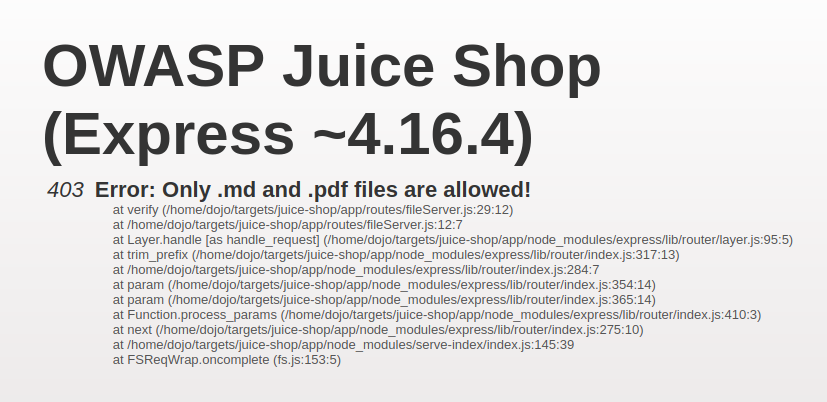
**We now know the password to the mc.safesearch@juice-sh.op account is "Mr. N00dles"**

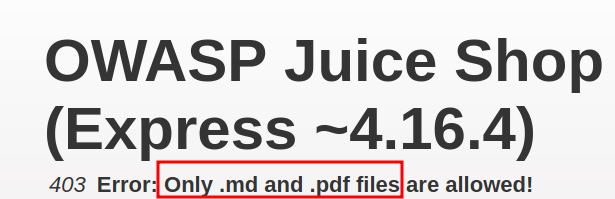
****

****

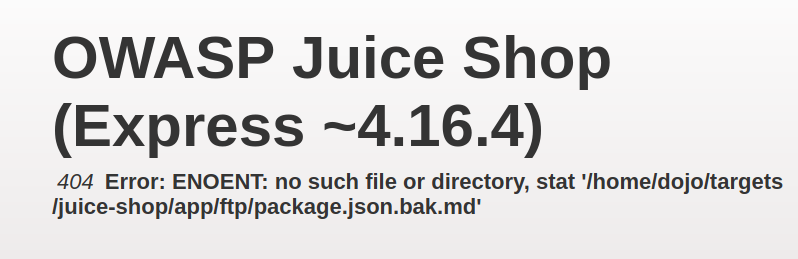
* + - **Download package.json.bak. How did you get past the error?**

****

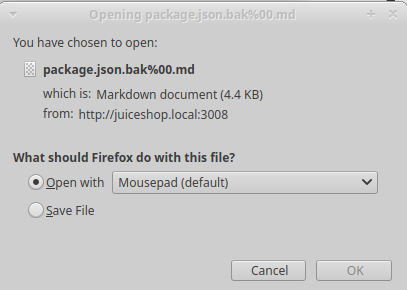
****

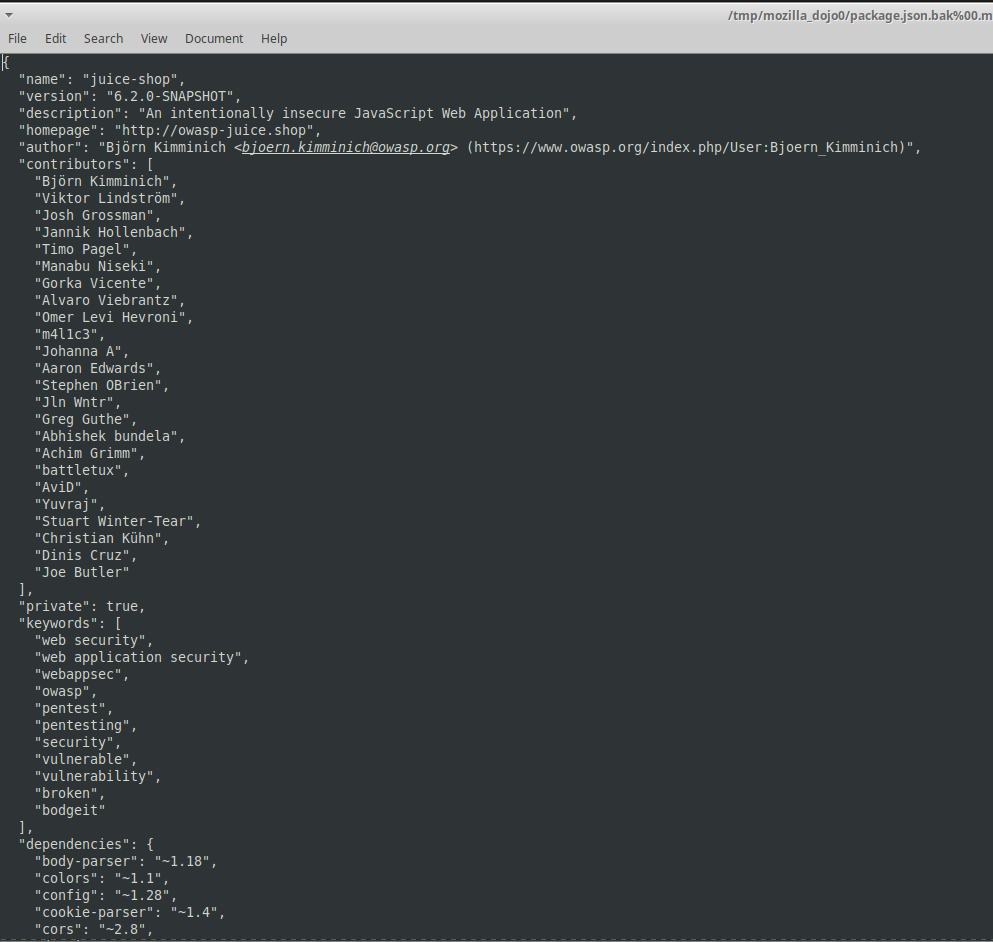
****

****

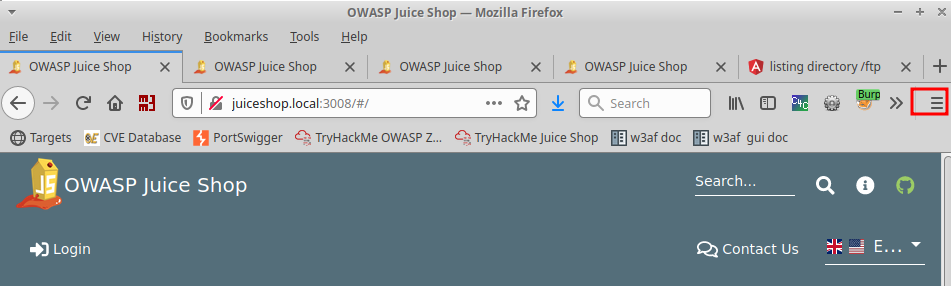
****

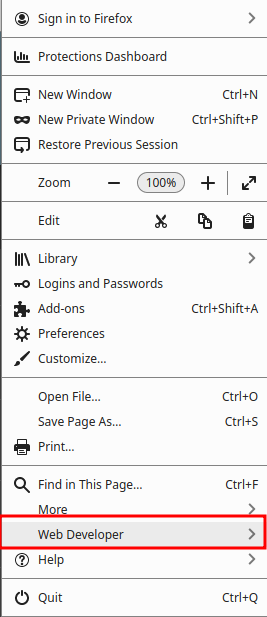
****

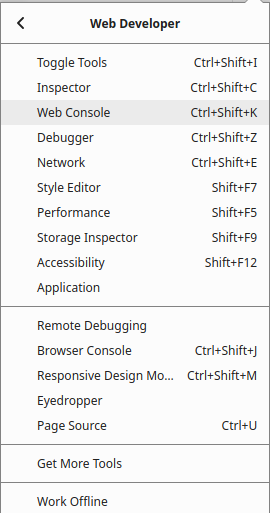
****

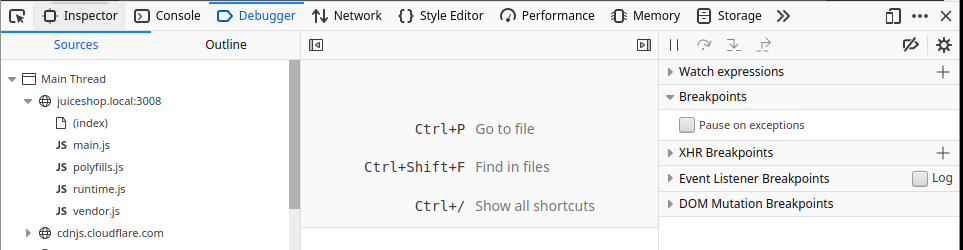
****

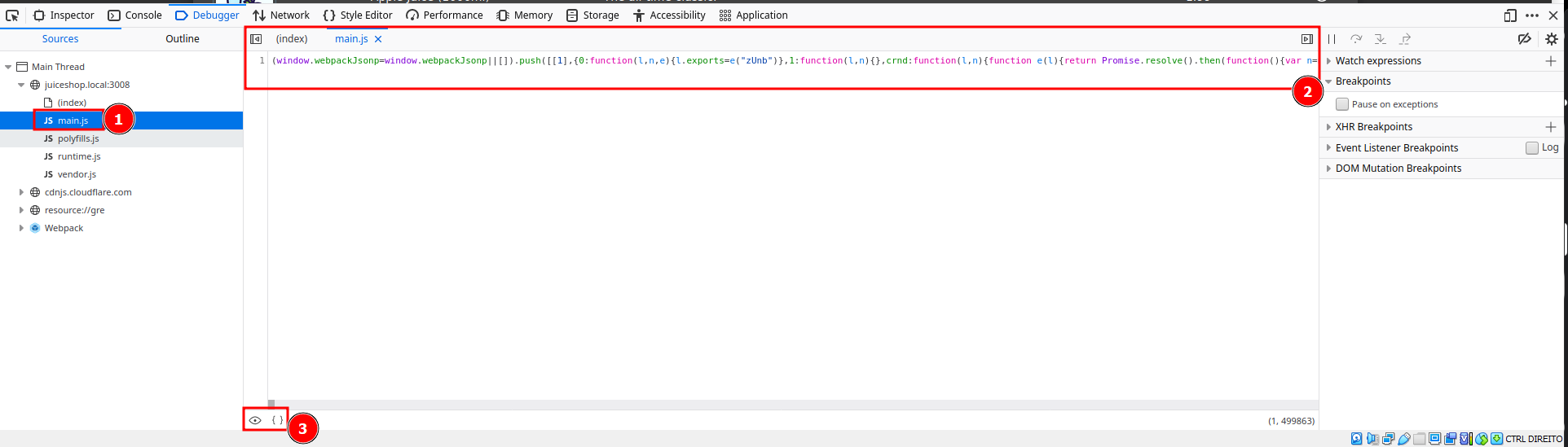
* + **Task 6: Who’s flying this thing?**
    - **Access the administration page. How did you do it?**

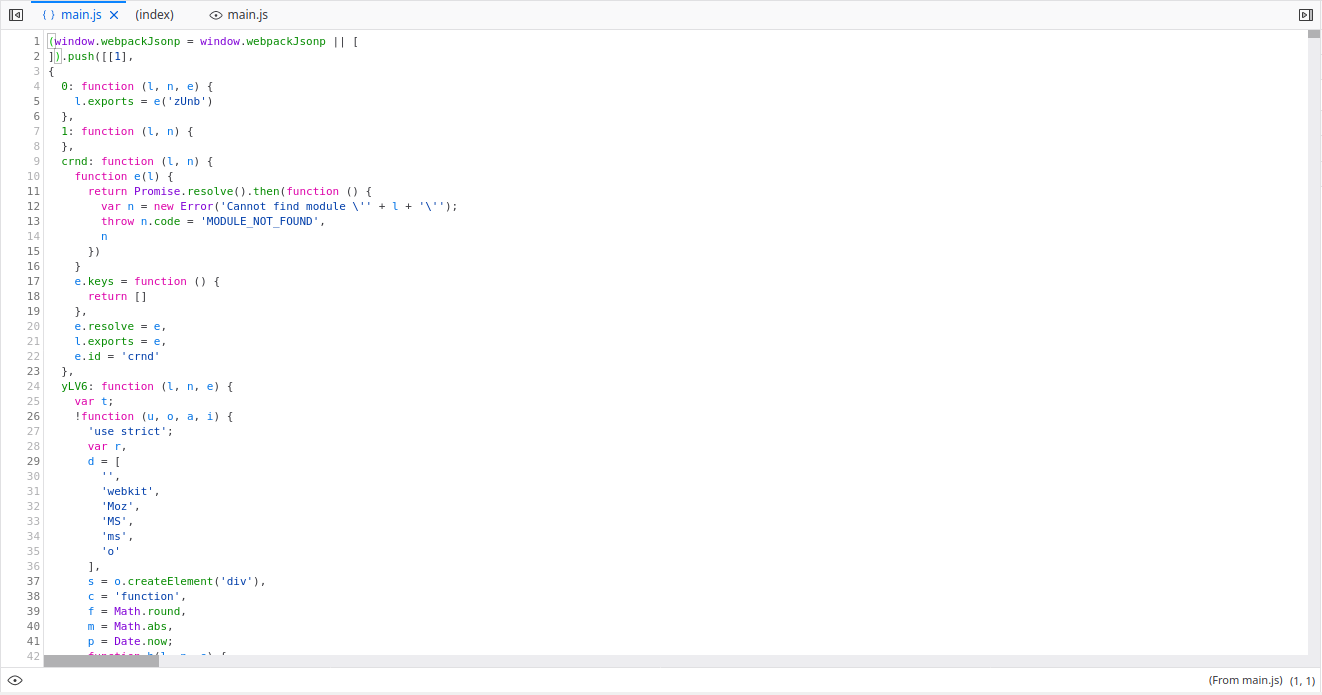
****

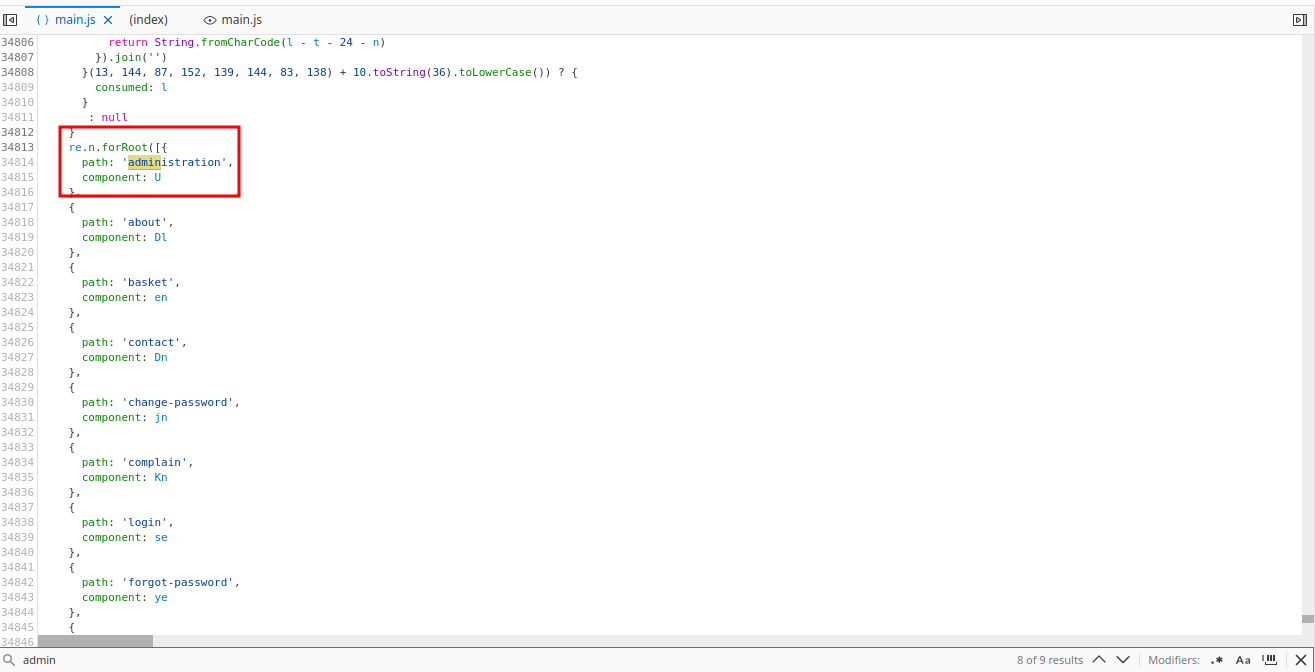
****

****

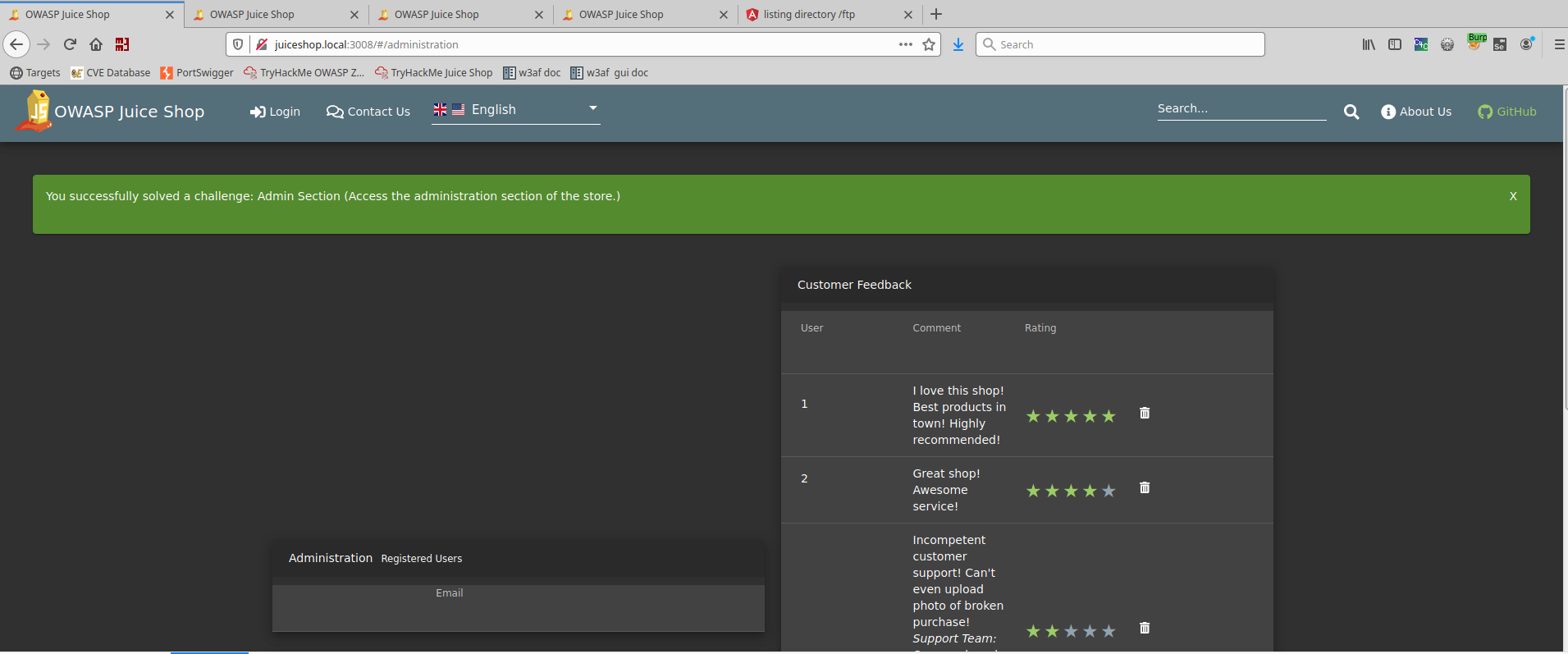
****

****

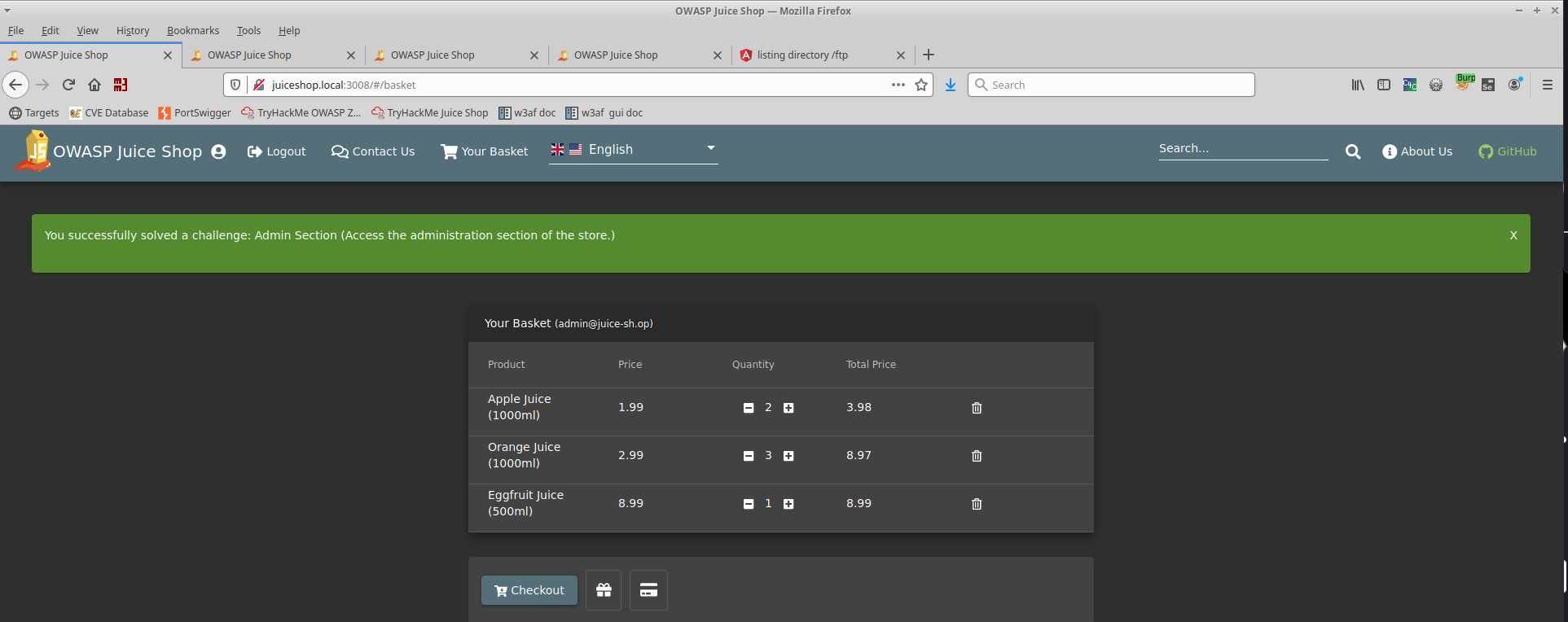
****

****

****

****

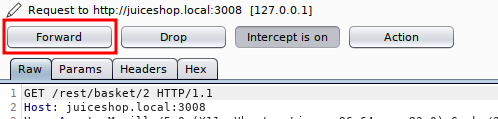
* + - **View another user’s shopping basket. How did you do it?**

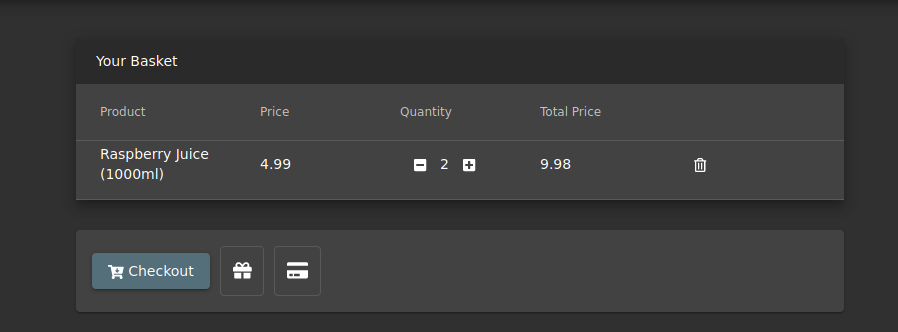
****

****

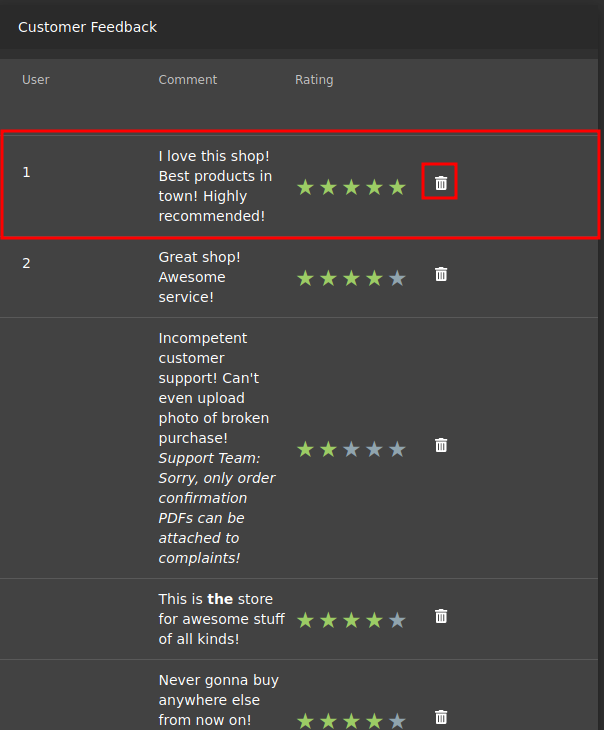
****

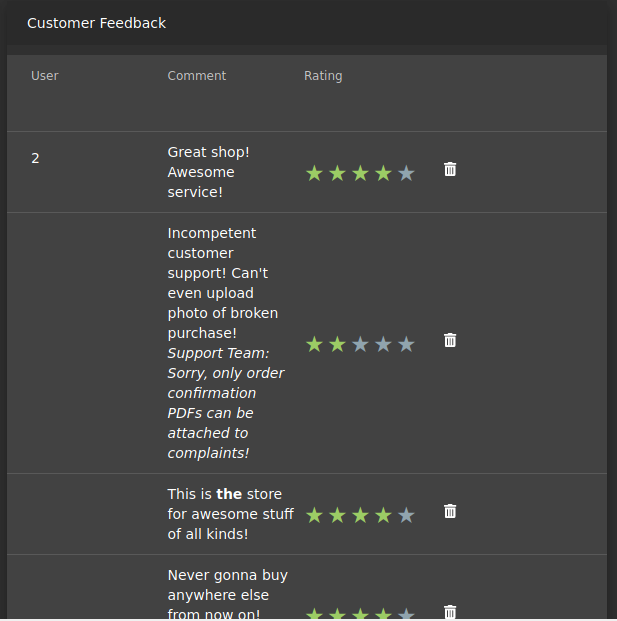
****

****

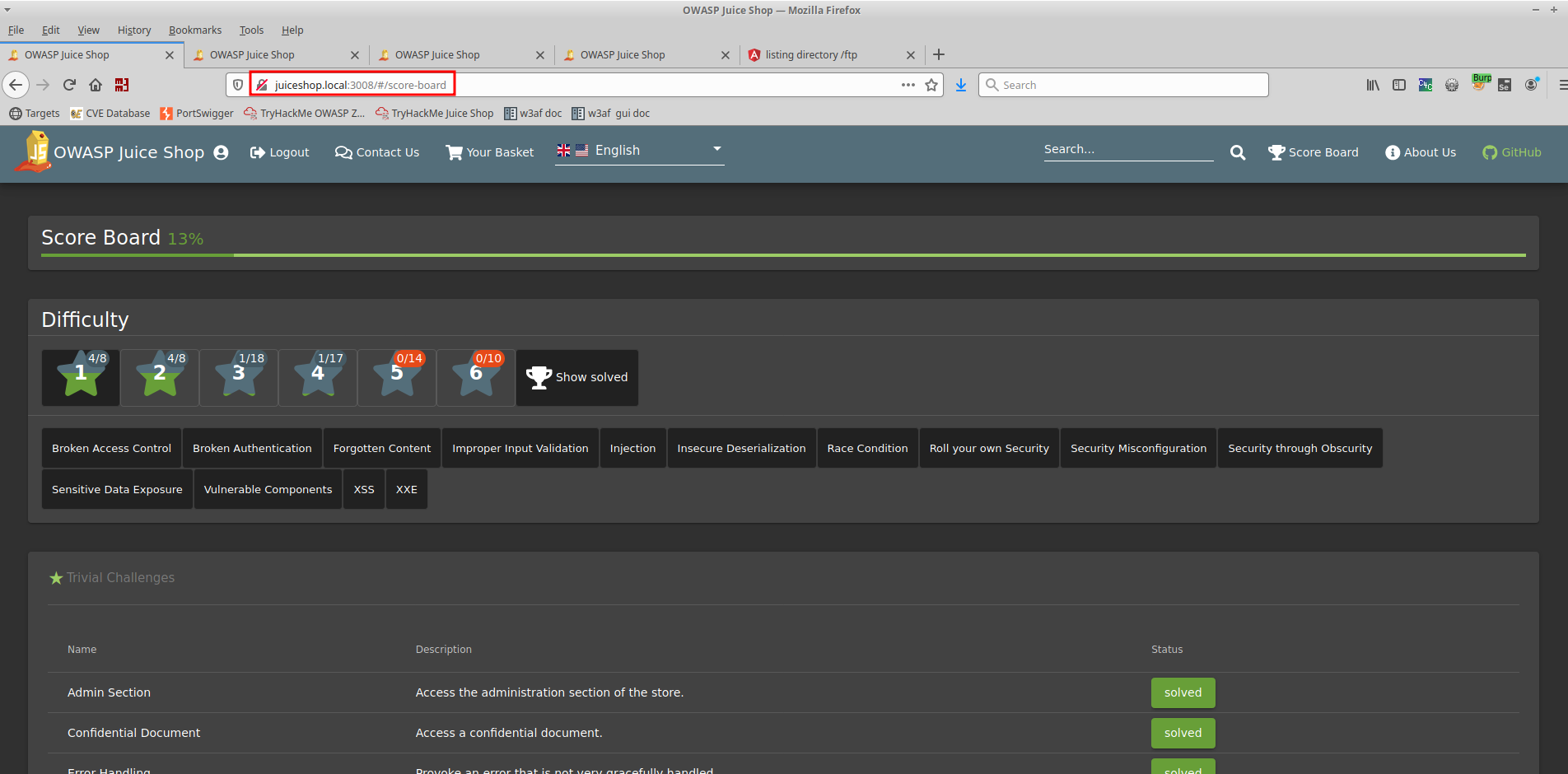
****

* + - **Remove all 5-star reviews. How did you accomplish this?**

****

****

* + **Task 7: Where did that come from?**
    - **This task does not need to be completed, no action required.**
  + **Task 8: Exploration!**
    - **View the scoreboard page, no action required.**

****

### 

### 

### **Part 3: Reporting**

**Define the below terms in your own words:**

* **Injection**

**A threat actor injects malicious code into a system, typically through input fields or data entry points and this malicious code can manipulate the behavior of the system.**

* **Broken authentication**

**Broken authentication is a security weakness that occurs when the mechanisms used for user authentication are compromised or improperly implemented.**

* **Sensitive data exposure**

**Confidential or private information is inadequately protected and becomes accessible to unauthorized parties.**

* **Broken access control**

**A system fails to enforce proper restrictions on users' access to resources or functionalities.**

* **XSS**

**Attackers inject malicious scripts into web pages that are viewed by other users. These scripts can then be executed in the context of the victim's browser, allowing the attacker to steal information, manipulate content, or perform actions on behalf of the user without their consent.**