**OWASP JUICE SHOP CTF from Tryhackme**

This is a jeopardy type of CTF, so we will follow the hints.

1. As always connect your vpn:

* sudo openvpn {name\_of\_vpn}

1. Then check if the machine is online

* ping {target\_ip}
* traceroute {target\_ip}

A screenshot of a computer program

Description automatically generated

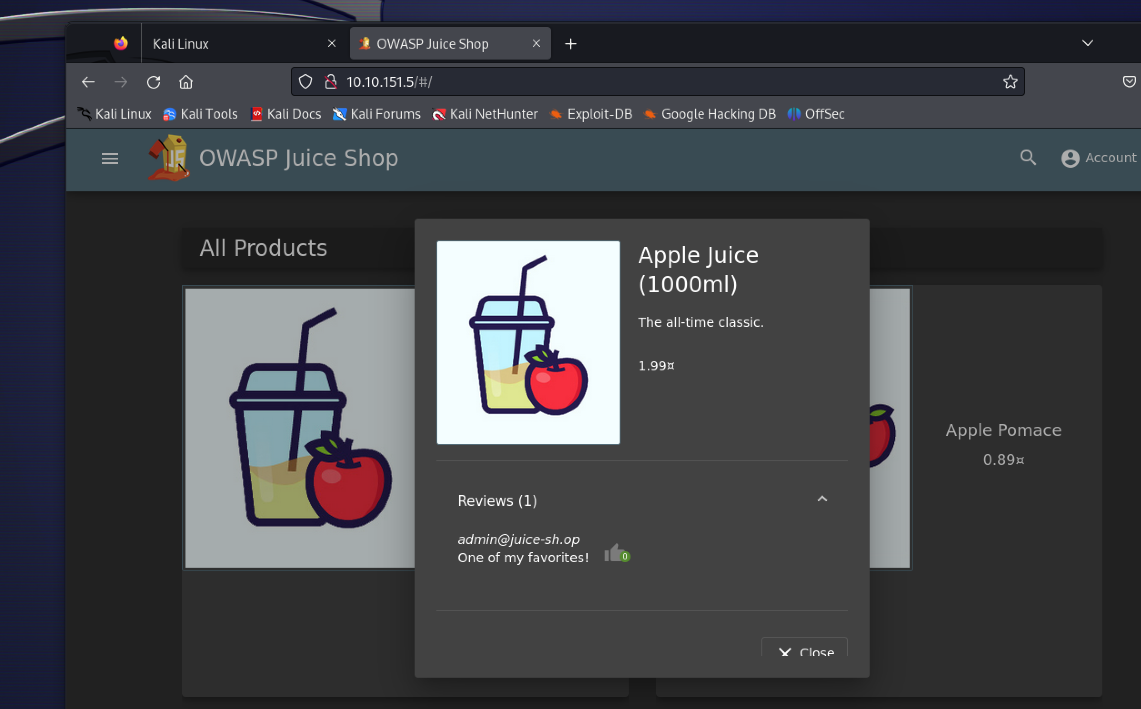
1. Now let’s scan our target using nmap

* nmap -F -Pn {target\_ip}
* -F = fast mode
* -Pn = no ping

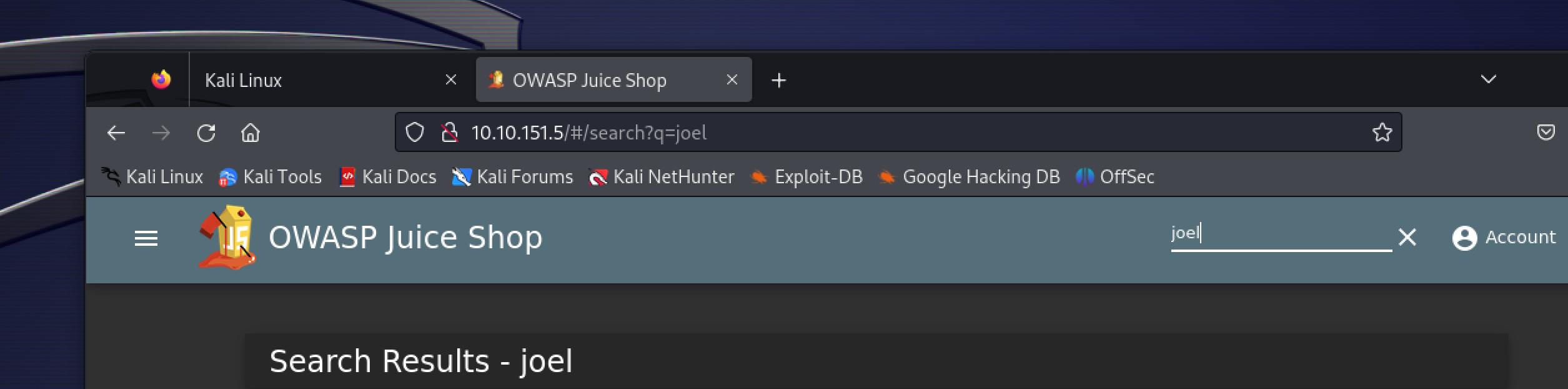
A computer screen with white text

Description automatically generated

1. Since we see that port 80 which is http is open, we navigate to the website.
2. After opening the website, we investigate it.
3. On clicking the links, we find a review and on clicking the review we find there are emails of employees.



1. We take note of the usernames and move on to the next task.
2. When we search for staff using the search bar and notice the url we see what the search parameter is.



1. On reviewing the green smoothie, we find the username of jim and clue which is word (replicator).

* Searching for the word replicator we find another clue (star trek), which is a movie name.

A screenshot of a menu

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Now we open our burpsuite and turn the intercept on and turn our foxy proxy to burp. Then we will capture the login and use **sql injection** to login to the admin page.

* On the capture we will change the email with **“ ‘ or 1=1- -”**
* ‘ = will close the brackets on sql query
* Or = return true if either is true and 1=1 is always true.
* - - = used in sql to comment data.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* When forwarding the request, we will login to the admin page.

A screenshot of a computer

Description automatically generated

1. Now let’s try to bypass another login page with a known email, for instance for Bender.

* When we capture the login for Bender, we will alter the email with [**bender@juice-sh.op’--**](mailto:bender@juice-sh.op’--)
* Here 1=1 is not needed because we know the email, or the email is valid so we only use **‘- -** bypass the login.

NOTE

* 1=1 is used when email or username is not known or not valid.

A screenshot of a computer

Description automatically generated

* We loged into bender account bypassing the login.

A screenshot of a computer

Description automatically generated

1. On the above method we tried to alter the database to login now we will try to brute force to know the password of the admin.

* We will once again capture a login request, but instead of sending it through the proxy, we will send it to Intruder and change the password using the “**add$**” option on right corner.

A screenshot of a computer

Description automatically generated

* Then go to the payload option and we will choose the **best1050.txt from Seclists** from the following path:
* /usr/share/wordlists/SecLists/Passwords/Common-Credentials/best1050.txt
* And then we start the attack and look for status code of 200.

A screenshot of a computer

Description automatically generated

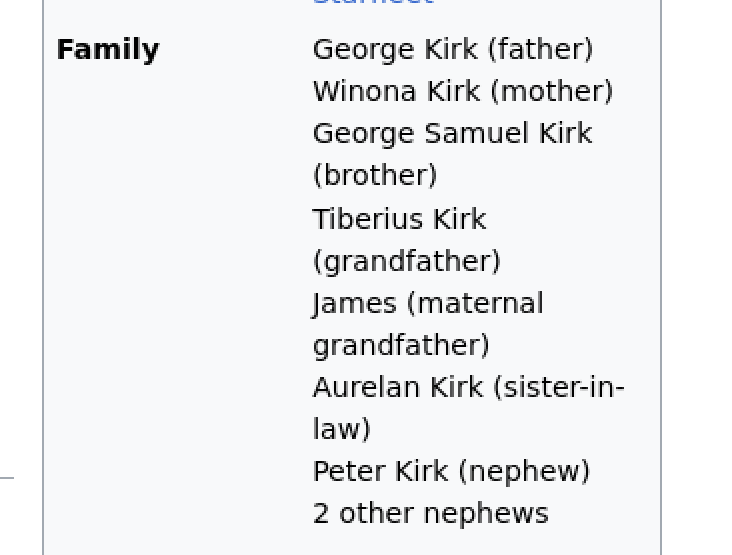
* As you can see there is a status code of 200 on **admin123** (so this is the password).
* Now we can login into the admin page using the password and username.

A screenshot of a login box

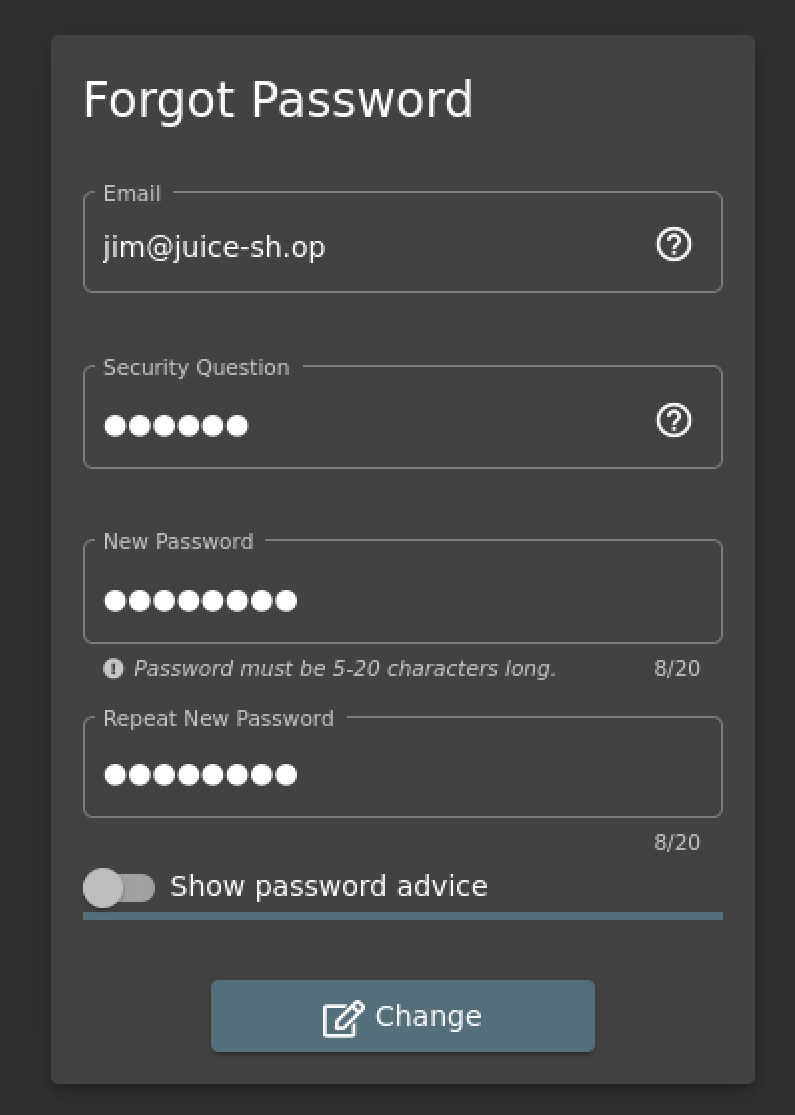
Description automatically generated

1. Now we will try to reset Jim’s password using the forgot password option on the login page.

* Jim’s security question is set to "Your eldest siblings middle name?".
* And since we have gathered information on jim we search for “**Jim star trek**” and we find the following data.

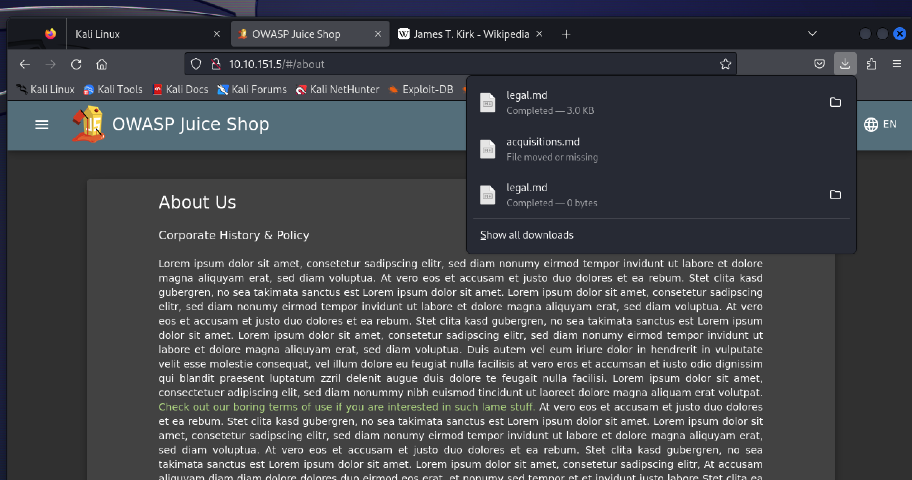


* As you can see, he has only one brother with the name **George Samuel** and when we try, we find out that the answer for the security question is **Samuel**.
* Now let’s change the password to whatever we want to be.



1. Now we will try to access sensitive information, in our case lets go to the about us page and click the link and we will download a file.

* Now on the url let’s navigate to the subdirectory of ftp and we will find a page with juicy files and let’s download **acquisition.md** file.



A screenshot of a computer

Description automatically generated

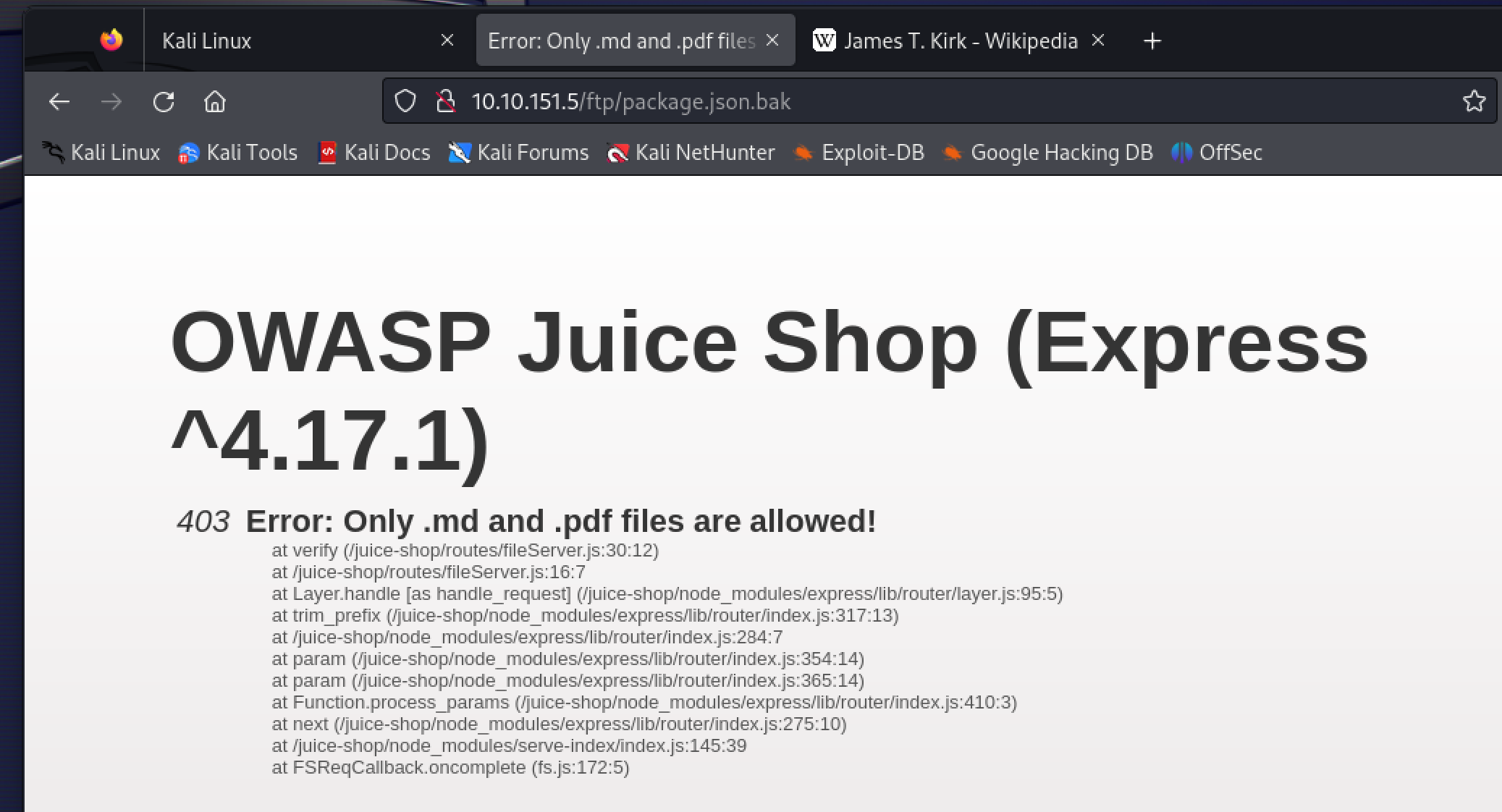
1. Next, we will listen to music and try to get the username and password by listening to the music.

* From the music we find that the singer is disclosing information which might be helpful to us.

A screenshot of a login screen

Description automatically generated

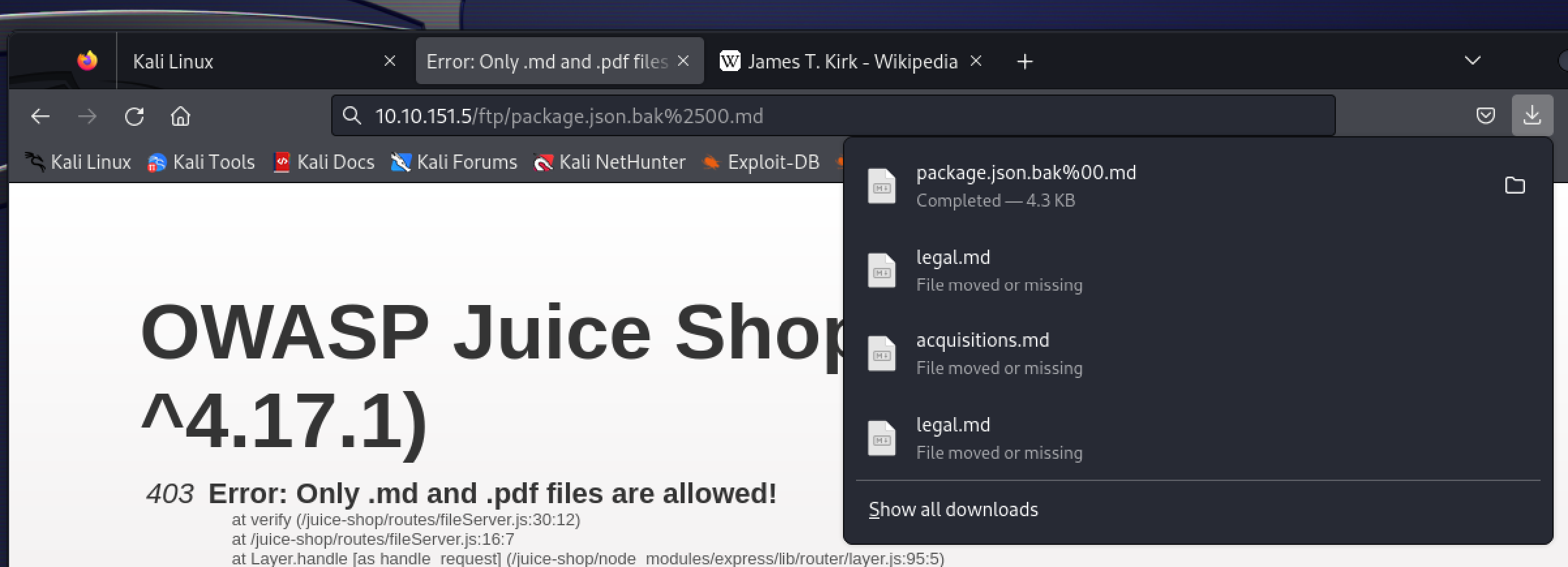
1. Now we will try to download a file called **package.json.bak** from the ftp page but we encounter a **403 error** which means access is forbidden.



* To bypass this error, we will use **Poison Null Byte** attack by adding **%2500** and then a **.md** to the end will bypass the 403 error.

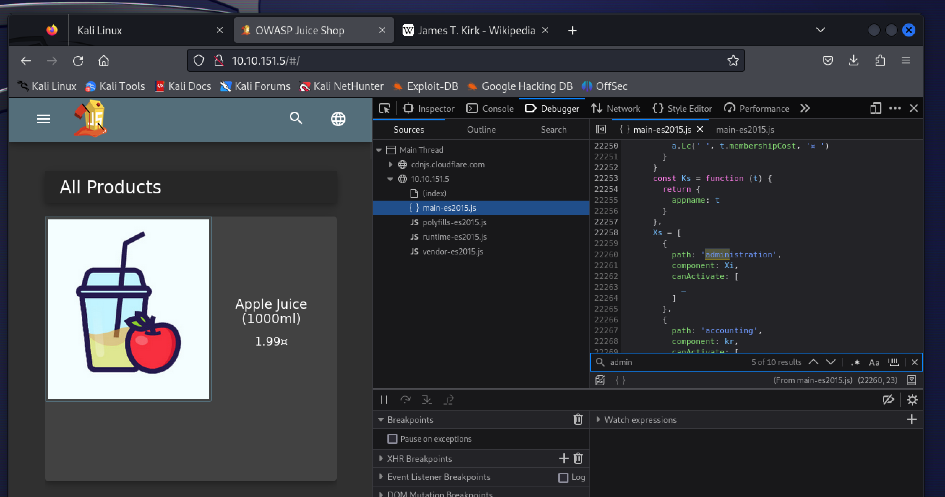
NOTE

* Poison Null Byte attack places a NULL character in the string at a certain byte, the string will tell the server to terminate at that point, nulling the rest of the string.

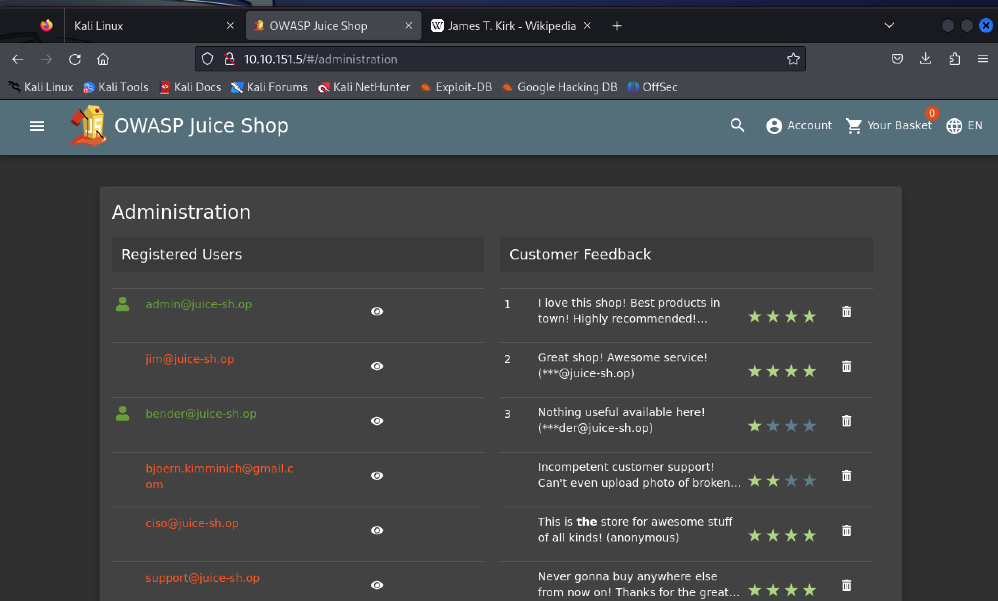


1. Here we will see privilege escalation but first let’s see two types of privilege escalation:

* **Horizontal Privilege Escalation**: Occurs when a user can perform an action or access data of another user with the same level of permissions.
* **Vertical Privilege Escalation**: Occurs when a user can perform an action or access data of another user with a higher level of permissions.
* Now to access the administration page we right click on the page and click inspect and go to the **debugger** and there open the javascript file **main-es2015.js**.
* Then searching for administration, we see there is a path and when we try to navigate to it we see 403 error (Forbidden).

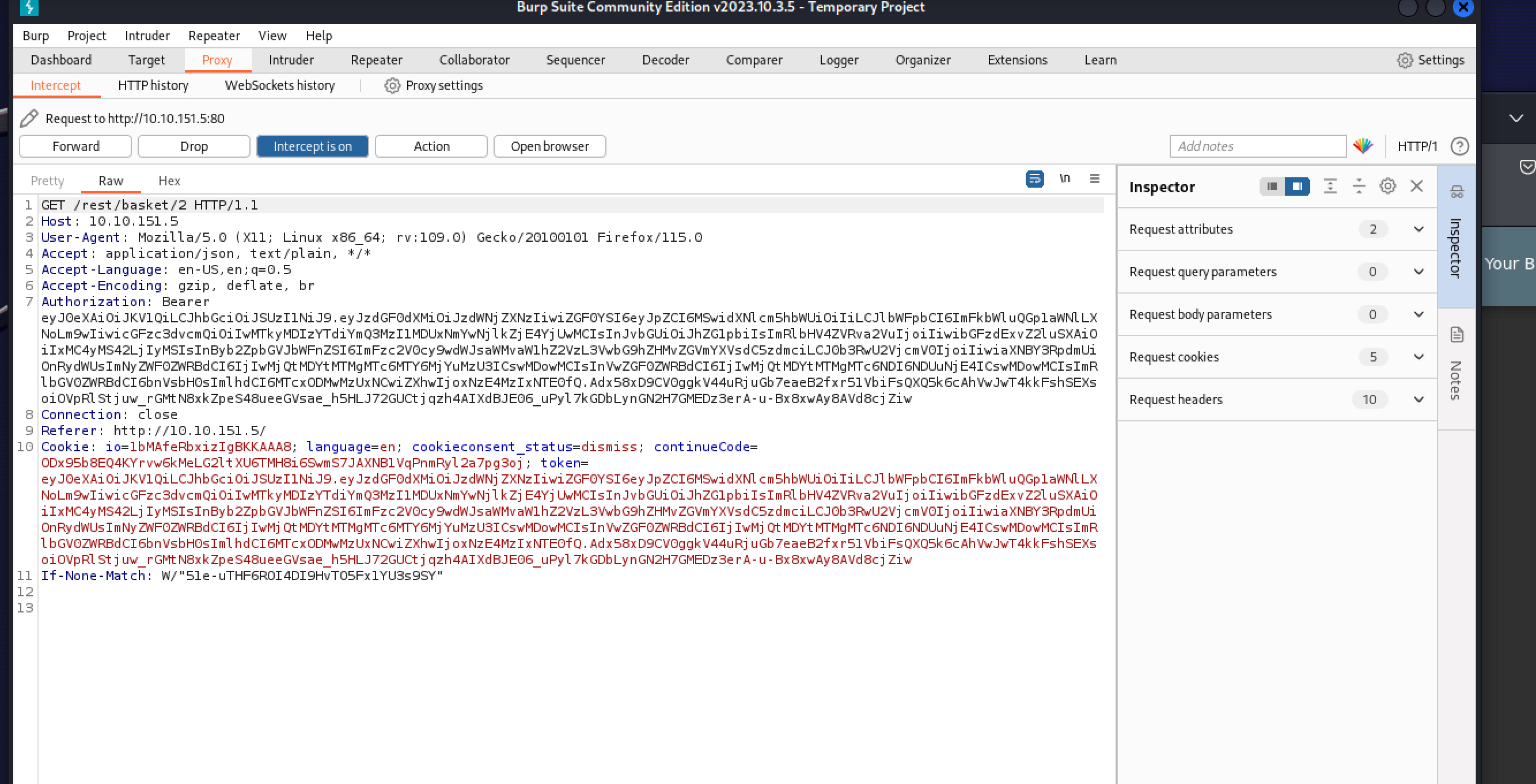


* When we login using the admin username and password and navigate to the administration page, this is what it looks like.

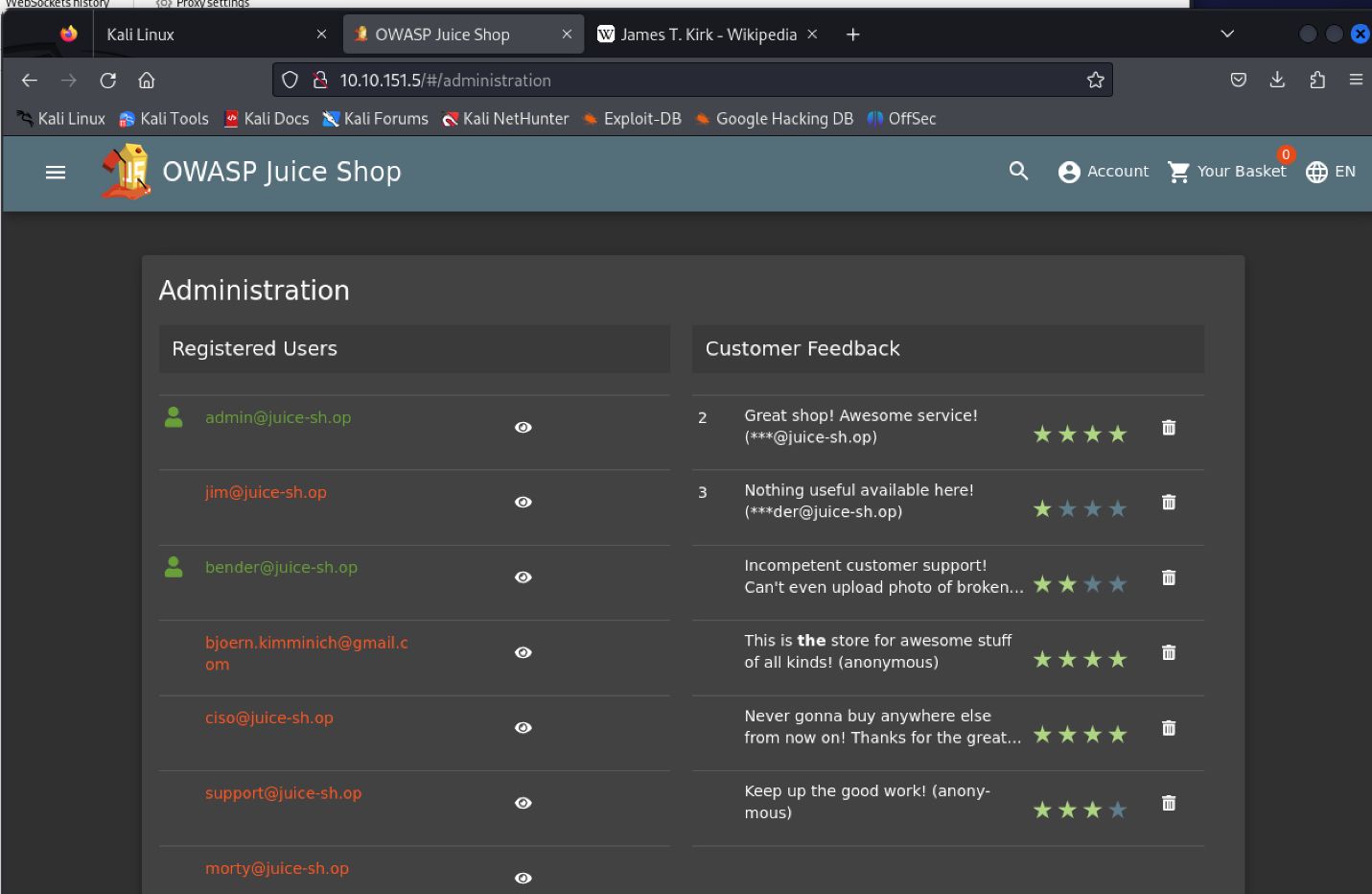


1. Login to the Admin account and clicking on 'Your Basket' and capturing the request using burp suite and altering the request.

* we are going to change the number 1 after /basket/ to 2 on GET

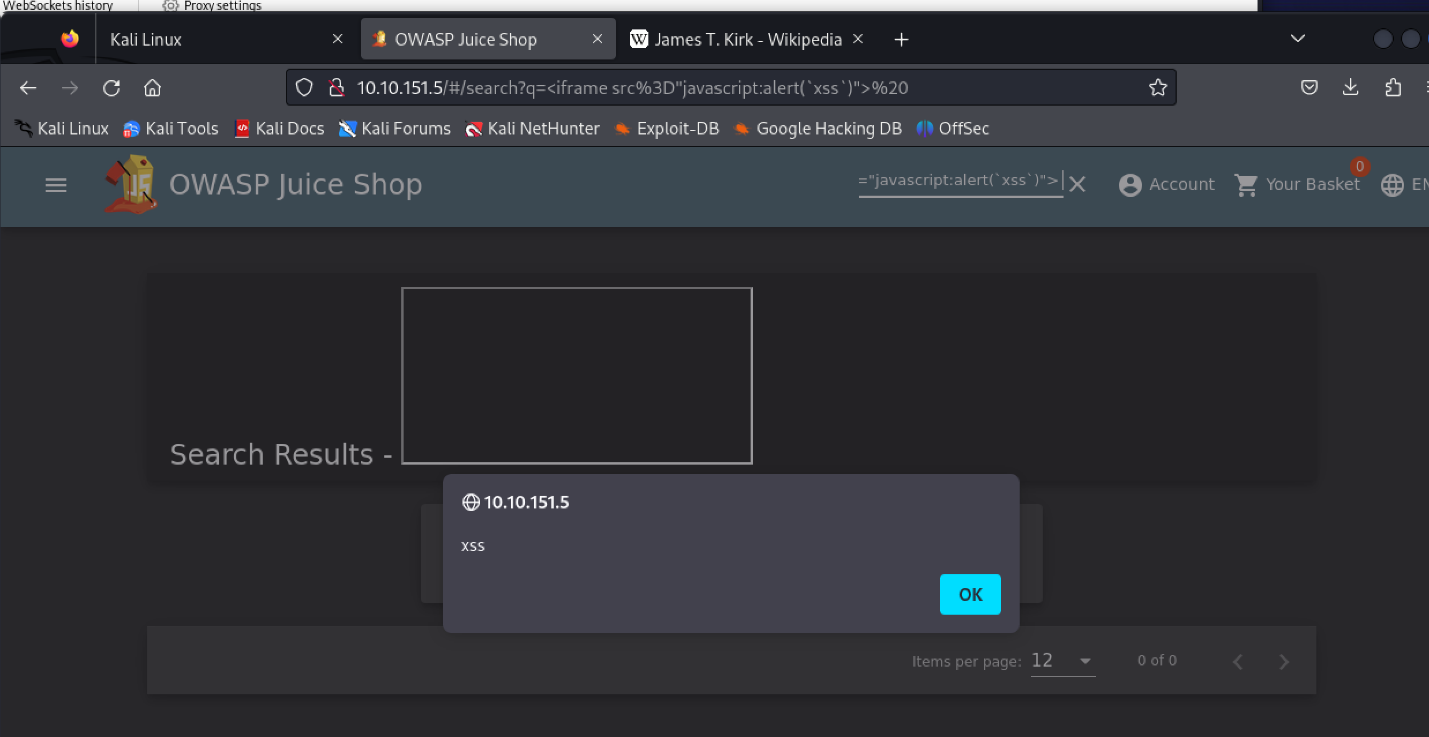


1. We can also delete staff after privilege escalation, for instance we will delete the review with 5 stars on the administration page we saw above.

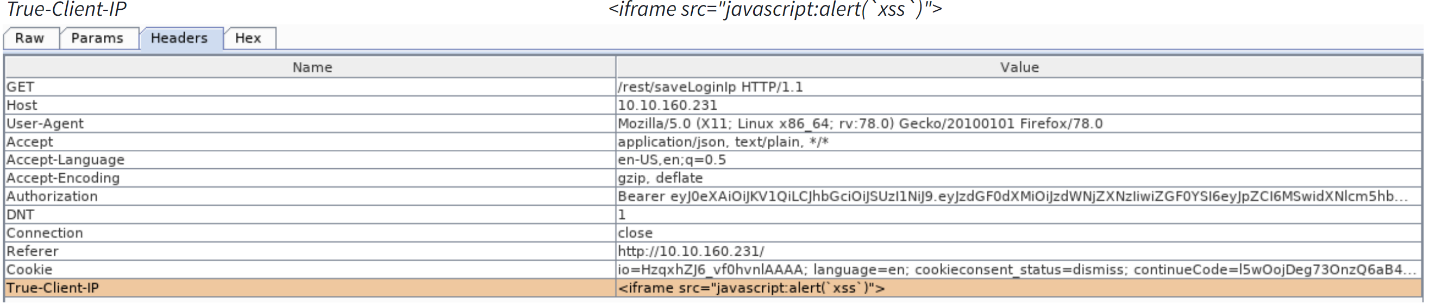


1. Here we will see XSS (Cross site scripting), so let’s define it and its types.

* **XSS**: is a vulnerability that allows attackers to run javascript in web applications.
* **DOM XSS**: uses the HTML environment to execute malicious javascript.
* **Persistent XSS**: is javascript that runs when the server loads the page containing it.
* **Reflected XSS**: is javascript that is run on the client-side end of the web application.
* Now to perform DOM XSS attack we are going to use a HTML tag called **iframe** with javascript alert tag.
* <iframe src="javascript:alert(`xss`)"> we will type this on our search bar and attack the server cause it doesn’t have correct input sanitation.
* This type of XSS is called Cross-Frame Scripting.



* To perform Persistent XSS we will do the following, we will still be using the iframe.
* First Login to admin and go to last login ip and you will see an Ip.
* Then turn intercept on and log out and capture the request.
* Then go to the Headers tab and add a header and forward it

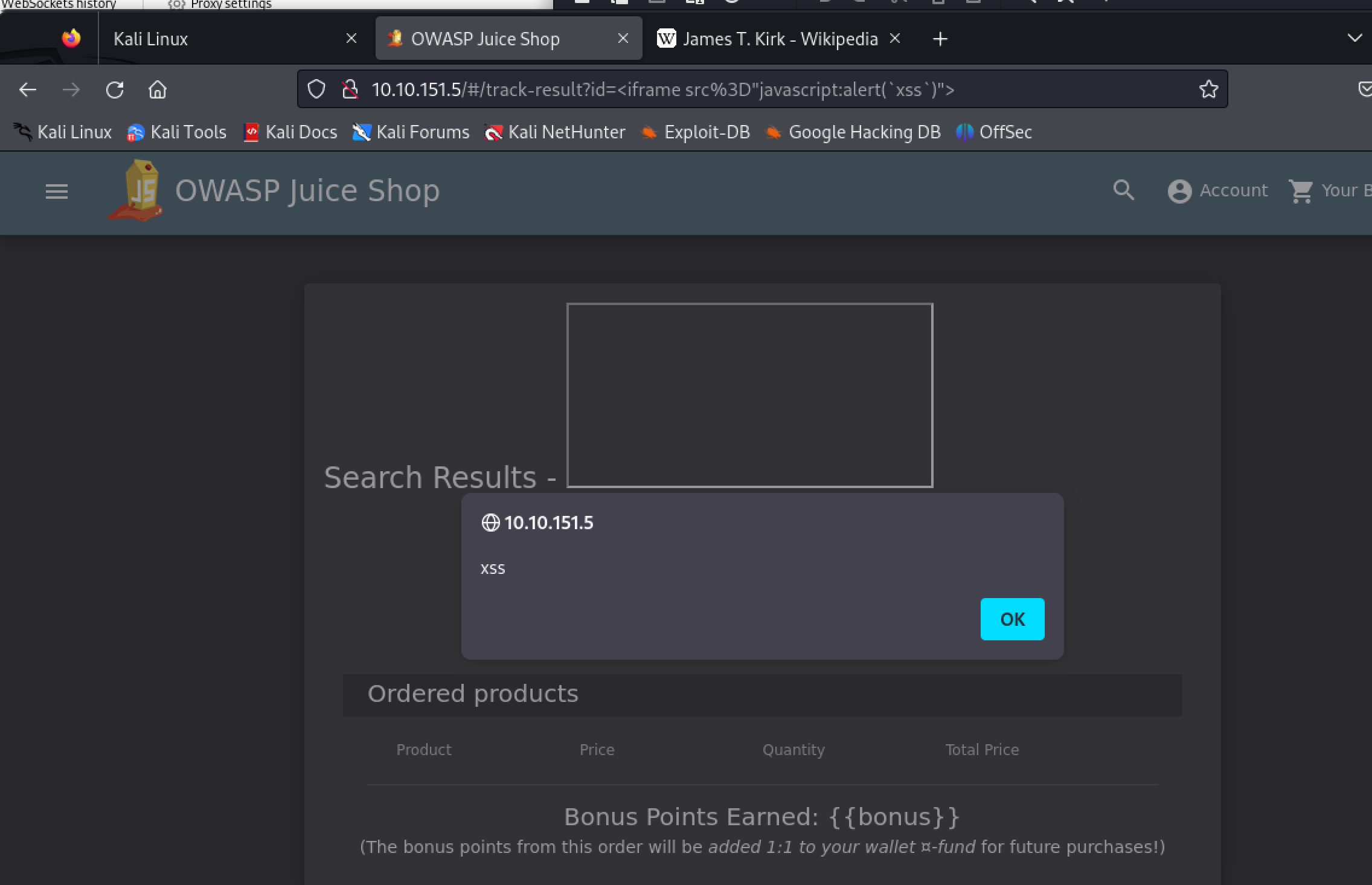


* Now when login in and going to the last login you will see the XSS alert.

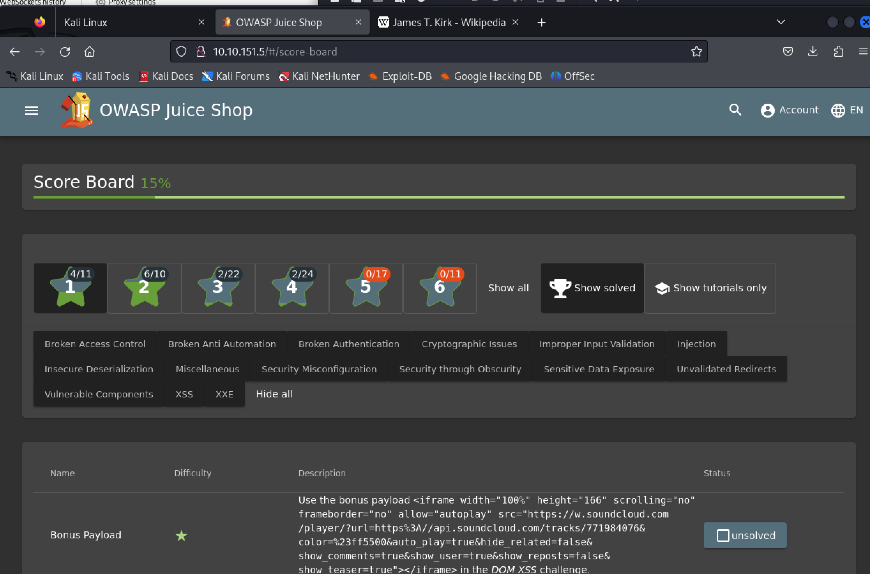
A screenshot of a computer

Description automatically generated

* To perform a reflected XSS, we will be doing the following:
* Login to the admin page and navigate to the order history
* Then click the truck icon and you will see the truck result on the url with id=
* Now replace what is after the id= with <iframe src="javascript:alert(`xss`)"> on the url and run the script



1. Finally, we will explore the /#/score-board and see what tasks we have done



1. Last but not least the accomplishments page

