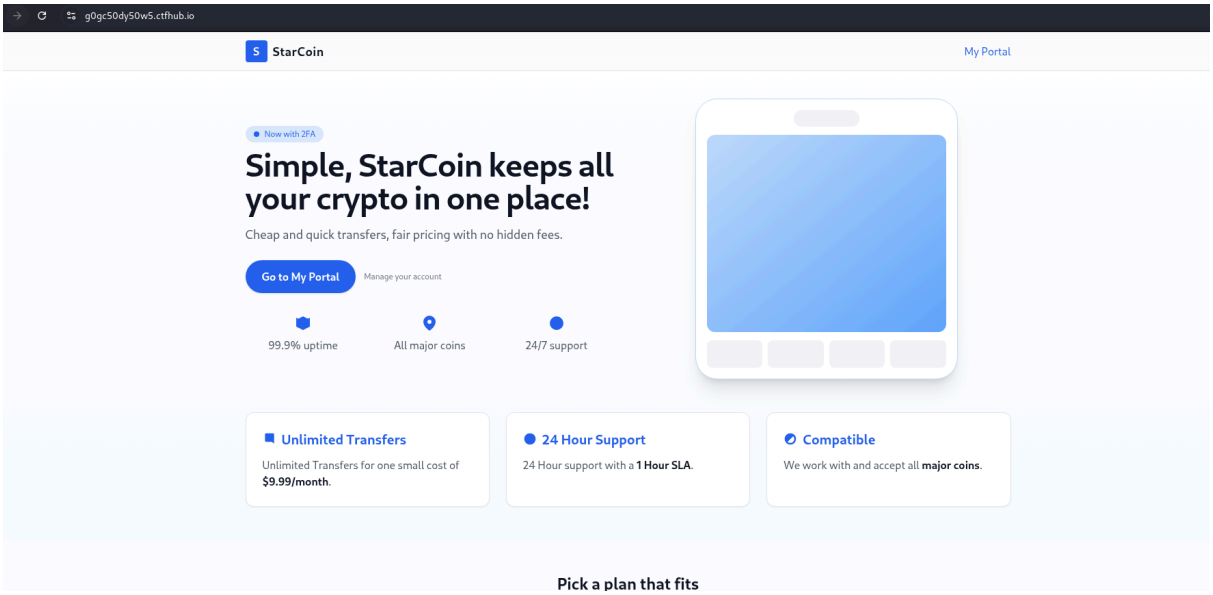
2FA Madness

Description

```
We've found an authentication problem on this website.

Use the below login details as an example but then try and
hack the second account when you've found the bug!
Account One:

Mobile: +1-415-555-0000

Password: password

2FA Code: 123456
Account Two:

Mobile: +1-415-555-9999

Password: hunter2

2FA Code: Can you bypass it?
```

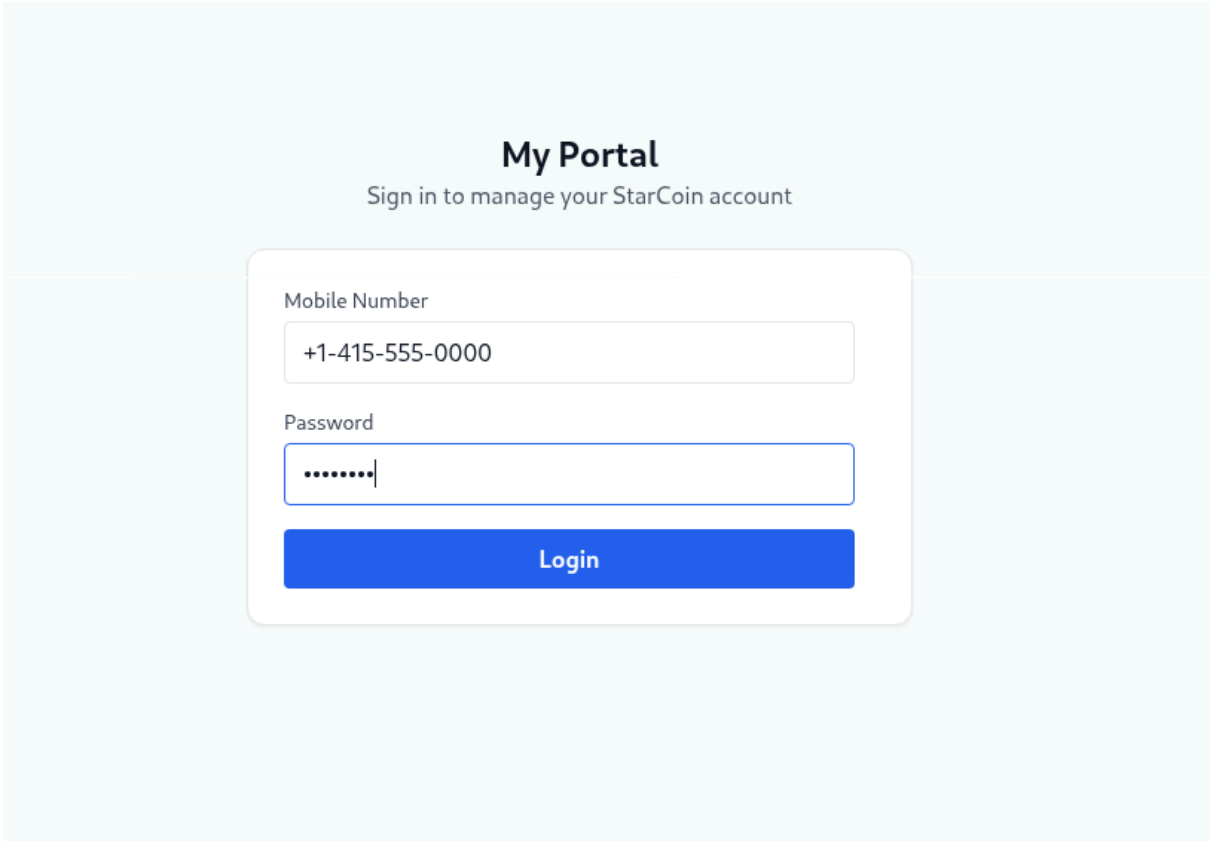
Scope: g0gc50dy50w5.ctfhub.io
OSINT Domain: N/A

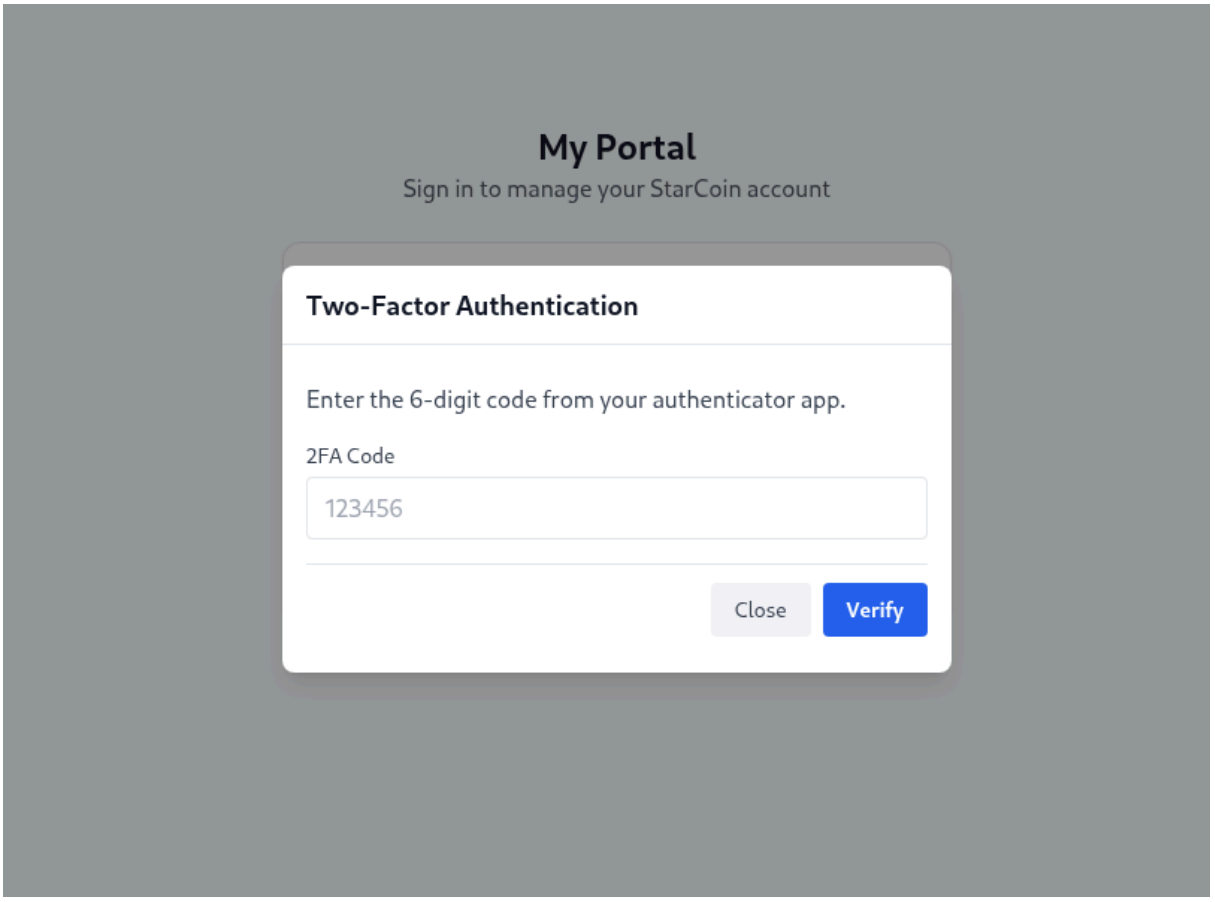
This is the homepage



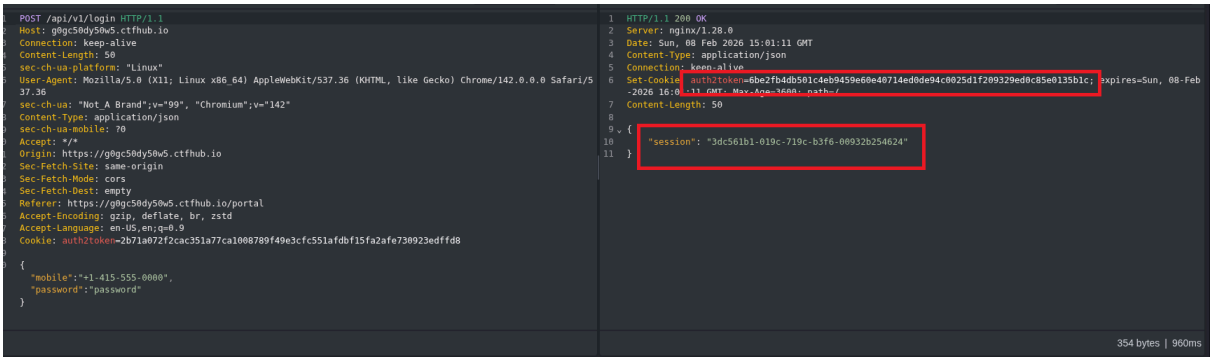
Clicking on the `My Portal` on the top right directs us to the login page.

Using the credentials provided in the challenge: +1-415-555-0000:password



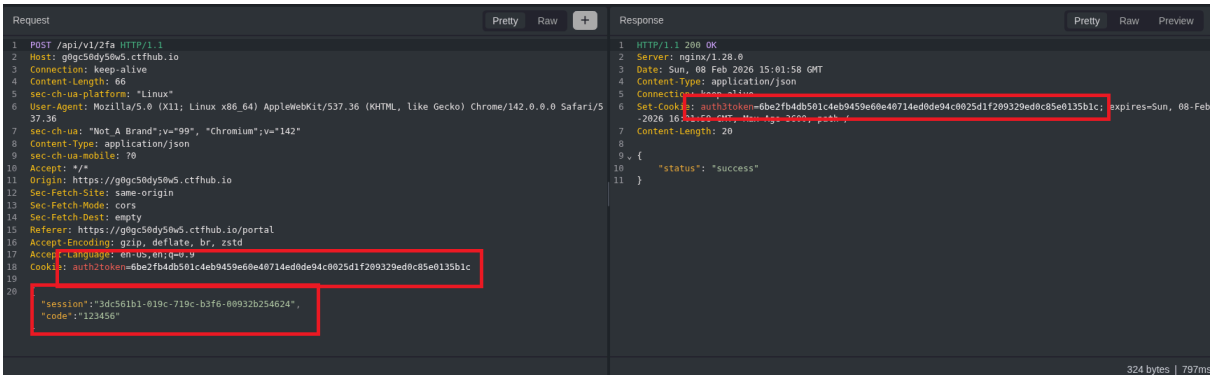


We are intercepting the requests in either Burp Suite or Caido. I am using Caido



Upon entering phone number and password, and sending the request, a session is created. And a cookie named `auth2token` is set.

This is session is used when we send the OTP.

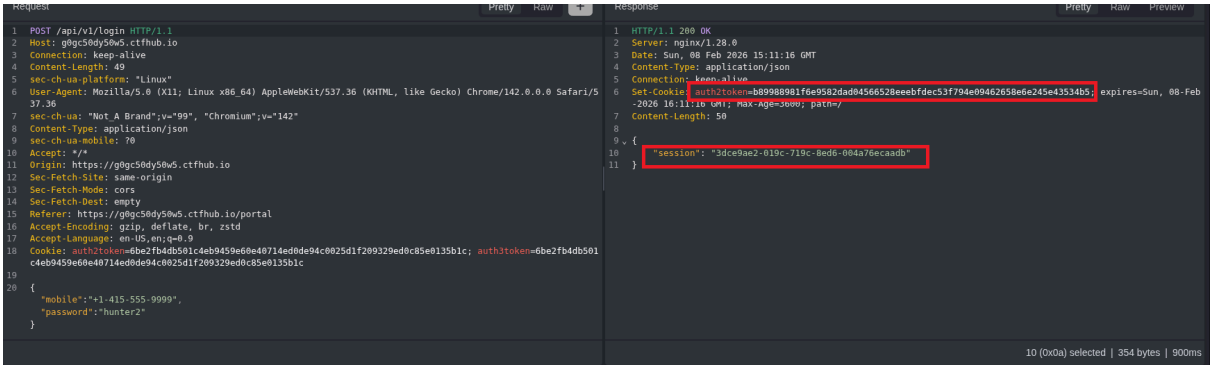


The `auth2token` and the `auth3token` is the same.

After logging, when a POST request to access the account is sent, both the cookies, `auth2token` and `auth3token` is sent and also the session, which was created when the phone number and password was entered and sent, is also sent.

So to access the other account, we just need the session cookie and auth2token.

Session cookie can be obtained by entering the phone number and the password. And the Response to this Request will give us the auth2token.



Ignore the already set auth2token and auth3token.

We have to use the session cookie and the auth2token to access the account.

Send the request from the account 1 to repeater, changed the required cookie and sent the request.