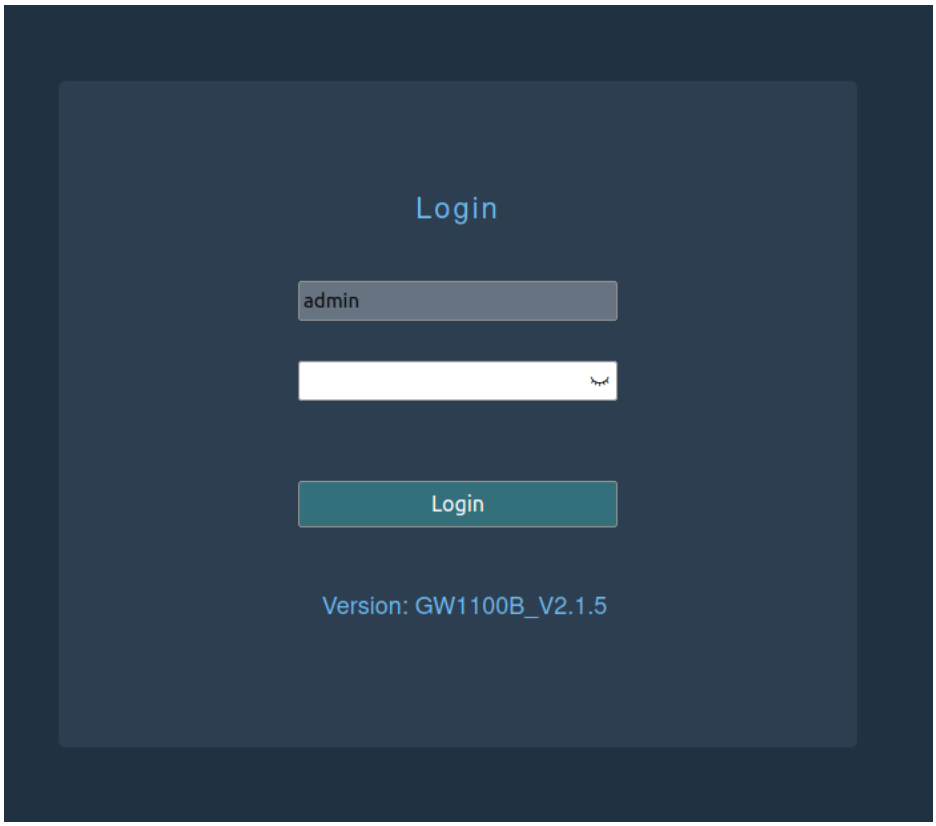
The Incredibly Insecure Weather Station

Edit: This was given CVE-2022-35122.

I recently purchased the ECOWITT GW1102 Home Weather Station. It's exactly what it sounds like – a mini weather station for your house. It has all the usual sensors you'd expect a weather station to have, and I'm actually very pleased with the hardware, considering the cheap price.

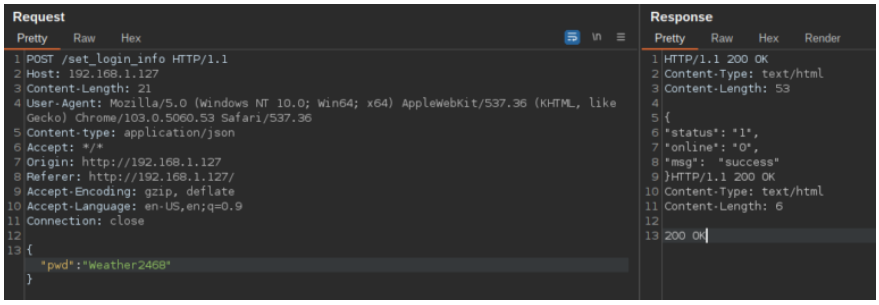
However, it is missing one thing – software security. But really, what did I expect from a cheap home weather station?

Comically, the landing page of the weather station's server gives an illusion of some sort of security.



Password goes here.

Let's intercept a request of us logging in.



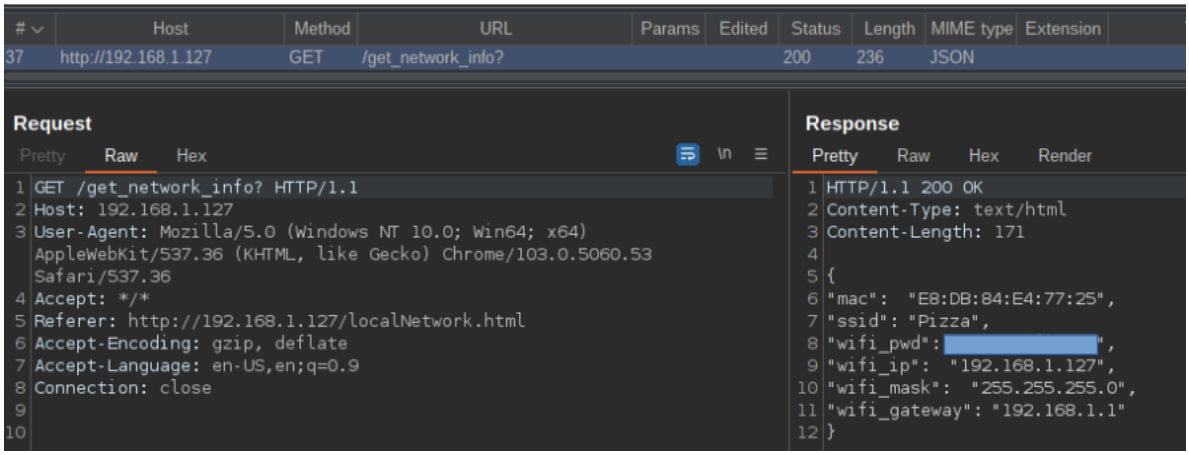
Don't steal my password.

This is all over HTTP. We post our password to `/set_login_info` – which seems like an odd endpoint for logging in. Notice the response does not set any cookies or seem like it actually does any sort of verification. Hmmm.

Anyway, after logging in, we are directed to `/liveData.html`. This page does exactly what its name implies. But let's look at the links on the side of the page – particularly the Local Network link.

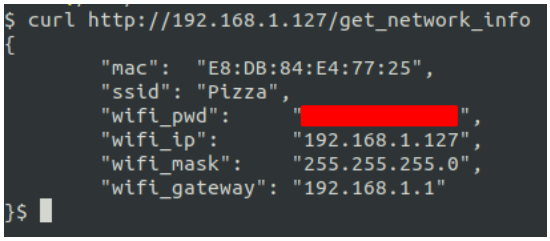
Click the Local Network link on the left-hand side.

If we intercept the requests in Burp after we click the Local Network link, we see a call to a `/get_network_info` endpoint. This returns info about the WiFi network to which the weather station is connected.



That's my WiFi SSID and password.

Interesting. Notice again that there appears to be no authentication going on with this request. Let's try to curl this endpoint



Uh oh.

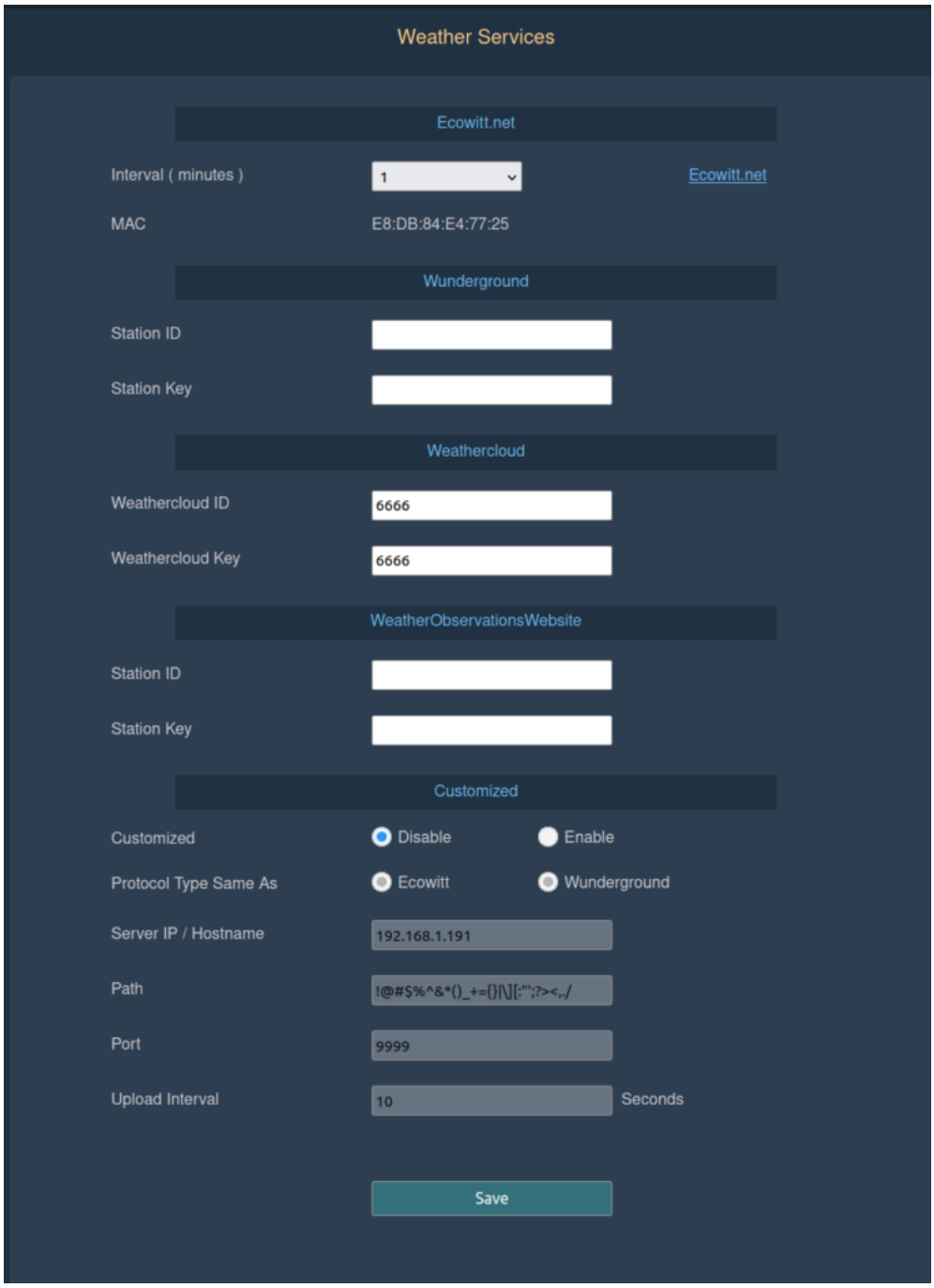
Or how about the device password (not that you actually need the password now).

The password is now Weather24689 because I changed it without being authorized.

You can also do fun things like reboot the station, or get the user's external weather reporting site's API keys, etc. I notified ECOWITT support, but I'm assuming this won't be fixed any time soon.

Edit: added this because someone didn't understand this is an issue.

Edit: I added this picture above of the get_ws_settings endpoint. As you can see, I'm not using any authentication. You can also see I was trying some shenanigans, but nonetheless, you can also see this returns several API keys for other services, which is not a good thing to be handing out. It basically is the API endpoint for this page that is behind the 'authentication' of the application.



I ***did*** find some of these exposed to the internet, but I'd probably avoid that, if I were you. With that said, I actually like the hardware. It's fun to play around with, and it is inexpensive.

This entry was posted in blog, CVE, cybersecurity, hacking, infosec and tagged cybersecurity, ecowitt, hacking, infosec, self hosting on June 30, 2022 [https://www.pizzapower.me/2022/06/30/the-incredibly-insecure-weather-station/] .