# Objective: Recover the Ring of Fire—Answers Only

## Buy a Hat

The process should be simple. Select a hat at the vending machine, then go to the KTM and authorize a transfer for the price of the hat to the vending machine’s wallet. Return to the vending machine to complete the purchase.

Text

Description automatically generated

Here is a sample transaction as an example. Record the Block number so you can find your transaction in the blockchain. Over 100,000 blocks in the chain already! Wow.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

## Blockchain Divination

The contract address is in the first block  
Text, email

Description automatically generated

## Exploit a Smart Contract

### Answer 1: A Problem with the Site

When you try to send a made up walletID and proofs to the BSRS site, it tells you (rudely) that you are not on the Merkle tree and cannot purchase an NFT. This is expected.  
Text

Description automatically generated

When you look at the request the browser sends to BSRS (this is the Network tab of Firefox web developer tools) you see something interesting.  
Graphical user interface, text, application, email

Description automatically generated

The browser needs to send the WalletID, Proof, and Session key, but why does it send Root? The root of a Merkle tree is unique to the tree—you could say that it specifies the tree. If we can get them to check our WalletID and Proof against a Root that we give them, we could trick them into validating that we are in our own tree instead of validating our presence in their tree.

In the early days of the Internet, some web stores allowed the browser to send the price of an item in the purchase request to the server. Enterprising people soon learned they could change the price of the item sent to the store. Then you could buy a $500 TV for $1! The BSRS site allowing the browser to send the Root of the tree is essentially making the same mistake.

So, if we create a tree that includes our WalletID, we can send our Root instead of theirs. Before we can create a tree, we need to install the [software in Prof. Q’s repo](https://github.com/QPetabyte/Merkle_Trees).

### Answer 2: Install merkle\_tree.py

Git and Docker are supported on most major operating systems. Here are [instructions for installing Git](https://git-scm.com/book/en/v2/Getting-Started-Installing-Git), and here are [instructions for installing Docker](https://docs.docker.com/engine/install/).

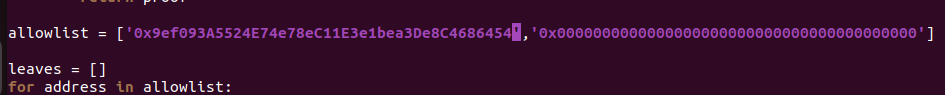
Once you have Git and Docker installed just clone Prof. Q’s repo, build it, and run it in Docker. These commands will work in Ubuntu.  
git clone <https://github.com/QPetabyte/Merkle_Trees.git>  
cd Merkle\_Trees  
sudo docker build -t merkletrees .  
sudo docker run -it --rm --name=merkletrees merkletrees

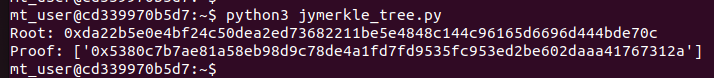
### Answer 3: Create a Merkle Tree

You will need to edit merkle\_tree.py to put your WalletID into the allow list. However, you do not have the permissions to do that.  


Just copy the file, and you will have the correct permissions for the copy.  
Text

Description automatically generated

Edit merkle\_tree.py with vim or nano to insert your WalletID into the allow list. I chose to replace the entry for 0x1337133713371337133713371337133713371337 with my WalletID. By default, the program computes the proof for the first item [0] in allowlist. 

The program will give you the root and the proof that go with your tree and WalletID.  


### Answer 4: Plant Your Merkle Tree

Firefox has a useful feature under the Network tab called Edit and Resend. It is helpful when you do not want to bother with spinning up Burp Suite.

Using Firefox, enter your walletID and your proof into the BSRS presale page so that all you will have to edit is the root value. Open the webdev tools if you haven’t already, and select the Network tab. Then click Go! on the BSRS presale page. They will deny your request saying that you are not on the list, but that is fine, the attack is coming.

Find the packet you just sent in the Networking tab and right-click on it. One of the choices is Edit and Resend, which is exactly what we want to do.  
Graphical user interface, text, application

Description automatically generated

The Body is shown at the bottom of the page. If you put your walletID and proof into the web page before you clicked Go, all you edit is the root. Change the root to the value you got from the merkle\_tree.py script. Now you are telling BSRS to check that your walletID is in the tree you created, and not theirs. The silly sporcs do it.Graphical user interface, text, application, email

Description automatically generated

You should get a message telling you that you have been validated and can purchase an NFT.

### Answer 5: Buy an NFT

Follow the steps properly, and the BSRS site will take your 100 KC and give you this message.

*Success! You are now the proud owner of BSRS Token #000147. You can find more information at* [*https://boredsporcrowboatsociety.com/TOKENS/BSRS147,*](https://boredsporcrowboatsociety.com/TOKENS/BSRS147,) *or check it out in the gallery!<br>Transaction: 0xccad6b3c139676d81d4f488f1cbd731d0ef7c4bee8b421548bf279f1bc782a85, Block: 58630<br><br>Remember: Just like we planned, tell everyone you know to <u><em>BUY A BoredSporc</em></u>.<br>When general sales start, and the humans start buying them up, the prices will skyrocket, and we all sell at once!<br><br>The market will tank, but we'll all be rich!!!*

The link will show you your NFT. Your NFT is also available in the BSRS Gallery, although you may have to scroll for a while to find it. You can look up your Block number in the Blockchain Explorer and see your transaction recorded there all time (or at least while the blockchain exists.) Congratulations!