**Task 1 (Open for business!)**

**Q: Deploy the VM attached to this task to get started! You can access this machine by using your browser machine, or if you’re connected through**OpenVPN**.**

No answer needed

Q: **Once the machine has loaded, access it by copying and pasting its IP into your browser; if you’re using the browser-based machine, paste the machines IP into a browser on that machine.**

No answer needed

**Task 2 (Let’s go on an adventure!)**

**Q: What’s the Administrator’s email address?**

A screenshot of a computer

Description automatically generated

**Reviews on products display the user's email address. We can view the administrator's email by clicking the first product.**

**Q: What parameter is used for searching?**

****

Simply searching in the search field reveals that the search parameter following the page url is the letter q.

**Q: What show does Jim reference in his review?**

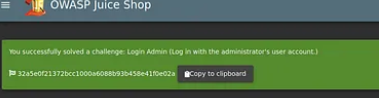
****

We can tell it's from Star Trek by Googling replicator.

**Task 3 (Inject the Juice)**

**Q: Log into the administrator account!**

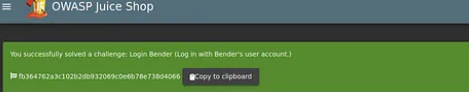
**We can enter**  **‘ or 1=1 —  in the email field** and forward our request .



**OR' in a SQL query returns true if both sides are true. Because 1=1 is always true, the entire statement is correct. As a result, it will notify the server that the email is valid and log us into user id 0, which is the administrator account.**

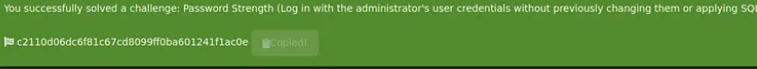
**Q: Log into the Bender account!**

**Following similar approach as above, we can log in.**



**Task 4 (Who broke my lock?)**

**Q: Brute force the Administrator account’s password!**



We will intercept a login request using burp suite and transmit it to Intruder. Then we will select the Clear button after going to Positions.

In the password field we will then place two § inside the quotes marking the position we will be doing the brute force attack on.

For the payload, we will be using the default wordlist that comes in kali “rockyou.txt” and start our attack.

We will get the password and so we can log in.

**Q: Reset Jim’s password!**



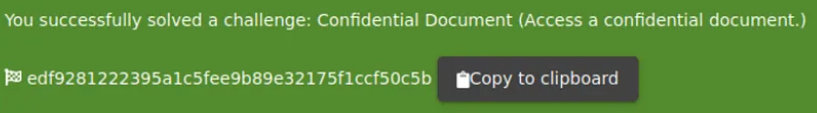
 Jim’s security question is set to “Your eldest siblings middle name?”*.*

We discovered in Task 2 that Jim might be connected to Star Trek. We may get Jame T. Kirk's wiki page by searching "Jim Star Trek" on Google. He has a brother, as we can see from his wiki page. It appears that Samuel is his brother's middle name.

You can successfully change his password by entering that information on the Forgot Password page. Any alteration you wish can be made!

**Task 5 (AH! Don’t look!)**

**Q: Access the Confidential Document!**



Hover your cursor over "Check out our terms of use" on the About Us page. It links to http://10.10.38.60/ftp/legal.md, as you can see. When you navigate to the /ftp/ directory, you can see that it is accessible to everyone.

We'll save the acquisitions.md file after downloading it. There appear to be additional interesting files present. Go to the home page after downloading it to get the flag.

**Q: Log into MC Safe Search’s account!**

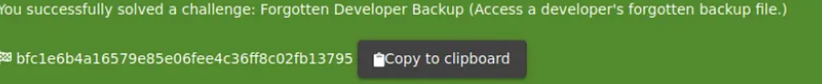


Following the viewing of the video, some elements of the song stick out.

Mr. Noodles is his password, but he says that he has changed certain "vowels into zeros," which simply means that he changed the o's into 0's.

We now know that "Mr. N00dles" serves as the account's password for [mc.safesearch@juice-sh.op](mailto:mc.safesearch@juice-sh.op).

**Q: Download the Backup file!**



Returning to the http://10.10.38.60/ftp/ subdirectory, we will try to download package.json.bak at this time. However, it appears that we are only allowed to download.md and.pdf files after receiving a 403 error.

We will employ a character bypass known as "Poison Null Byte" to get past this. This is how a Poison Null Byte appears: %00.

(Encoding) Now, the Poison Null Byte will appear as follows:%2500. The 403 error can be avoided by adding this followed by a.md to the end!

**Task 6 (Who’s flying this thing?)**

**Q: Access the administration page!**

A screenshot of a computer

Description automatically generated

We'll start by launching Firefox's Debugger. You can do this by selecting it from the Web Developers menu.

Next, we'll reload the page and search for a javascript file containing main-es2015.js. After that, we'll navigate to that page at 10.10.38.60/main-es2015.js. Click the bottom button to convert this into a format we can read.

Do a search for "admin" right now. There are a few words that contain "admin," but the one we're looking for is "path: administration."

The about path a few lines below indicates that this points to a page called "/#/administration," however accessing it while not logged in is ineffective.

It makes logical that we need to be in the Admin account in order to read this page since it is an Administrator page. Visit the /administration page after logging into the admin account.

**Q: View another user’s shopping basket!**

A screenshot of a computer

Description automatically generated

Log in to the Admin account and go to the 'Your Basket' section. Check that Burp is running so that you can capture the request! Continue forwarding each request until you see: HTTP/1.1 GET /rest/basket/1. Now we'll replace the number 1 after /basket/ to 2. It will now display UserID 2's basket. You can do the same for other UserIDs, as long as they have one!

**Q: Remove all 5-star reviews!**

Navigate to the <http://10.10.38.60/#/administration> page again and click the bin icon next to the review with 5 stars!

**Task 7 (Where did that come from?)**

**Q: Perform a DOM XSS!**

A screenshot of a computer

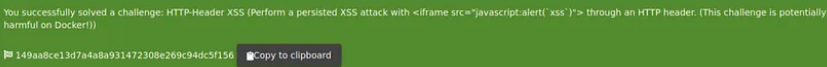
Description automatically generated

<iframe src=”javascript:alert(`xss`)”>

Inputting this into the search bar will cause the alert to be triggered.

This sort of XSS, also known as XFS (Cross-Frame Scripting), is one of the most popular types of XSS detection in online applications. Websites that allow users to change the iframe or other DOM components are likely to be vulnerable to XSS.

**Q: Perform a persistent XSS!**

****

To begin, log in to the admin account. For this assault, we will go to the "Last Login IP" page.

The last IP address should be listed as either 0.0.0.0 or 10.x.x.x. We will now log out so that it may record the "new" IP as it records the "last" login IP.

To ensure that the logout request is intercepted, turn on Burp intercept. Next, we'll switch to the Headers tab and add a new header.

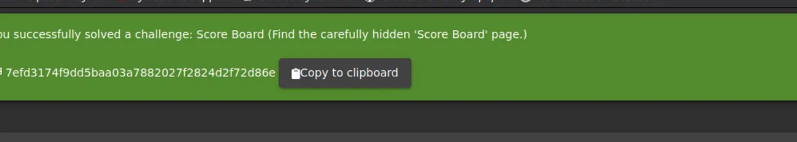
**Q: Perform a reflected XSS!**

Go to the 'Order History' tab after logging into the admin account.

A "Truck" icon will appear there; clicking on it will take you to the track result page. You'll also see that the order is coupled with an id. We'll employ iframe XSS. When you submit the URL and then reload the page, an XSS warning will appear.

**Task 8 (AH! Don’t look!)**

**Q: Access the /#/score-board/ page**

****