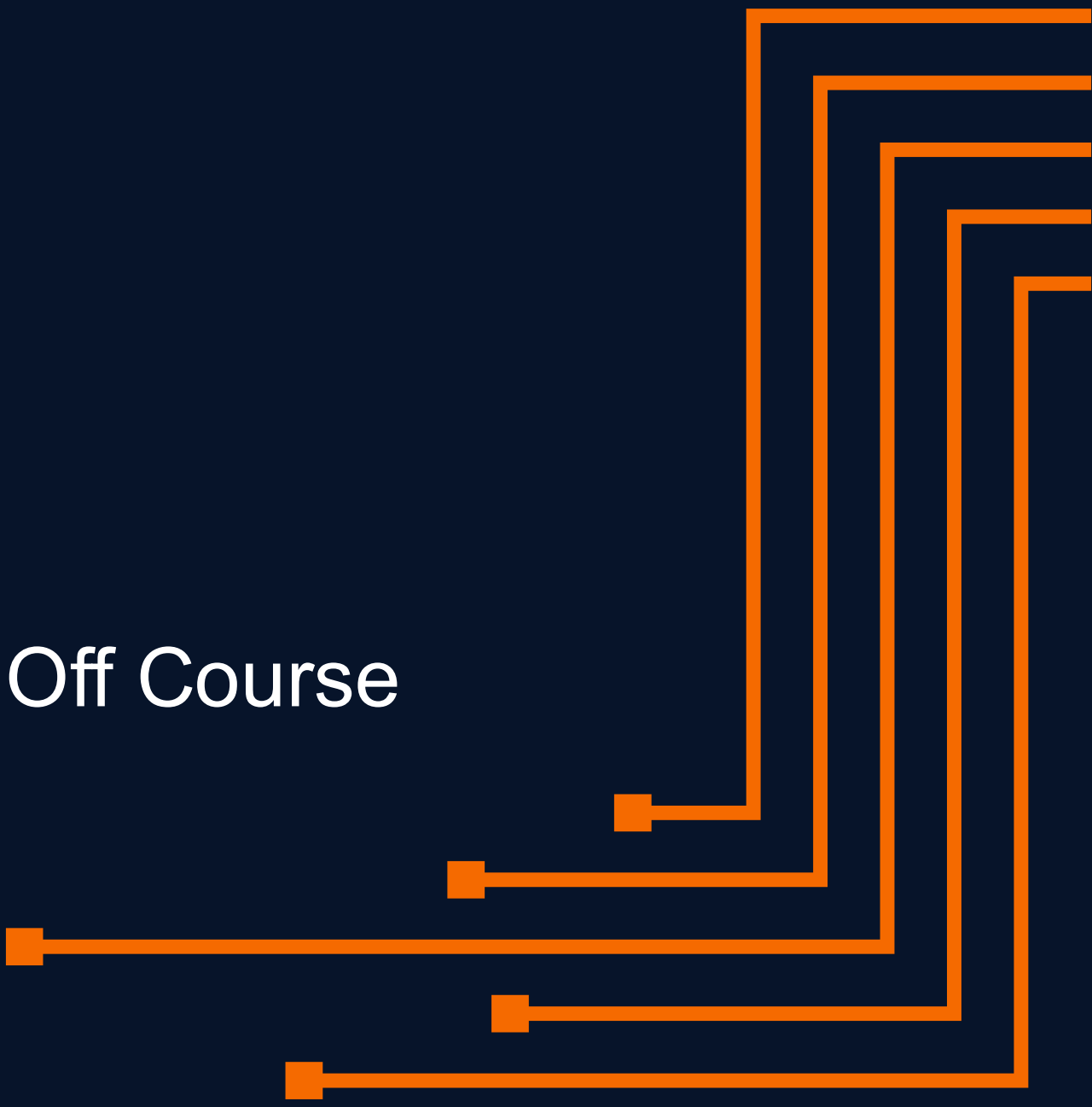




Rudder Nonsense: Steering Smart Rowers Off Course

Presented by Shane Kell, Senior Security Consultant

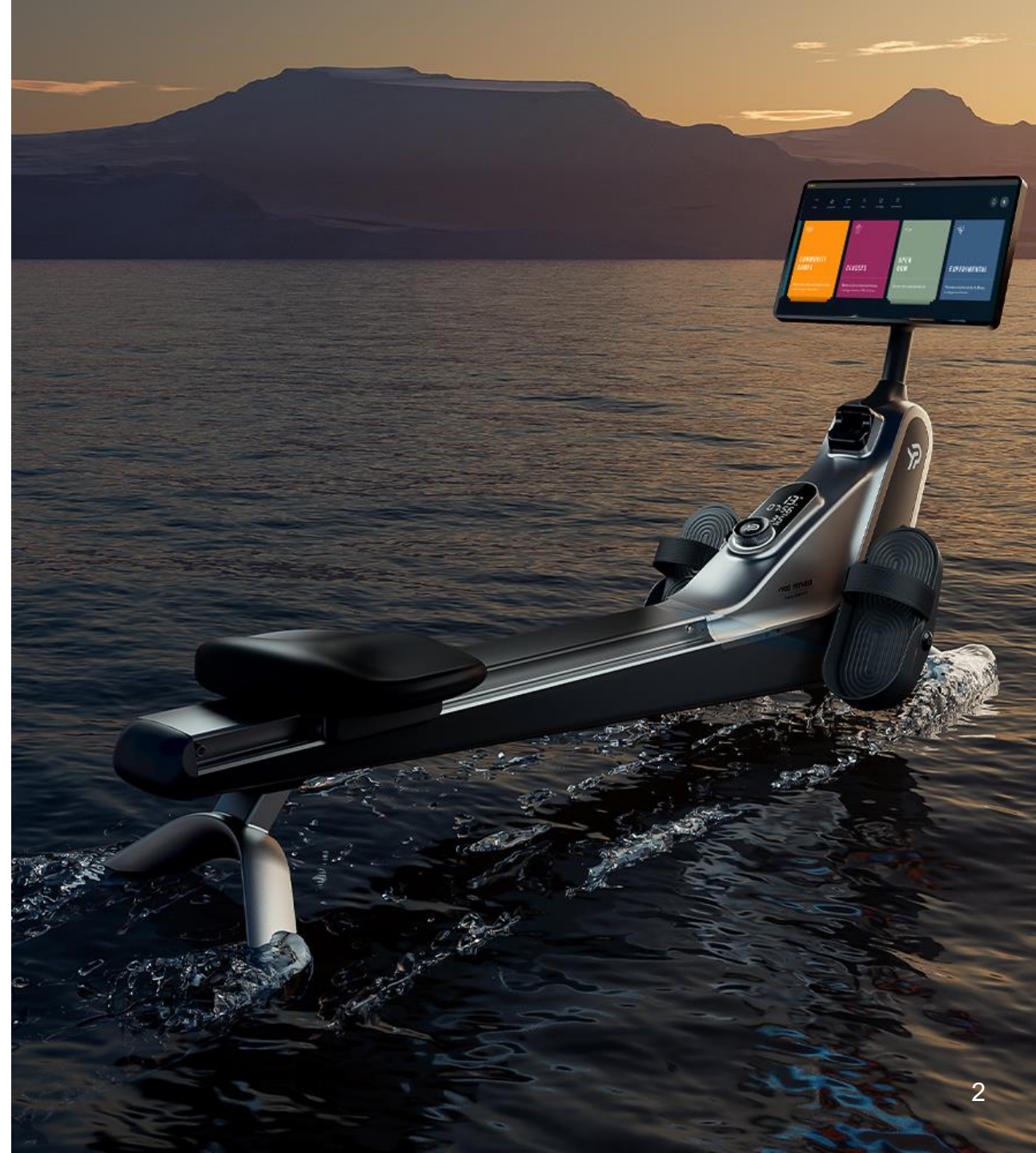
10.25.24





The Rower

- Smart rowing machine
- Android-powered user interface
- Gamified workout experience requires a subscription
- Rower is usable without subscription as a normal machine





Phase 1:

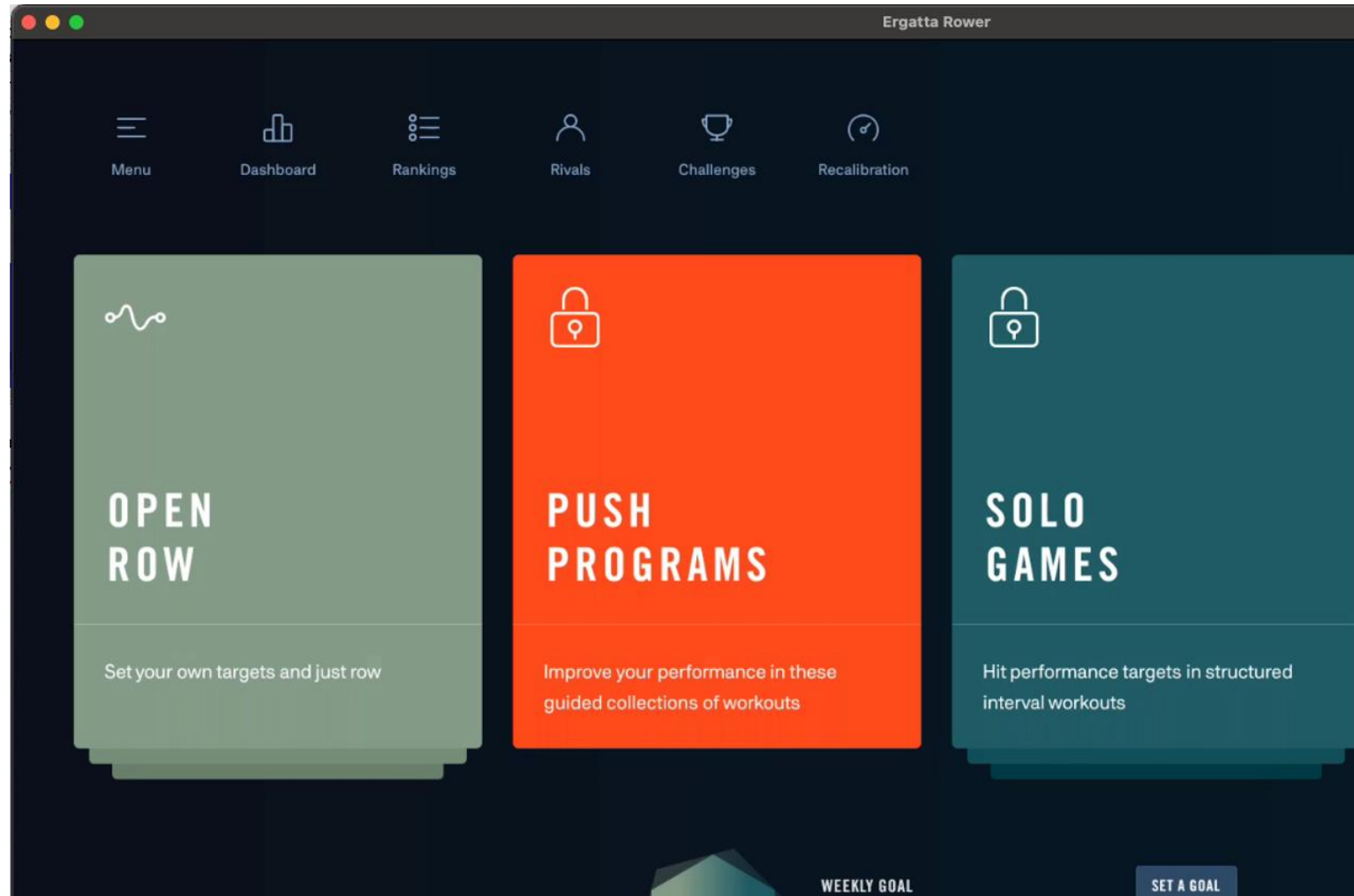
Proxying and Manipulating Traffic

- What traffic is it sending?
- How is it handling authorizations?



The Lay of the Land

- Auto loads workout app on startup
- No virtual or physical buttons
- Locks denote modes that require a subscription
- Nmap port scan reported all ports closed





External Ports

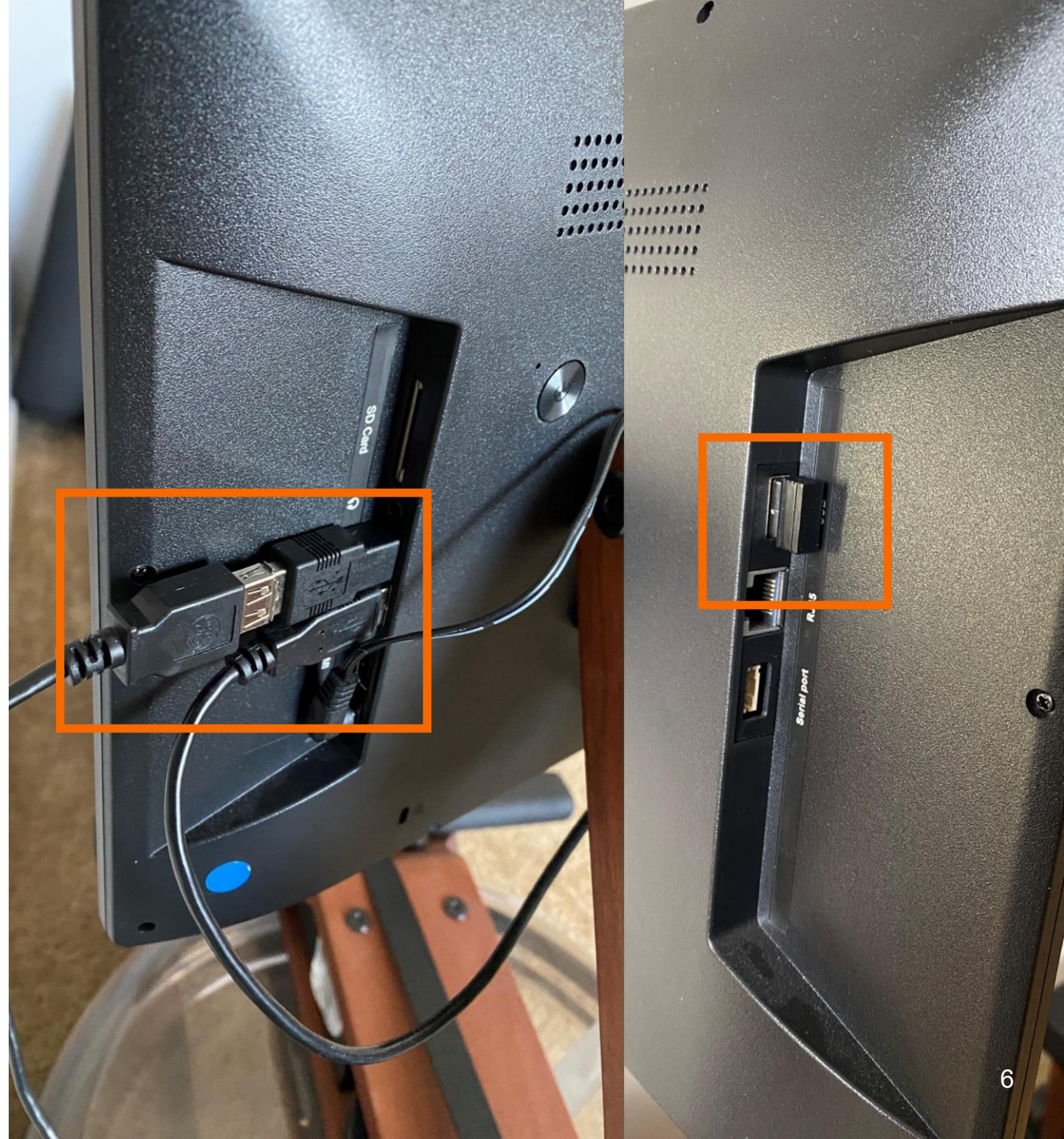
- Two open USB ports on the back





External Ports

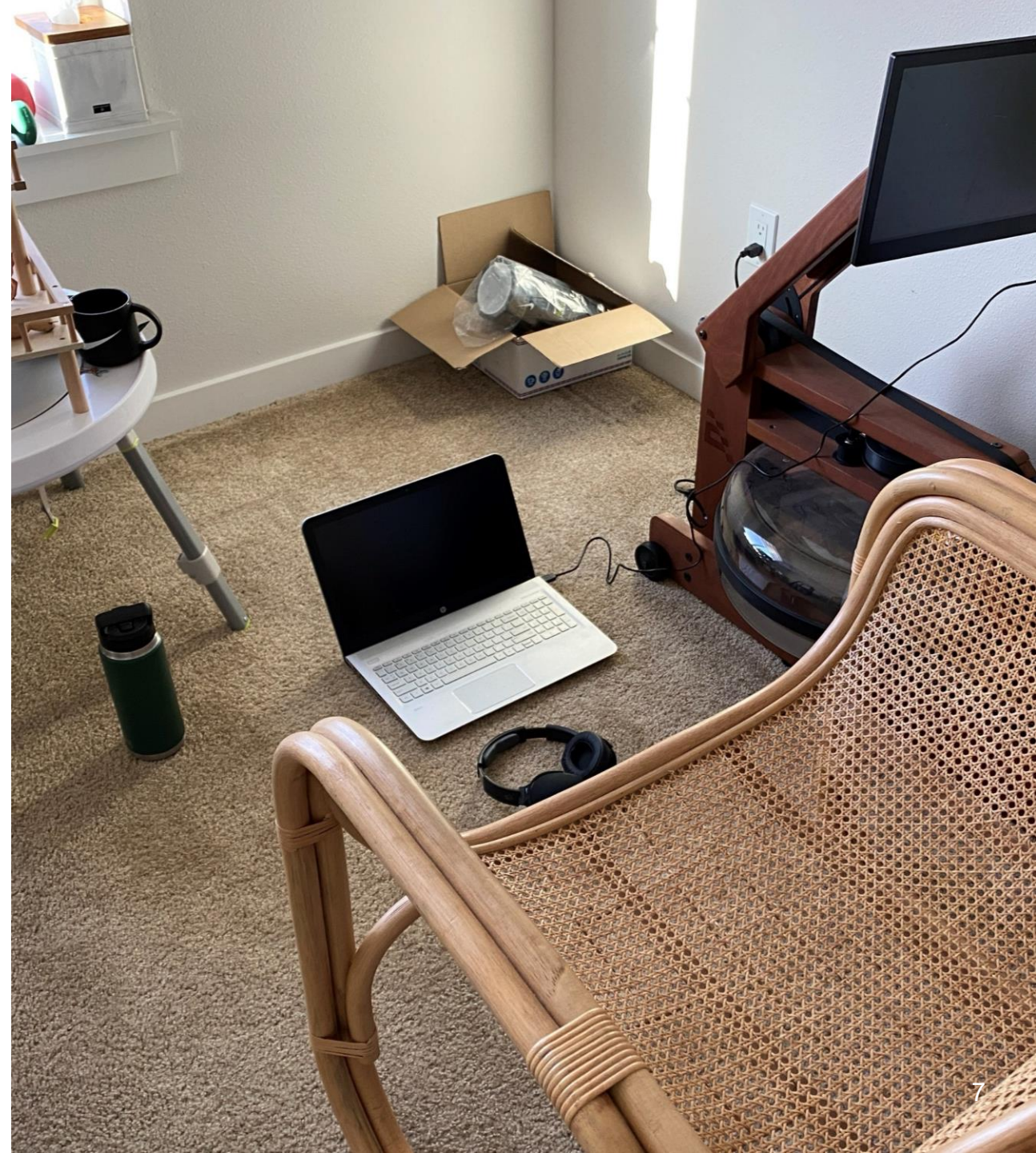
- Two open USB ports on the back
- Keyboard dongle on the left
- Mini-USB adapter on the right connected to laptop





Next Steps

- alt+tab to switch views on the tablet display
- Loaded the settings menu
- Enabled developer options
- Enabled USB debugging





Android Debug Bridge (ADB)

- Rename Burp cert to be compatible with Android

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ ls
cacert.der
```

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ hashed_name=`openssl x509 -inform DER -subject_hash_old -in cacert.der | head -1` && cp cacert.der $hashed_name.0
```

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ ls
9a5ba575.0 cacert.der
```

- Remount system directory to be writable
- Push the cert
- Alter cert permissions
- Reboot

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ adb root
restarting adbd as root
```

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ adb remount
remount succeeded
```

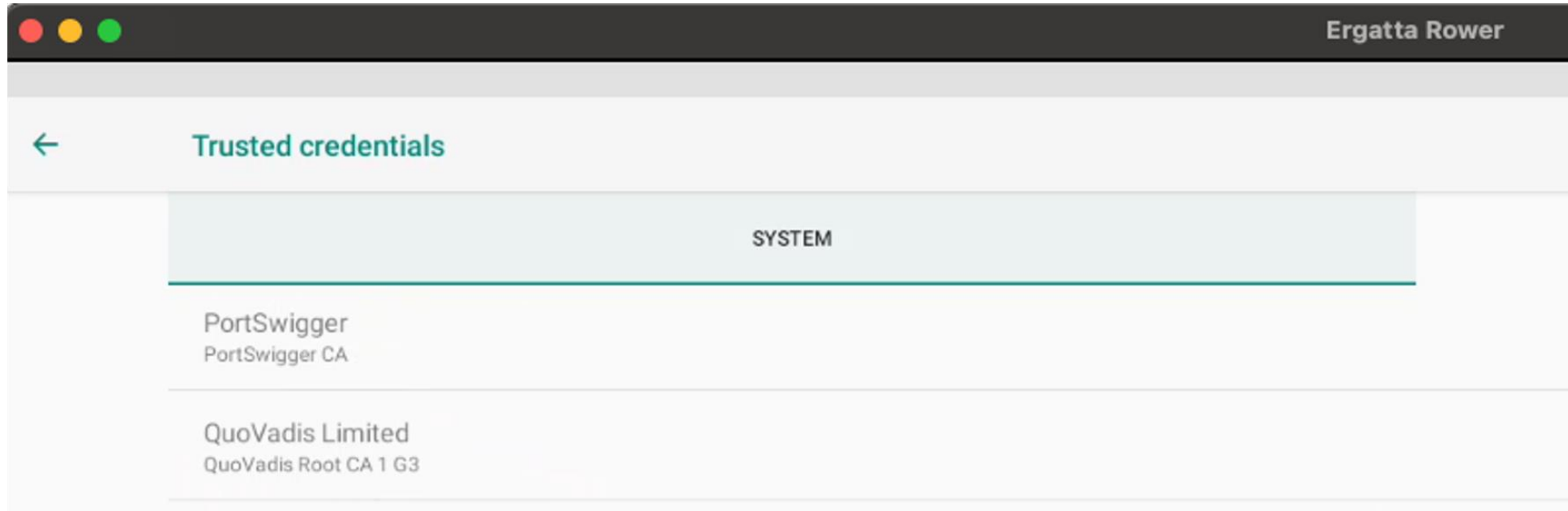
```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ adb push 9a5ba575.0 /system/etc/security/cacerts
9a5ba575.0: 1 file pushed, 0 skipped. 3.7 MB/s (940 bytes in 0.000s)
```

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ adb shell chmod 664 /system/etc/security/cacerts/9a5ba575.0
```

```
(assess|US-JPV2X61YKD|z)-[2.7.18]-[~/test]
$ adb reboot
```



Burp CA in Trusted Credentials





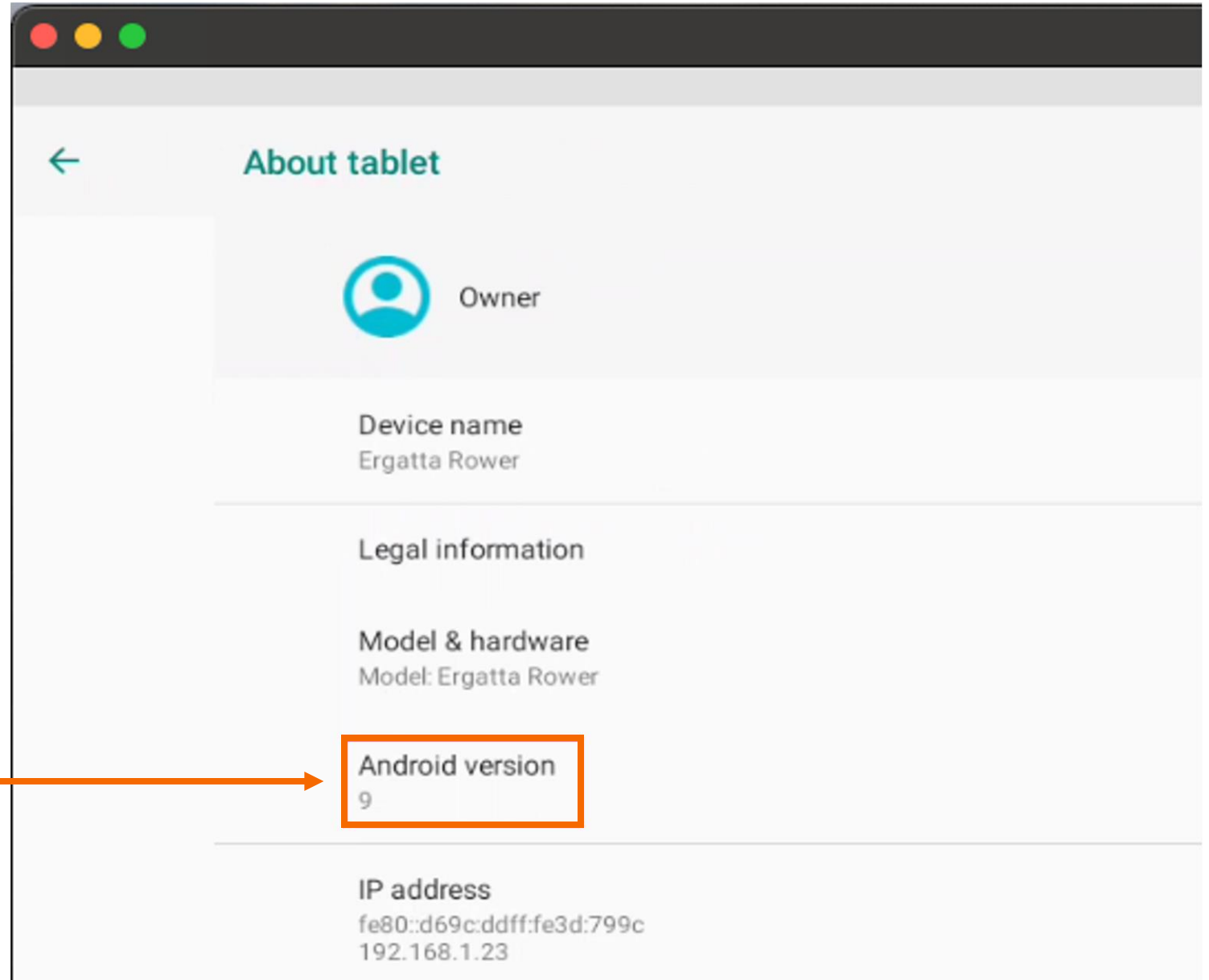
Wait...

You can't just remount
system to be writable in
current versions of Android.





Android Version





Configure Burp Proxy Listener

From Proxy Listeners:

- Select Edit
- Specific Address
- Then the internal network interface

The screenshot shows the 'Proxy listeners' configuration window in Burp Suite. It features a table with columns: Running, Interface, Invisible, Redirect, and Certificate. Two listeners are listed: one on 192.168.1.3:8000 and another on 127.0.0.1:8080, both marked as 'Per-host'. Below the table, the 'Edit proxy listener' dialog is open, showing the 'Binding' tab. The 'Bind to port' is set to 8000, and 'Bind to address' is set to 'Specific address' with the value 192.168.1.3.

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use the proxy.

Running	Interface	Invisible	Redirect	Certificate
☒	192.168.1.3:8000			Per-host
☒	127.0.0.1:8080			Per-host

Edit proxy listener

Binding Request handling Certificate TLS Protocols HTTP

These settings control how Burp binds the proxy listener.

Bind to port:

Bind to address: ☐ Loopback only ☐ All interfaces ☒ Specific address:



Rower Upstream Proxy

- Edit the WiFi connection
- Set the proxy to manual
- Set proxy hostname and proxy port of your Proxy Listener

Fleming2
Password
(unchanged)

☐ Show password

Advanced options ^

Metered

Detect automatically ▼

Proxy

Manual ▼

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname
192.168.1.23

Proxy port
8081

Bypass proxy for
example.com,mycomp.test.com,localhost

IP settings

DHCP ▼

CANCEL SAVE



Check the Proxy

Intercept HTTP history WebSockets history Proxy settings						
Filter settings: Hiding CSS, image and general binary content						
#	Host	Method	URL	Params	Edited	Status code
28	https://feed.fm	POST	/api/v2/session	✓		200
27	https://images.ergatta.com	GET	/customers/profile/[REDACTED]/image			403
26	https://images.ergatta.com	GET	/customers/profile/0/image			403
25	https://api.ergatta.com	GET	/deleted_workouts?filter=deleted_at%3E2022-07-27T10%3A54%3A51.396-07%3A00	✓		200
24	https://api.ergatta.com	GET	/favorite_workouts?filter=updated_at%3E2023-09-30T10%3A39%3A45.779-07%3A00	✓		200
23	https://api.ergatta.com	GET	/notifications			200
22	https://api.ergatta.com	GET	/calibrated			200
21	https://api.ergatta.com	GET	/accounts/[REDACTED]/feature_flags			200
20	https://api.ergatta.com	GET	/accounts/[REDACTED]			200
19	https://images.ergatta.com	GET	/images/profiles/meta			200
18	https://api.ergatta.com	GET	/users/[REDACTED]			200
9	https://images.ergatta.com	GET	/customers/profile/[REDACTED]/image			403
8	https://api.ergatta.com	GET	/accounts/[REDACTED]			200
7	https://api.ergatta.com	GET	/update_cdn/metadata			200
6	https://api.ergatta.com	GET	/update_cdn/metadata			200
4	https://images.ergatta.com	GET	/customers/profile/0/image			403
3	https://firebase-remote-config-realtime.firebaseio.com	POST	/v1/projects/[REDACTED]/namespaces/firebase:streamFetchInvalidations	✓		
2	https://images.ergatta.com	GET	/images/profiles/meta			200
1	https://crashlytics-reports.firebaseio.com	POST	/v1/firelog/legacy/batchlog			200



Request for billing_state

Request

PrettyRawHexJSON Web Tokens

1GET /accounts/ HTTP/2
2Host: api.ergatta.com
3X-Rudder-Version: 33
4X-Seaborn-Flavor: standard
5Authorization: Bearer
6
7User-Agent: Seaborn/2024.08.01/1001
8Accept-Encoding: gzip, deflate, br
9

Response

PrettyRawHexRenderCopy Response

1HTTP/2 200 OK
2Date: Mon, 23 Sep 2024 17:52:03 GMT
3Content-Type: application/json; charset=utf-8
4Content-Length: 195
5Vary: Accept-Encoding
6
7{
8 "message": "ok",
9 "data": {
10 "billing_state": "Canceled",
11 "cbSubscriptionId": ,
12 "rootUserId": ,
13 "countryCode": "US",
14 "partner": null,
15 "id": ,
16 "created_at": "
17 }
18}





Request for billing_state

Request

PrettyRawHexJSON Web TokensCopy ...

1 GET /accounts/ HTTP/2
2 Host: api.ergatta.com
3 X-Rudder-Version: 33
4 X-Seaborn-Flavor: standard
5 Authorization: Bearer
6
7 User-Agent: Seaborn/2024.08.01/1001
8 Accept-Encoding: gzip, deflate, br
9

Edited response

PrettyRawHexRenderCopy Response

1 HTTP/2 200 OK
2 Date: Mon, 23 Sep 2024 17:56:30 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 193
5 Vary: Accept-Encoding
6
7 {
8 "message": "ok",
9 "data": {
10 "billing_state": "Active",
11 "cbSubscriptionId": ,
12 "rootUserId": ,
13 "countryCode": "US",
14 "partner": null,
15 "id": ,
16 "created_at": "
17 }
18 }



Request for feature_flags

Request

PrettyRawHexJSON Web Tokens

1GET /accounts/[redacted]/feature_flags HTTP/2

2Host: api.ergatta.com

3X-Rudder-Version: 33

4X-Seaborn-Flavor: standard

5Authorization: Bearer

[redacted]

6User-Agent: Seaborn/2024.08.01/1001

7Accept-Encoding: gzip, deflate, br

8

9

Response

PrettyRawHexRenderCopy Response

1HTTP/2 200 OK

2Date: Mon, 23 Sep 2024 17:52:03 GMT

3Content-Type: application/json; charset=utf-8

4Content-Length: 238

5Vary: Accept-Encoding

6

7{

8 "message": "success",

9 "data": {

10 "accountID": [redacted],

11 "canaryUpdateChannel": false,

12 "liveRaceUI": false,

13 "gameInfinity": false,

14 "classes": true,

15 "updateChannels": [

16 {

17 "name": "Main",

18 "baseUrl": "https://appupdates.ergatta.com/Se

19 }

20]

21 }

22}





Request for feature_flags

Request

PrettyRawHexJSON Web TokensCopy R...🔍📄ln≡

1GET /accounts/[redacted]/feature_flags HTTP/2

2Host: api.ergatta.com

3X-Rudder-Version: 33

4X-Seaborn-Flavor: standard

5Authorization: Bearer

[redacted]

6User-Agent: Seaborn/2024.08.01/1001

7Accept-Encoding: gzip, deflate, br

8

9

Edited response

PrettyRawHexRenderCopy Response

1HTTP/2 200 OK

2Date: Mon, 23 Sep 2024 17:57:38 GMT

3Content-Type: application/json; charset=utf-8

4Content-Length: 235

5Vary: Accept-Encoding

6

7{

8 "message": "success",

9 "data": {

10 "accountID": [redacted],

11 "canaryUpdateChannel": true,

12 "liveRaceUI": true,

13 "gameInfinity": true,

14 "classes": true,

15 "updateChannels": [

16 {

17 "name": "Main",

18 "baseUrl":

19 "https://appupdates.ergatta.com/Seaborn/\$/

20 }

21]

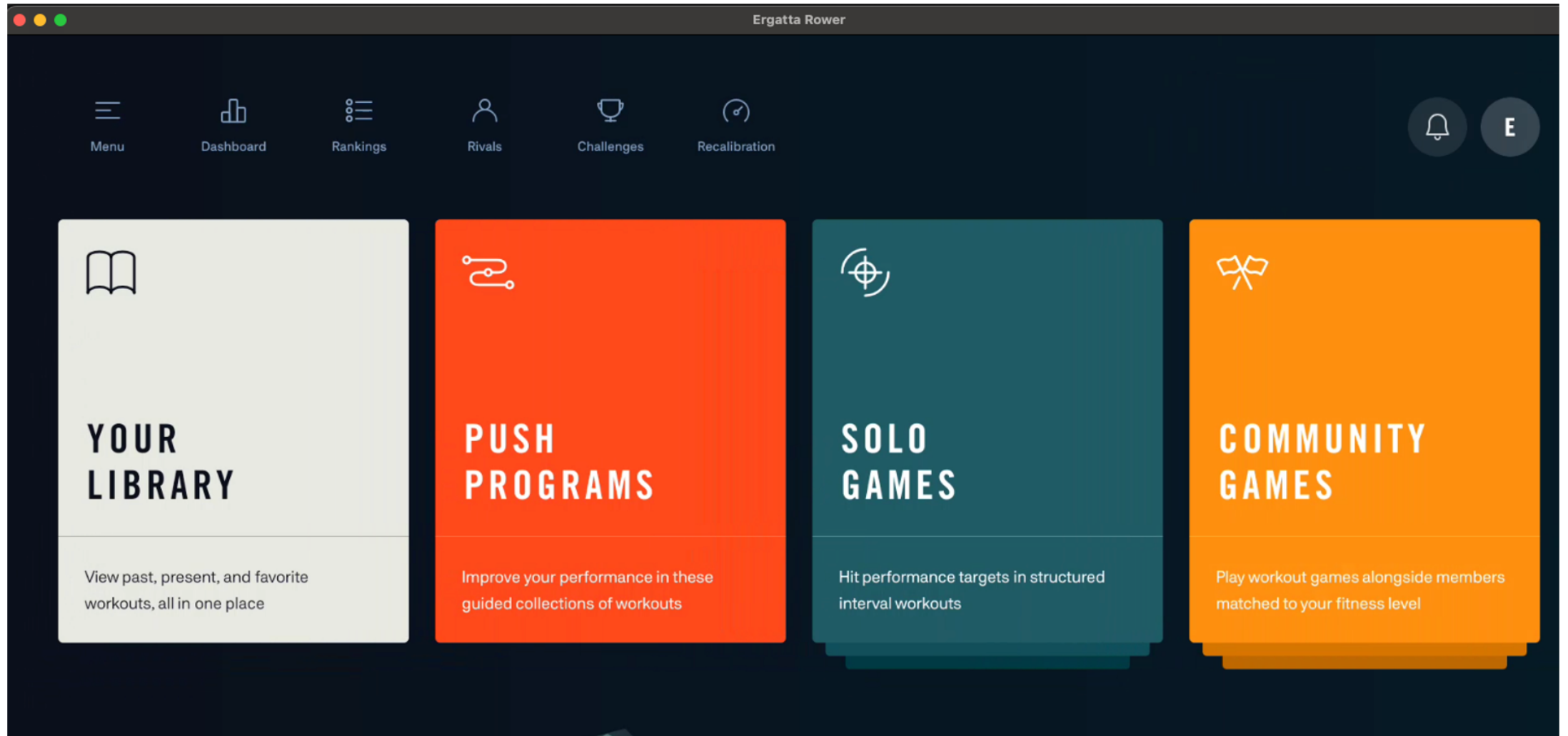
22 }

23}

18



UI after Editing Requests





Phase 2: Automation

- The rower will go through this flow several times while navigating the UI.
- Is there a good way to automate this?



Mitmproxy

- Intercepting proxy
- Light weight
- Open source
- Runs well from the Command Line

```
Flows
>>04:43:28 HTTPS POST ...pa.googleapis.com /v1/firelog/legacy/batchlog 200 ..plication/json 140b 2.02s
04:43:30 HTTP HEAD www.rockchip.com /OtaUpdater/android?product=ErgattaRower&version=1.0.0&sn=202103100BA6&c... 404 text/html 13b 17ms
04:43:31 HTTPS GET api.ergatta.com /health 200 ..plication/json 73b 116ms
04:43:31 HTTPS GET api.ergatta.com /accounts/14822 200 ..plication/json 194b 21ms
04:43:32 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ..plication/json 1.3k 128ms
04:43:32 HTTPS POST ...ig.googleapis.com /v1/projects/86365864961/namespaces/fireperf:fetch 200 ..plication/json 70b 125ms
04:43:34 HTTPS GET ...dates.ergatta.com /Seaborn/com.ergatta.seaborn/main/latest?Expires=1727153611&Signature=C0... 200 ..plication/json 345b 259ms
04:43:35 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ..plication/json 1.3k 111ms
04:43:35 HTTPS POST ...iad-05.braze.com /api/v3/data 201 ..plication/json 41b 201ms
04:43:35 HTTPS GET ...dates.ergatta.com /Seaborn/com.ergatta.seaborn/main/app.apk?Expires=1727153614&Signature=P... 200 ..ntent missing]
04:44:08 HTTPS POST ...iad-05.braze.com /api/v3/data 201 ..plication/json 49b 210ms
04:44:08 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ..plication/json 1.3k 123ms
04:44:08 HTTPS GET ...dates.ergatta.com /Seaborn/com.ergatta.seaborn/main/latest?Expires=1727153648&Signature=As... 200 ..plication/json 345b 41ms
04:44:08 HTTPS POST ...me.googleapis.com /v1/projects/86365864961/namespaces/firebase:streamFetchInvalidations
04:44:09 HTTPS GET images.ergatta.com /images/profiles/meta 200 ..plication/json 144b 447ms
04:44:09 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ..plication/json 1.3k 110ms
04:44:09 HTTPS GET ...dates.ergatta.com /Seaborn/com.ergatta.seaborn/main/app.apk?Expires=1727153648&Signature=X... 200 ..ntent missing]
04:44:11 HTTPS GET images.ergatta.com /customers/profile/0/image 403 application/xml 243b 670ms
04:44:19 HTTPS GET api.ergatta.com /accounts/14822 200 ..plication/json 194b 24ms
04:44:20 HTTPS GET images.ergatta.com /customers/profile/32445/image 403 application/xml 243b 364ms
04:44:51 HTTPS POST ...pa.googleapis.com /v1/firelog/legacy/batchlog 200 ..plication/json 140b 2.15s

8 [1/21] [scripts:1] [*:8080]
```



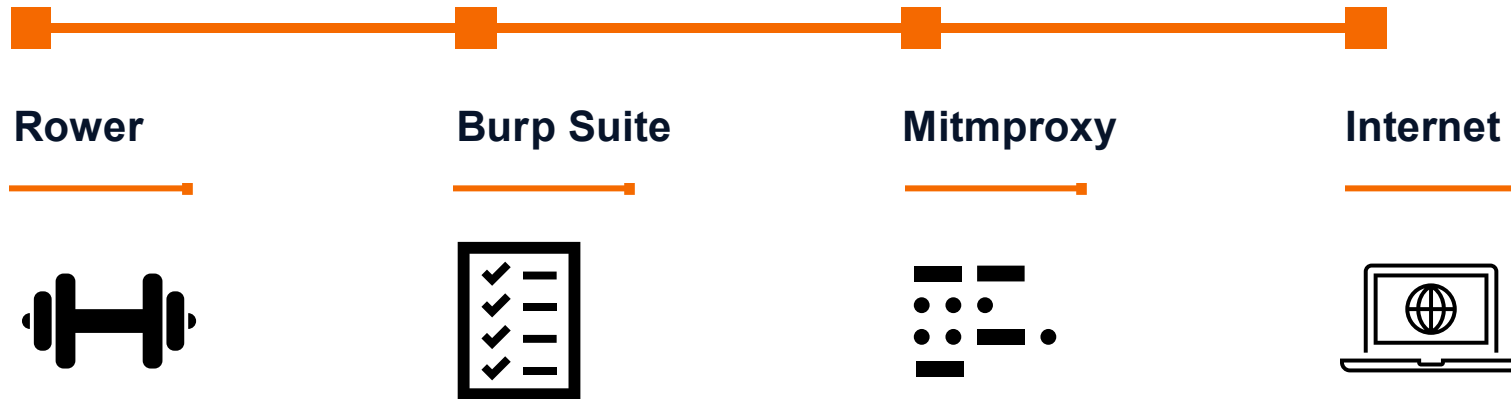
Mitproxy AddOn Structure

```
1  # mitmproxy -s ./path/to/addon.py
2
3  from mitmproxy import http
4
5  class ChangeSomeTraffic:
6
7      def __init__(self):
8          pass
9
10     # mitmproxy response event
11     def response(self, flow: http.HTTPFlow) -> None:
12         if 'target.host' in flow.request.host: #if our target host is in the host for a request
13             modified_response = open("some/file", "r").read() #open file
14             flow.response.text = modified_response #replace body in response with body from file
15             print("Request modified!")
16
17     # mitmproxy request event
18     def request(self, flow: http.HTTPFlow) -> None:
19         match str(flow.request.host):
20             case 'target.host': #if the host is the target host
21                 modified_response = open("some/file", "r").read() #open file
22                 flow.response.text = modified_response #replace body in response with body from file
23                 print("Request modified!")
24
25     addons = [
26         ChangeSubStatus()
27     ]
28
```



Proxy Testing

Traffic chain: Rower -> Burp -> Mitmproxy -> Internet





Burp Upstream Proxy Settings

Settings -> Network -> Connections -> Upstream proxy servers

? Upstream proxy servers

⚙ Use these settings to control whether Burp sends outgoing requests to an upstream proxy server, or directly to the destination web server. The first destination host is used. To send all traffic to a single proxy server, create a rule with * as the destination host.

☐ Override options for this project only

Add	Enabled	Destination host	Proxy host	Proxy port	Auth type	Username
Edit	☒	*	192.168.1.29	8080		
Remove						
Up						
Down						



First Mitmproxy AddOn Script

```
#mitmproxy response event
def response(self, flow: http.HTTPFlow) -> None:
    if 'api.ergatta.com' in flow.request.host:
        regex = re.compile('/accounts/14822$')
        regex2 = re.compile('/accounts/14822/feature_flags')
        found = regex.search(flow.request.path)
        found2 = regex2.search(flow.request.path)

        if found:
            modified_response = open("_accounts_14822.json", "r").read()
            flow.response.text = modified_response
            print("----->Changed Billing Value<-----")
        elif found2:
            modified_response = open("_accounts_14822_feature_flags.json", "r").read()
            flow.response.text = modified_response
            print("----->Changed Flag Value<-----")
```



Body Files for AddOn

Account

```
{"message": "ok", "data": {"billing_state": "Active", "cbSubscriptionId": "16CVqQSijd1y2EAVX", "rootUserId": 32445, "countryCode": "US", "partner": null, "id": 14822, "created_at": "2021-09-11T20:06:55.618Z"}}
```

Feature Flags

```
{"message": "success", "data": {"accountID": 14822, "canaryUpdateChannel": true, "liveRaceUI": true, "gameInfinity": true, "classes": true, "updateChannels": [{"name": "Main", "baseUrl": "https://appupdates.ergatta.com/Seaborn/$APPLICATION_ID/main"}]}}
```



Test Run – It works!

```
ubuntu@ubuntu: ~/ergatta_proxy (ssh)  %1  assess@US-JPV2
----->Changed Billing Value<-----
04:35:06 HTTPS GET api.ergatta.com /health 200 ...
04:35:06 HTTPS POST ...d-05.braze.com /api/v3/data 201 ...
04:35:07 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ...
04:35:07 HTTPS POST ...d-05.braze.com /api/v3/data 201 ...
04:35:08 HTTPS GET ...es.ergatta.com /images/profiles/meta 200 ...
04:35:08 HTTPS PUT api.ergatta.com /device_info 201 ...
04:35:08 HTTPS GET ...es.ergatta.com /Seaborn/com.ergatta.seaborn/main/... 200 ...
04:35:08 HTTPS GET ...es.ergatta.com /customers/profile/[redacted]/image 403 ...
04:35:08 HTTPS GET api.ergatta.com /update_cdn/metadata 200 ...
04:35:08 HTTPS GET ...es.ergatta.com /Seaborn/com.ergatta.seaborn/mai
04:35:10 HTTP HEAD ...w.rockchip.com /OtaUpdater/android?product=Ergatt...
>>04:35:18 HTTPS GET api.ergatta.com /accounts/[redacted]
04:35:19 HTTPS GET ...es.ergatta.com /customers/profile/[redacted]/image 403 a
04:35:19 HTTP HEAD 192.168.1.143 /OtaUpdater/android?product=Ergatt... err
04:35:24 HTTPS POST ...googleapis.com /v1/firelog/legacy/batchlog 200 ...

[12/15] [scripts:1]
```

```
Flow Details
2024-10-02 04:35:18 GET https://api.ergatta.com/account
+ 200 application/json 194b 11

Request Res
date: Wed, 02 Oct 2024 04:35:19 GMT
content-type: application/json; charset=utf-8
content-length: 194
vary: Accept-Encoding
JSON
{
  "data": {
    "billing_state": "Active",
    "cbSubscriptionId": "[redacted]",
    "countryCode": "US",
    "created_at": "[redacted]",
    "id": [redacted],
    "partner": null,
    "rootUserId": [redacted]
  },
  "message": "ok"
}

[12/15] [scripts:1]
```



In Burp... No “Edited” Marker

Request

Pretty Raw Hex

```
1 GET /accounts/[REDACTED] HTTP/2
2 Host: api.ergatta.com
3 X-Rudder-Version: 33
4 X-Seaborn-Flavor: standard
5 Authorization: Bearer
[REDACTED]
6 User-Agent: Seaborn/2024.08.01/1001
7 Accept-Encoding: gzip, deflate, br
8
9
```

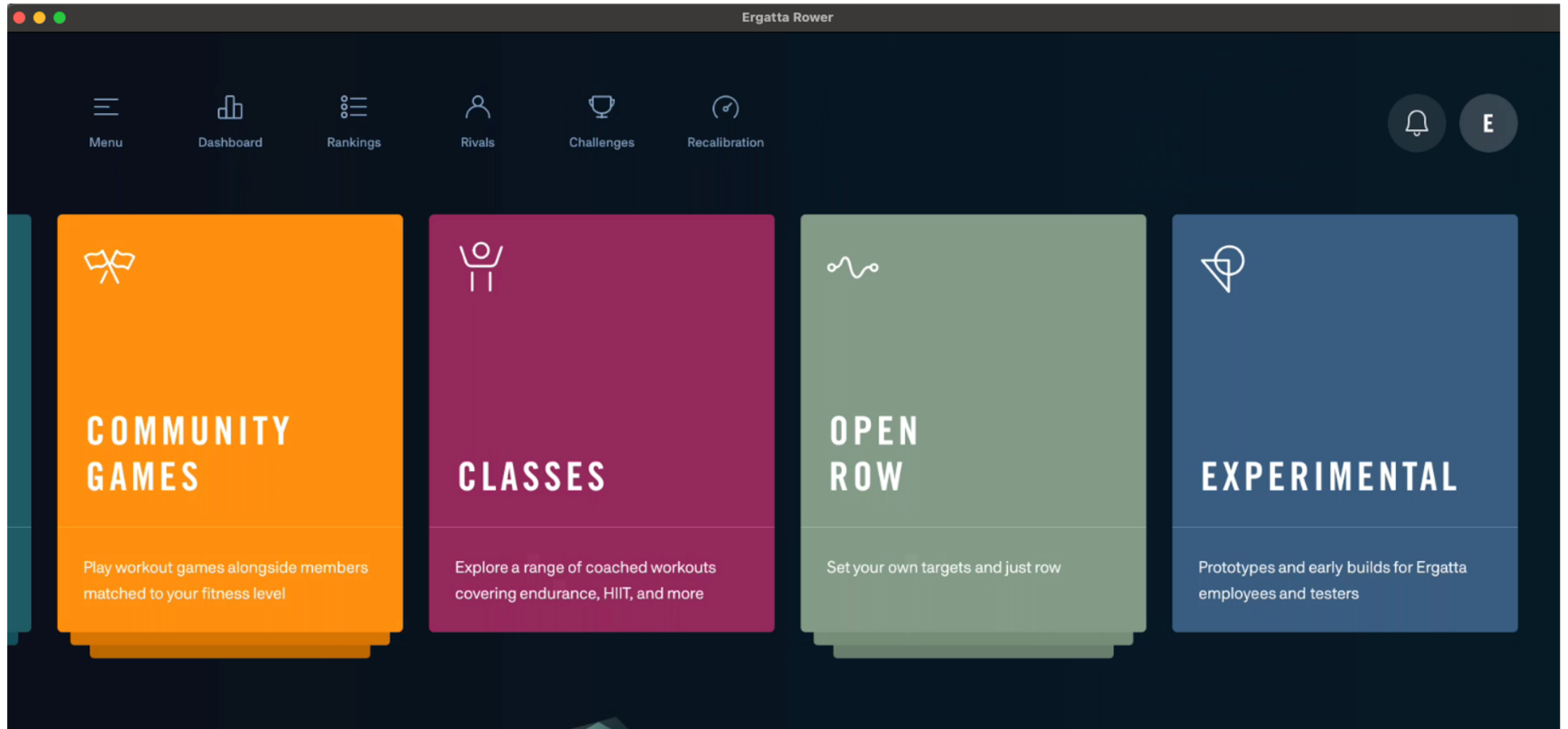
Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Wed, 02 Oct 2024 04:35:19 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 194
5 Vary: Accept-Encoding
6
7 {
  "message": "ok",
  "data": {
    "billing_state": "Active",
    "cbSubscriptionId": "[REDACTED]",
    "rootUserId": [REDACTED],
    "countryCode": "US",
    "partner": null,
    "id": [REDACTED],
    "created_at": "[REDACTED]"
  }
}
8
```



Confirming In-App – Extra Functions





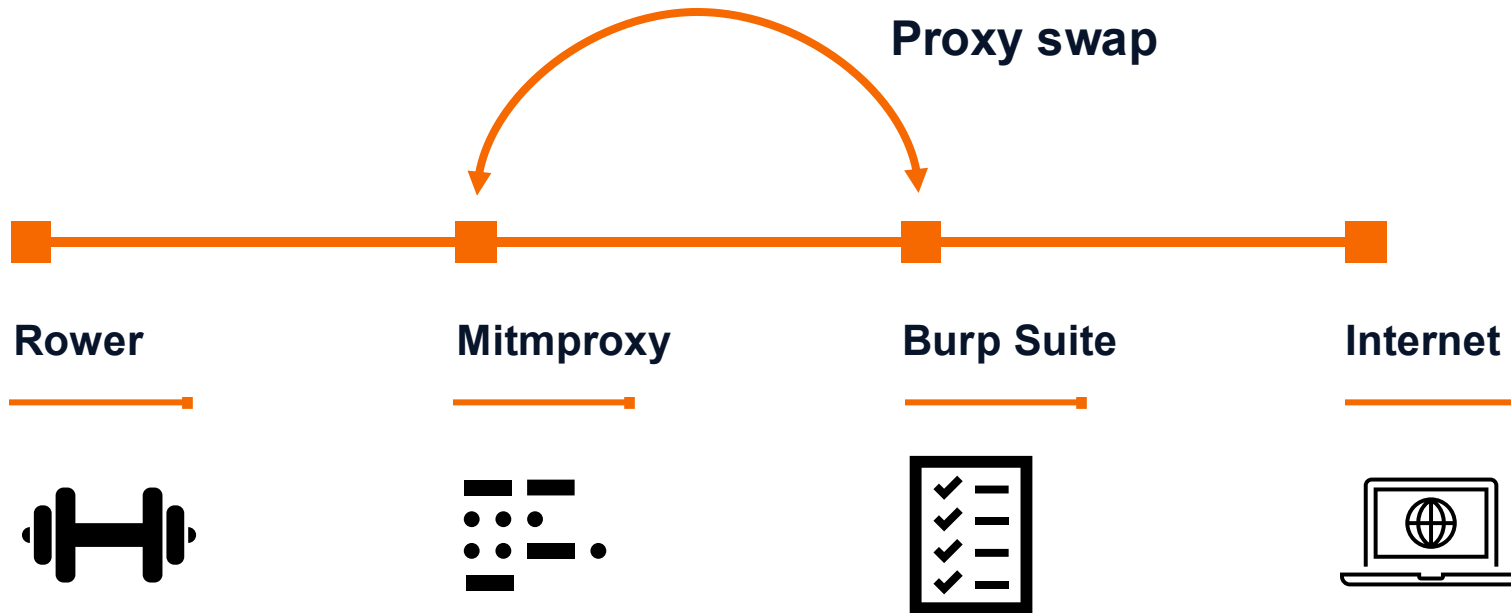
Phase 3:

Handle All Responses

- Mitmproxy has an example that states it does not send any data to the server
- Confirm this function works as documented
- Mitmproxy service running on Raspberry Pi
- Flesh out the addon to handle all the requests coming from the rowing machine



Proxy Testing





Update to AddOn

We are now acting on the request, not waiting for a response.

```
def request(self, flow: http.HTTPFlow) -> None:
    match str(flow.request.host):
        case 'api.ergatta.com': # if the host is a target host.
            path = str(flow.request.path)
            path = path.replace("/", "_") #change / to _ to filter characters we can't use to name files (sanitize input)
            filename = find_file_regex.find(path) #search if we have a .json file that matches the path

            if filename: #if we have a match, fabricate a response using the .json body from the file
                response_body = open(filename, "r").read()
                flow.response = http.Response.make(
                    200, # (optional) status code
                    response_body, # (optional) content
                    {"Content-Type": "application/json; charset=utf-8"}, # (optional) headers
                )
                print("----->"+filename+" supplied<-----")
```



Comparing Proxies

Note that these requests should have been here, but they are not.

```
Flows
19:51:10 HTTPS GET api.ipdata.co /time_zone?api-key=fed501755e3a71a6d998e9c
19:51:15 HTTPS GET api.ergatta.com /users/[redacted]
19:51:15 HTTPS GET images.ergatta.com /images/profiles/meta
>>19:51:15 HTTPS GET images.ergatta.com /customers/profile/[redacted]/image
19:51:15 HTTPS GET api.ergatta.com /accounts/[redacted]
19:51:15 HTTPS GET api.ergatta.com /accounts/[redacted]feature_flags
19:51:15 HTTPS GET api.ergatta.com /calibrated
19:51:15 HTTPS GET images.ergatta.com /customers/profile/[redacted]/image
19:51:15 HTTPS GET api.ergatta.com /deleted_workouts?filter=deleted_at%3E202
19:51:15 HTTPS GET api.ergatta.com /favorite_workouts?filter=updated_at%3E20
19:51:15 HTTPS GET images.ergatta.com /customers/profile/[redacted]/image
```

Time	Host	Method	URL
12:51:15 3 Oct 2024	https://api.ergatta.com	GET	/users/[redacted]
12:51:15 3 Oct 2024	https://images.ergatta.com	GET	/images/profiles/meta
12:51:15 3 Oct 2024	https://images.ergatta.com	GET	/customers/profile/[redacted]image
12:51:15 3 Oct 2024	https://api.ergatta.com	GET	/calibrated
12:51:15 3 Oct 2024	https://images.ergatta.com	GET	/customers/profile/[redacted]image
12:51:15 3 Oct 2024	https://api.ergatta.com	GET	/deleted_workouts?filter=deleted_at%3E20
12:51:15 3 Oct 2024	https://api.ergatta.com	GET	/favorite_workouts?filter=updated_at%3E20
12:51:15 3 Oct 2024	https://images.ergatta.com	GET	/customers/profile/[redacted]image

Command used to start mitmproxy:

```
mitmproxy -s ./AddOn.py --mode upstream:http://<ip-address>:<port> --ssl-insecure
```



Pitfall

Don't point your proxies at each other or this will happen to you

Event log

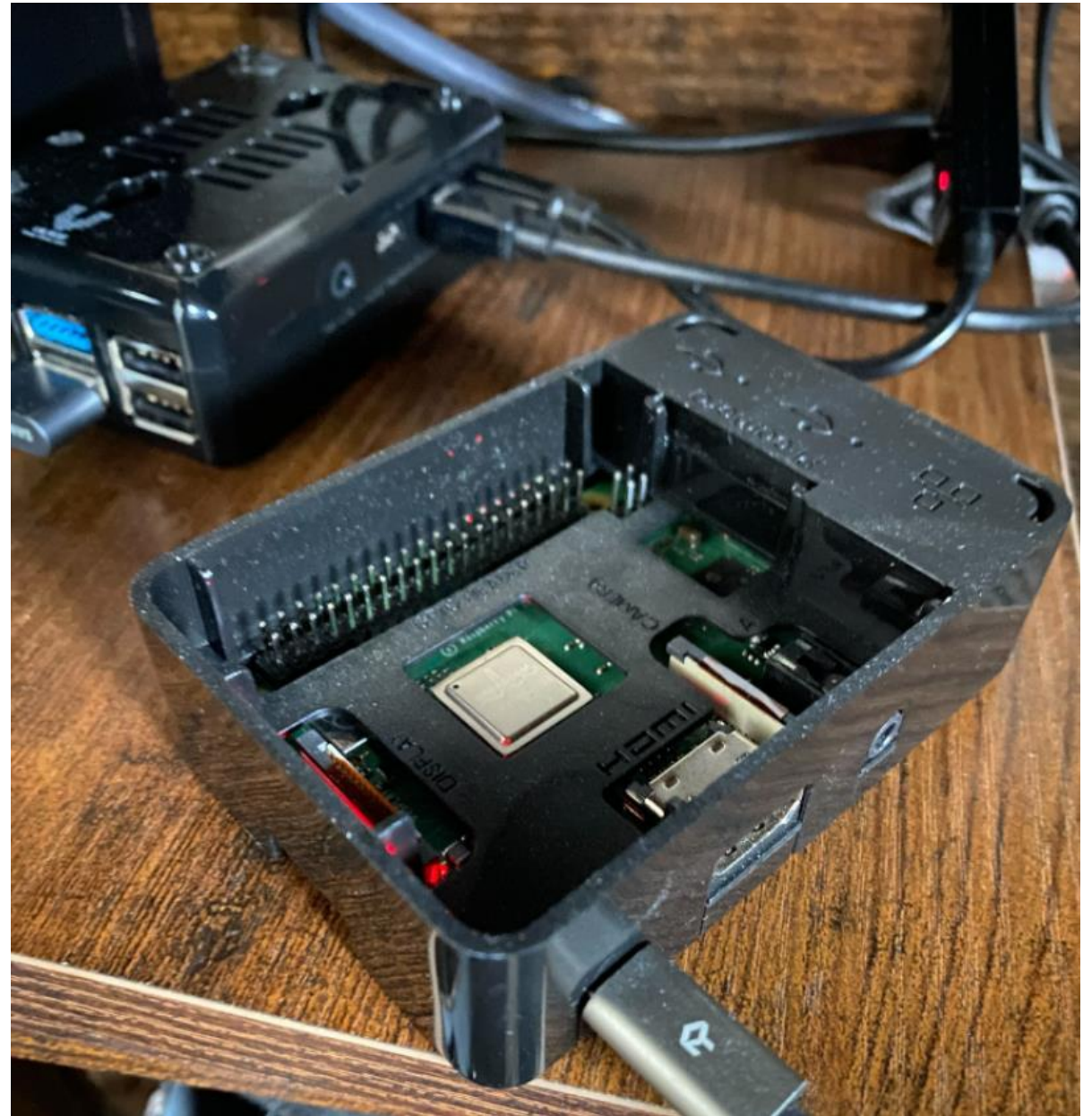
Filter **Critical** **Error** **Info** **Debug**

Time ▾	Type	Source	Message
21:14:37 1 Oct 2024	Error	Proxy	[10] Timeout waiting for stream allocation
21:14:37 1 Oct 2024	Error	Proxy	[6] Communication error: api.ergatta.com
21:14:15 1 Oct 2024	Error	Proxy	[2] Communication error: sdk.iad-05.braze.com
21:14:13 1 Oct 2024	Error	Proxy	Communication error: firebaselogging-pa.googleapis.com
21:14:10 1 Oct 2024	Info	Proxy	Throttling HTTP/2 requests to firebaselogging-pa.googleapis.com due to server concurrent stream limit.
21:13:42 1 Oct 2024	Error	Proxy	Communication error: images.ergatta.com
21:13:41 1 Oct 2024	Info	Proxy	Throttling HTTP/2 requests to sdk.iad-05.braze.com due to server concurrent stream limit.
21:13:40 1 Oct 2024	Info	Proxy	Throttling HTTP/2 requests to images.ergatta.com due to server concurrent stream limit.
21:13:37 1 Oct 2024	Error	Scanner	Failed to connect to the configured Collaborator server: polling.oastify.com.
21:13:34 1 Oct 2024	Info	Proxy	Throttling HTTP/2 requests to api.ergatta.com due to server concurrent stream limit.



Raspberry Pi 4 Model B

- Ubuntu Server Headless
- WiFi Connected





Mitmdump

- Even more CLI than Mitmproxy

```
ubuntu@ubuntu:~/ergatta_proxy$ mitmdump -s ./ergatta-proxy.py
Loading script ./ergatta-proxy.py
Proxy server listening at *:8080
192.168.1.16:53820: client connect
192.168.1.16:53822: client connect
192.168.1.16:53822: server connect firebase.googleapis.com:443 (74.125.1
192.168.1.16:53824: client connect
192.168.1.16:53820: server connect api.ergatta.com:443 (3.141.73.29:443)
192.168.1.16:53824: error establishing server connection: Multiple exceptions: [Er
111] Connect call failed ('::', 443, 0, 0)
192.168.1.16:53824: CONNECT app-measurement.com:443
<< 502 Bad Gateway 163b
192.168.1.16:53824: client disconnect
192.168.1.16:53828: client connect
192.168.1.16:53828: error establishing server connection: Multiple exceptions: [Er
111] Connect call failed ('::', 443, 0, 0)
192.168.1.16:53828: CONNECT app-measurement.com:443
<< 502 Bad Gateway 163b
192.168.1.16:53828: client disconnect
192.168.1.16:53820: GET https://api.ergatta.com/health HTTP/2.0
<< HTTP/2.0 200 OK 73b
----->_accounts_[REDACTED].json supplied<-----
192.168.1.16:53820: GET https://api.ergatta.com/accounts/[REDACTED] HTTP/2.0
<< HTTP/1.1 200 OK 194b
```



ergatta.service config

- Add <serviceservice>.service to /etc/systemd/system
- Note the WorkingDirectory parameter

```
[Unit]
Description=Ergatta mitmproxy addon service
After=network.target
[Service]
Type=simple
Restart=always
RestartSec=3
User=ubuntu
WorkingDirectory=/home/ubuntu/ergatta_proxy/
ExecStart=/home/ubuntu/ergatta_proxy/ergatta-script.sh

[Install]
WantedBy=multi-user.target
```



Ergatta-script.sh

```
#!/bin/bash
/usr/bin/mitmdump --ssl-insecure --set confdir=/home/ubuntu/.mitmproxy -s /home/ubuntu/ergatta_proxy/ergatta-proxy.py
&>> /home/ubuntu/ergatta_proxy/mitmdump.log
~
```



Start ergatta.service

- If all goes well it should be active (running) status
- Use `systemctl enable <some-service>.service` to have it start automatically on boot

```
ubuntu@ubuntu:~/ergatta_proxy$ sudo systemctl daemon-reload
ubuntu@ubuntu:~/ergatta_proxy$ sudo systemctl start ergatta.service
ubuntu@ubuntu:~/ergatta_proxy$ sudo systemctl status ergatta.service
● ergatta.service - Ergatta mitmproxy addon service
   Loaded: loaded (/etc/systemd/system/ergatta.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-10-03 21:02:48 UTC; 9s ago
     Main PID: 18340 (ergatta-script.)
       Tasks: 3 (limit: 853)
      Memory: 44.5M (peak: 44.9M)
         CPU: 4.703s
       CGroup: /system.slice/ergatta.service
              └─18340 /bin/bash /home/ubuntu/ergatta_proxy/ergatta-script.sh
                 └─18341 /usr/bin/python3 /usr/bin/mitmdump --ssl-insecure --set confdir=/home/ubuntu/

Oct 03 21:02:48 ubuntu systemd[1]: Started ergatta.service - Ergatta mitmproxy addon service.
```



Installation & Current State

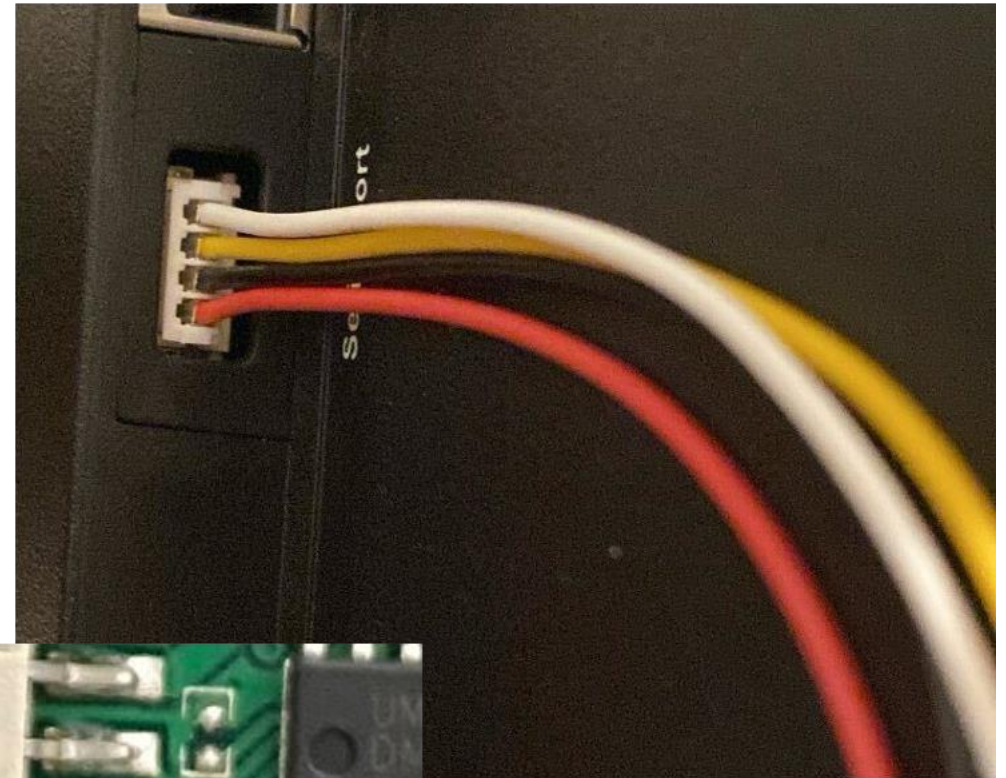
- Glued to the back of the monitor
- Powers up normally
- Powers down when rower does
- Might have some power warnings, but otherwise still seems to function





Next Steps

- 4 pin 2mm pitch PH connector w/ pigtail
- Looks like a UART port
- Common baud rates failed
- Logic analyzer to identify baud rate
- Sigrok rabbit hole





Firmware Update Domains

- Periodically reaches out to 2 domains for firmware updates
- Head requests are identical except for the Host

21:14:03 1 Oct 2024	http://www.rockchip.com:2300	HE... /OtaUpdater/android?product=ErgattaRower&version=1.0.0&sn=[REDACTED]&col
21:14:03 1 Oct 2024	http://192.168.1.143:2300	HE... /OtaUpdater/android?product=ErgattaRower&version=1.0.0&sn=[REDACTED]&col

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 HEAD http://www.rockchip.com:2300/OtaUpdater/android? product=ErgattaRower&version=1.0.0&sn=[REDACTED]& country=US&language=en HTTP/1.1 2 Host: www.rockchip.com:2300 3 Connection: keep-alive 4 User-Agent: rk29sdk/4.0 5 6</pre>		<pre>1 HTTP/1.1 200 OK 2 Connection: close 3 Cache-control: no-cache, no-store 4 Pragma: no-cache 5 X-Frame-Options: DENY 6 Content-Type: text/html; charset=utf-8 7 X-Content-Type-Options: nosniff 8 9</pre>	



Rockchip.com

- Might not be a squatter, but...
- Doesn't look like a firmware distribution website to me





Rock-chips.com

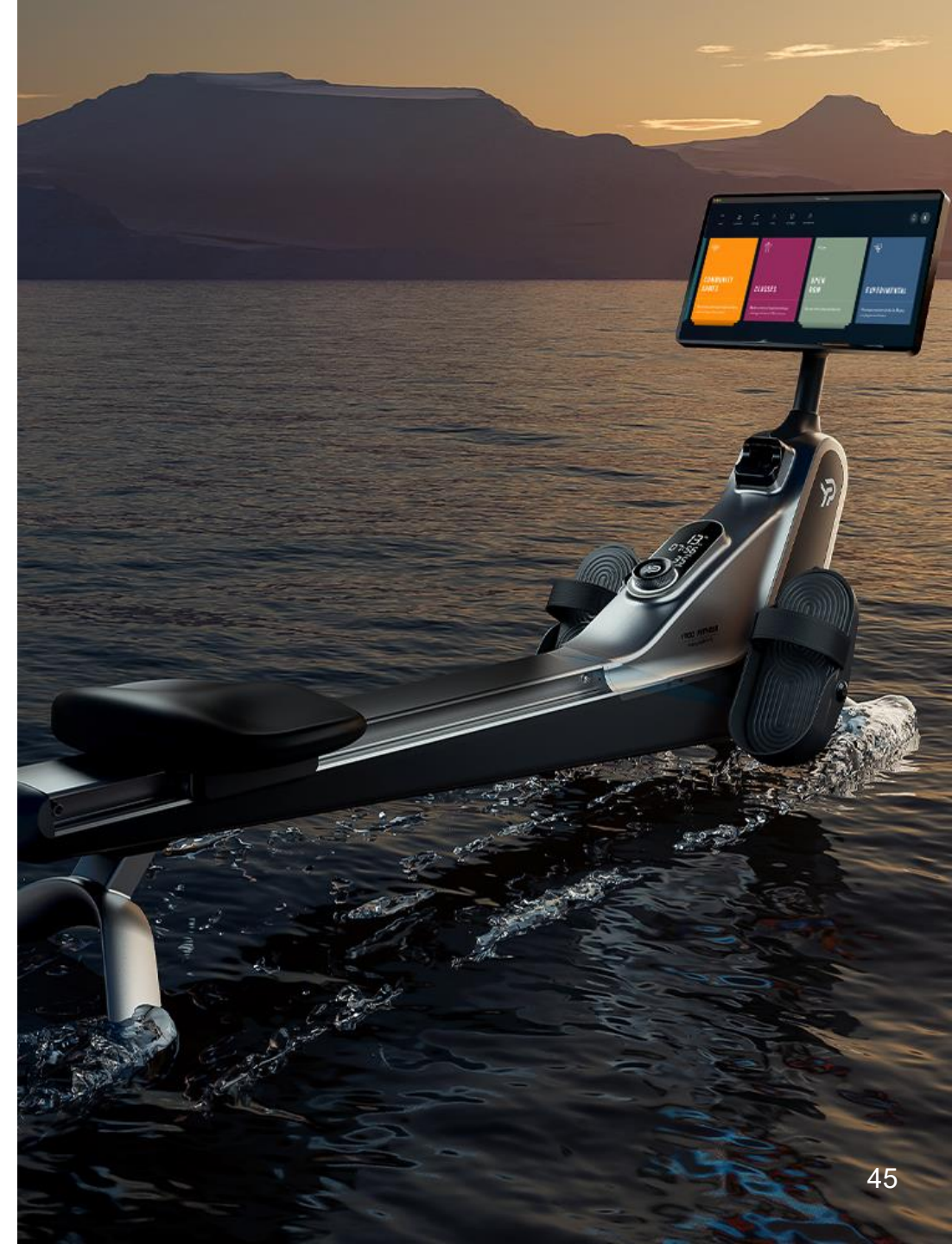
- New domain, new you
- Tried replacing the domain for the firmware update, no dice





Disclosure Schedule

- **July 19th**
 - LinkedIn contact attempts.
- **July 25th**
 - Called customer support then emailed wireshark capture for the firmware updates to them and their CTO Prasanna Swaminathan.
- **September 20th**
 - Email follow up, and first mention of authZ issues.
- **September 23rd**
 - Prasanna responded and asked for details. Shared screenshots and high-level findings.
- **September 27th**
 - Zoom meeting with Prasanna to talk through the authZ findings. 2 month patching window.





Questions?

Shane Kell

Senior Security Consultant

shane.kell@netspi.com

241 N 5th Ave Suite 1200
Minneapolis, MN 55401

netspi.com

