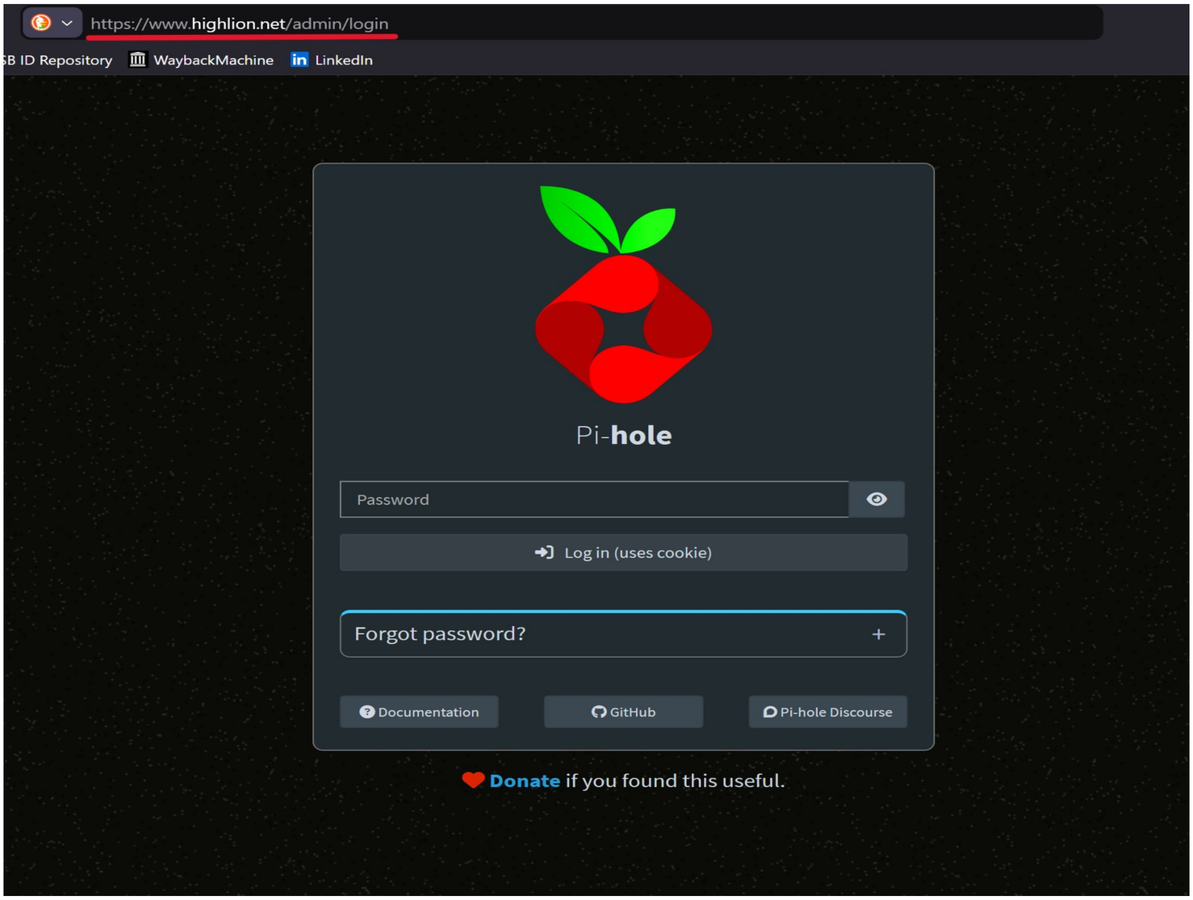
Incident Audit

Incident: Exposed Pi-Hole Admin Page
Date Written: 2.11.25
Status: Fixed

Summary:
In my home network, I discovered that the pi-hole admin login page was exposed to the internet through my domain.
I discovered this when reviewing my own attack surface, trying several admin paths and then verifying that the Pi-hole panel was reachable from outside the network.

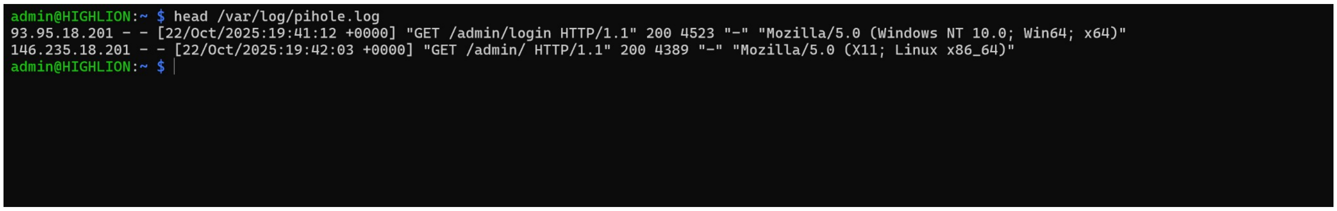
Environment:
Web server: running Apache and NGINX, with cloudflared as a reverse proxy
1-Pi-Hole instance
2-Public facing website
with public access via: https://www.highlion.net
both the website and the Pi-hole were behind the same server.

How I found it:
As part of my self testing my own network, I checked my domain from the outside.
I Browsed to the domain, and tried various admin paths including:
/admin
/admin/login
The latter directed me to the Pi-hole admin login page. I then confirmed the exposure from another external network to make sure it was not just a routing or DNS issue.



https://www.highlion.net/admin/login

Incident Audit



```
admin@HIGHLION:~ $ head /var/log/pihole.log
93.95.18.201 - - [22/Oct/2025:19:41:12 +0000] "GET /admin/login HTTP/1.1" 200 4523 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
146.235.18.201 - - [22/Oct/2025:19:42:03 +0000] "GET /admin/ HTTP/1.1" 200 4389 "-" "Mozilla/5.0 (X11; Linux x86_64)"
admin@HIGHLION:~ $
```

The cause:
The issue came from my reverse proxy configuration:
-Both the website and Pi-hole were running on the same server.
-The proxy rules for the domain did not include a proper catch all restriction.
-The proxy misconfiguration acted as a fallback for /admin/login.

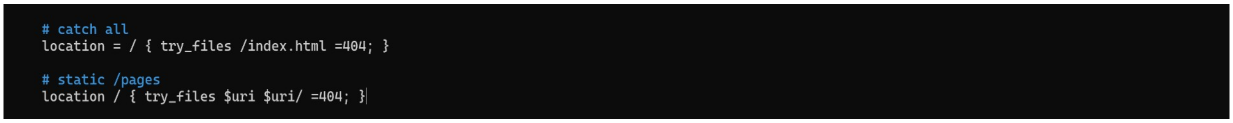
Because of this, HTTP requests to https://www.highlion.net/admin/login were routed to the Pi-hole backend, and the admin panel, which was meant to be purely internal, was exposed to the internet.

Fixes and Lessons:
In order to fix the found vulnerability and harden the network, I took these steps:

1-Fixed the configuration, by creating a catch-all for any non public facing pages.

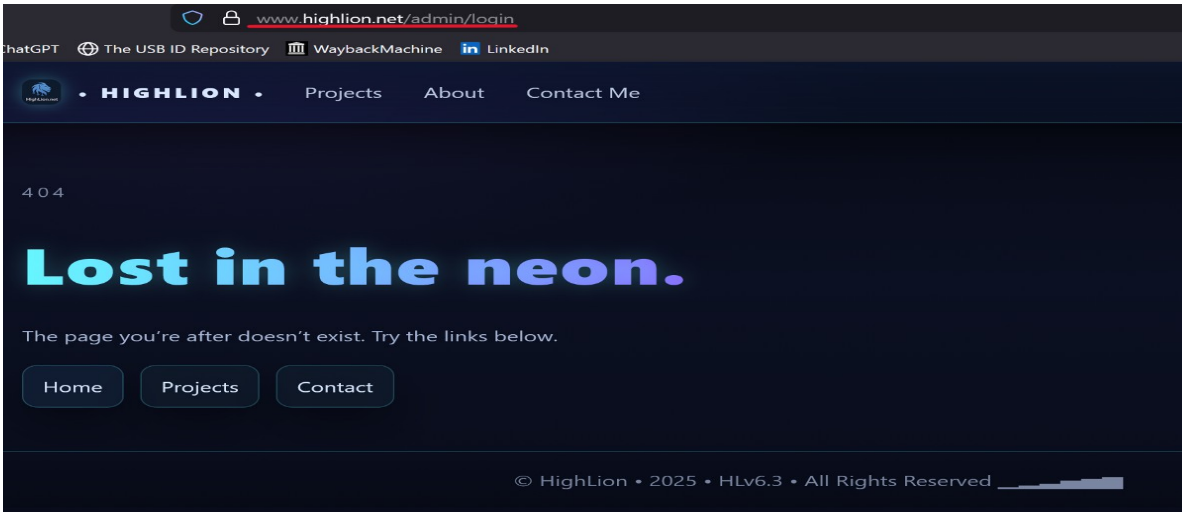
2-Moved the Pi-hole service to a different host, instead of sharing the server with the public website.

3-Limited Pi-hole admin access to specific admin IPs and verified that /admin and /admin/login no longer expose the panel and return a 404.



```
# catch all
location = / { try_files /index.html =404; }

# static /pages
location / { try_files $uri $uri/ =404; }
```



404

Lost in the neon.

The page you're after doesn't exist. Try the links below.

© HighLion • 2025 • HLv6.3 • All Rights Reserved