My Callsign Is My Passport

Responsible Testing and Disclosure
of Ham Radio Websites

Dan Norte WØBDP
Lucas Gahler NØOPS

Dan Norte | WØBDP

NETSPI®

- Senior Security Consultant
- 3 years experience in Web Application, External Network, API, and Cloud penetration testing
- Licensed for 6 years, now Amateur Extra
- Loves chasing DX and popping shells
- GLAARG Volunteer Examiner (VE)
- Drank the Yaesu kool-aid

Lucas Gahler | NØOPS

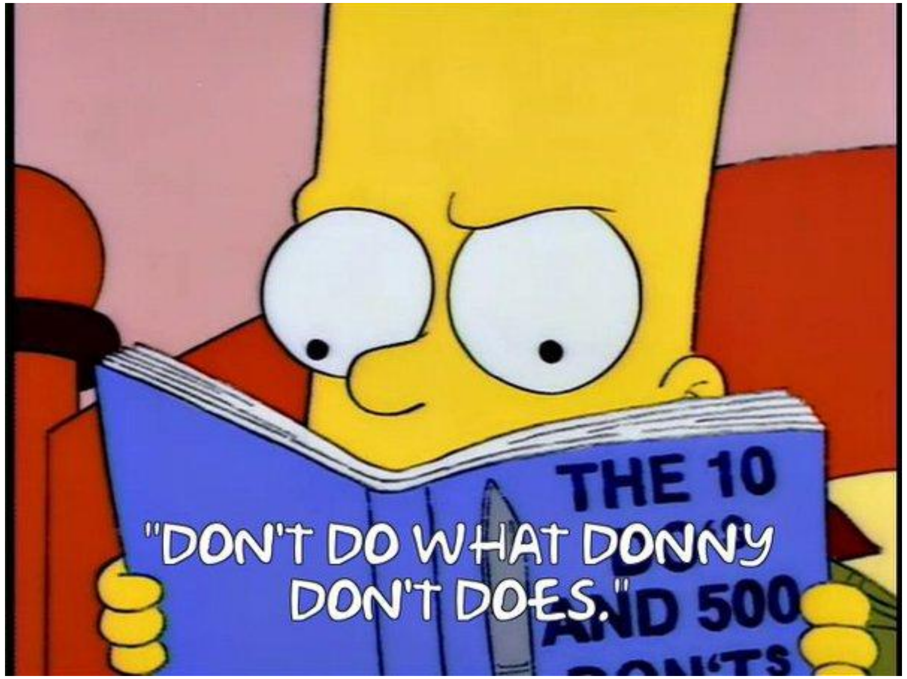
- 10 years in infosec industry
  - security operations | vuln mgmt | DFIR | pen testing
- Licensed for 14 years, now Amateur Extra
- GLAARG and ARRL Volunteer Examiner (VE)
- Primary interest areas are POTA and antenna design
- Callsign is an accurate descriptor of my on-air operations
- Handed Dan the Yaesu kool-aid

The Usual Disclaimer

- These opinions and actions are our own and not a reflection of our employers

- Don’t do what we did unless you know what you’re doing

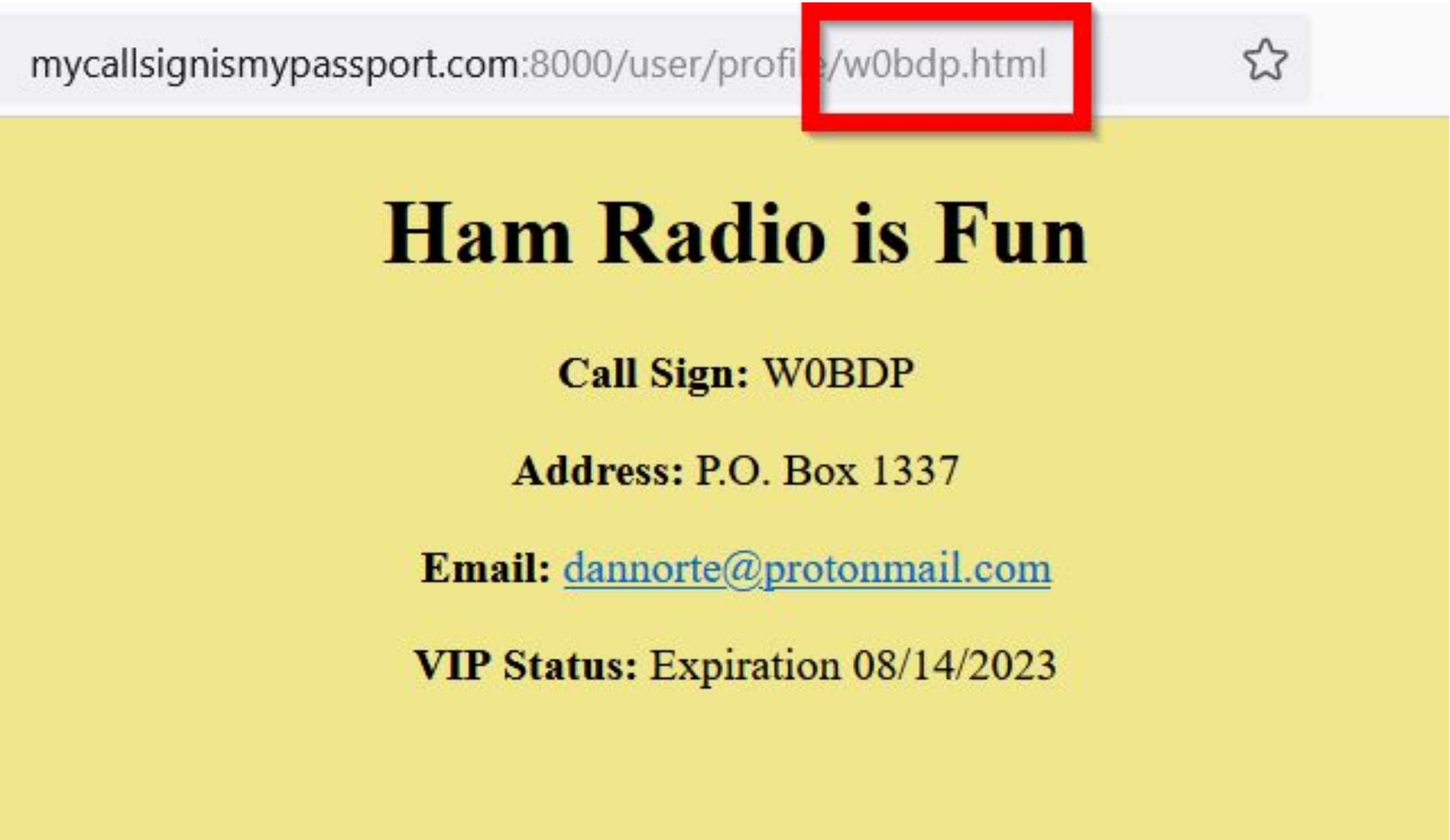
- Not our responsibility if you break something



This is how we POTA in MN

Dan’s Ham Shack – Great in the summer, not so much in the winter

Dan Accidentally Finds a Vulnerability



mycallsignismypassport.com:8000/user/profile/w0bdp.html

Ham Radio is Fun

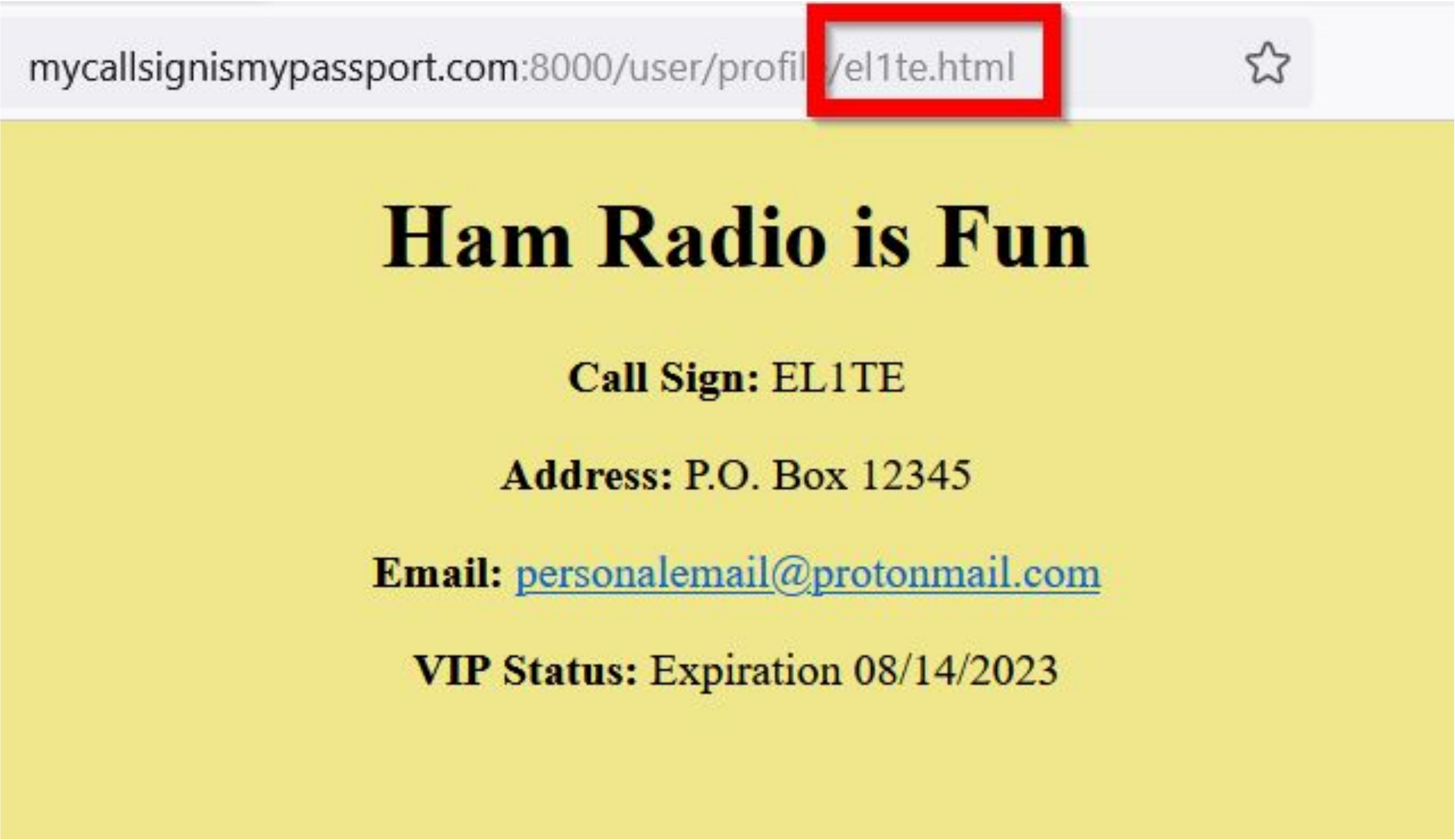
Call Sign: W0BDP

Address: P.O. Box 1337

Email: dannorte@protonmail.com

VIP Status: Expiration 08/14/2023

Insecure Direct Object Reference (IDOR)



mycallsignismypassport.com:8000/user/profile/el1te.html

Ham Radio is Fun

Call Sign: EL1TE

Address: P.O. Box 12345

Email: personalemail@protonmail.com

VIP Status: Expiration 08/14/2023

The Dilemma of Reporting

- F12 incident - MO state gov site disclosing teacher SSNs
- Four Students arrested for disclosing a vulnerability in FreeHour
  - https://timesofmalta.com/articles/view/we-wanted-help-students-arrested-exposing-freehour-security-flaw.1024757
- threats.disclose.io

It’s Dan, of course he’s going to full send

the site owner a detailed disclosure

Everything Turned Out Okay

- Owner was grateful and responsive
  - Remediated in a few days, validated the fix
- Most likely well-received due to:
  - Professional reporting
  - Verifying intended functionality
  - Being licensed

This is great

We helped make a fellow ham’s web presence more secure

We wanted to do more

- Approached site owner and offered to do an assessment
    - We are hams, here’s our callsigns
- Here’s what we are thinking for scope, how does that sound?
    - Avoiding destructive testing
    - Provide report back with findings
    - Not disclose specifics prior to remediation
    - Deconfliction
- He was 100% on board

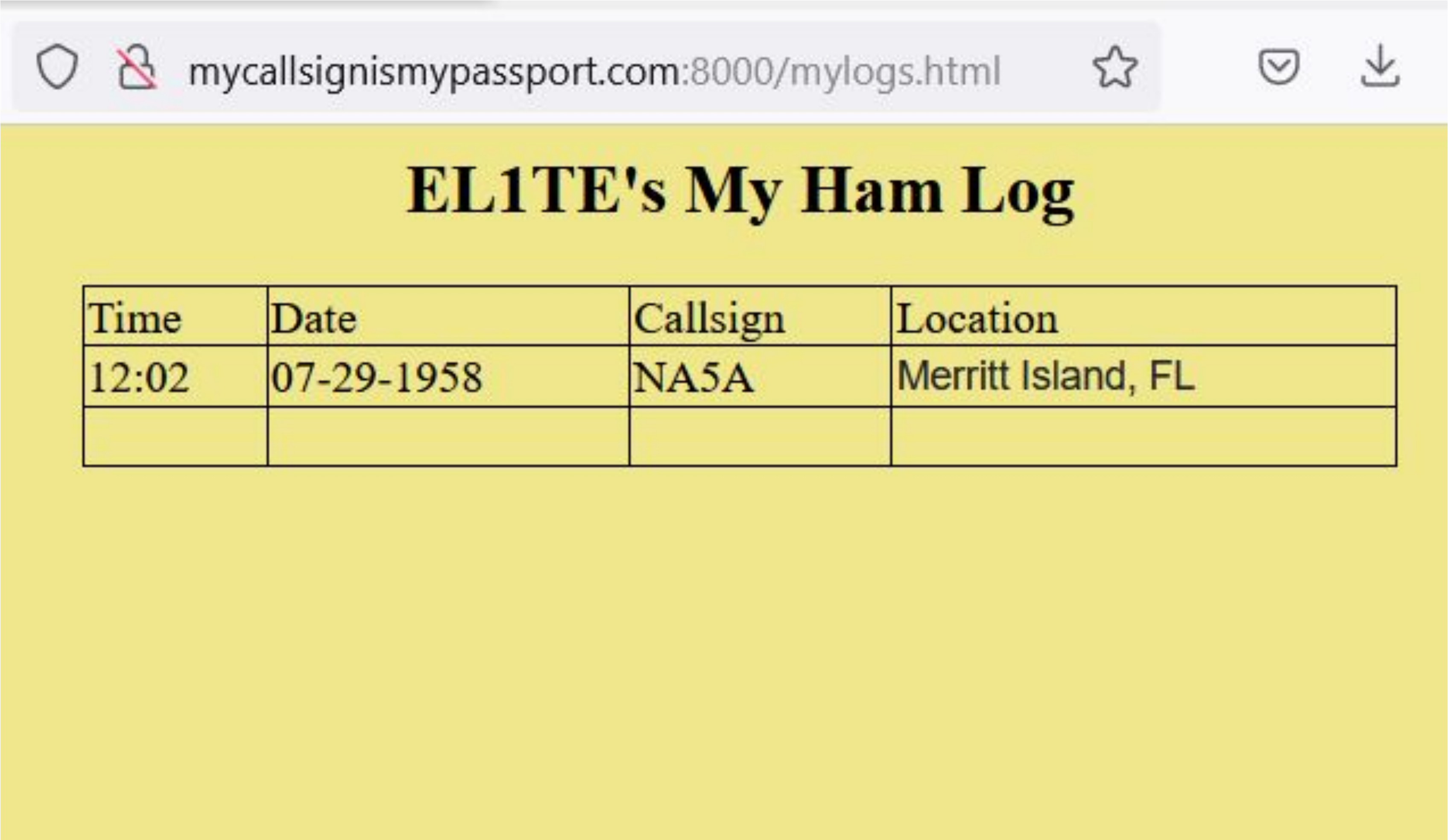
What We Found

Summary of Findings:

- 6 HIGH Vulnerabilities
- 3 MEDIUM Vulnerabilities
- 3 LOW Vulnerabilities
- 1 Informational Vulnerability

Estimated Effort: 12.5 hours!

What We Found

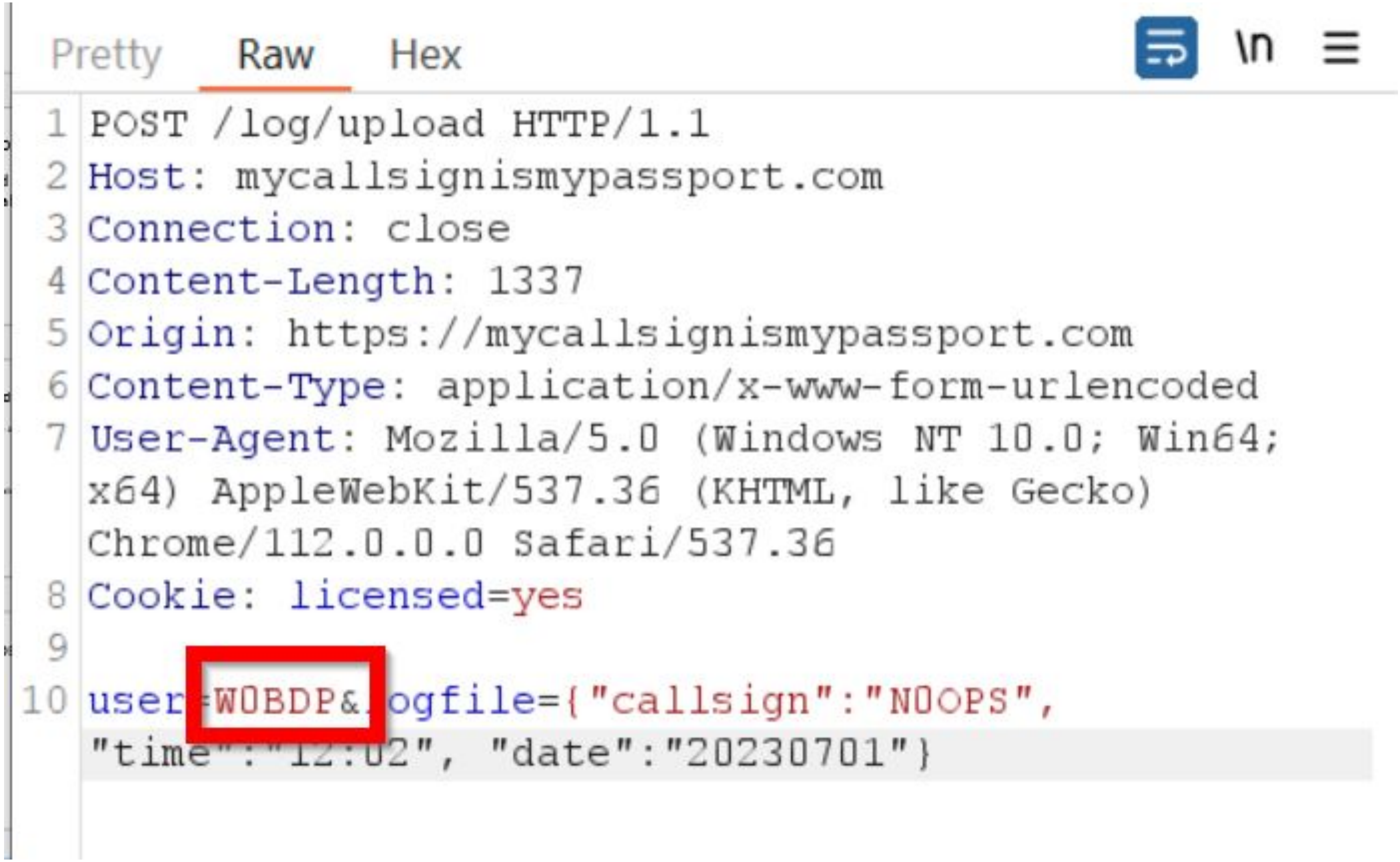


mycallsignismypassport.com:8000/mylogs.html

EL1TE's My Ham Log

Time	Date	Callsign	Location
12:02	07-29-1958	NA5A	Merritt Island, FL

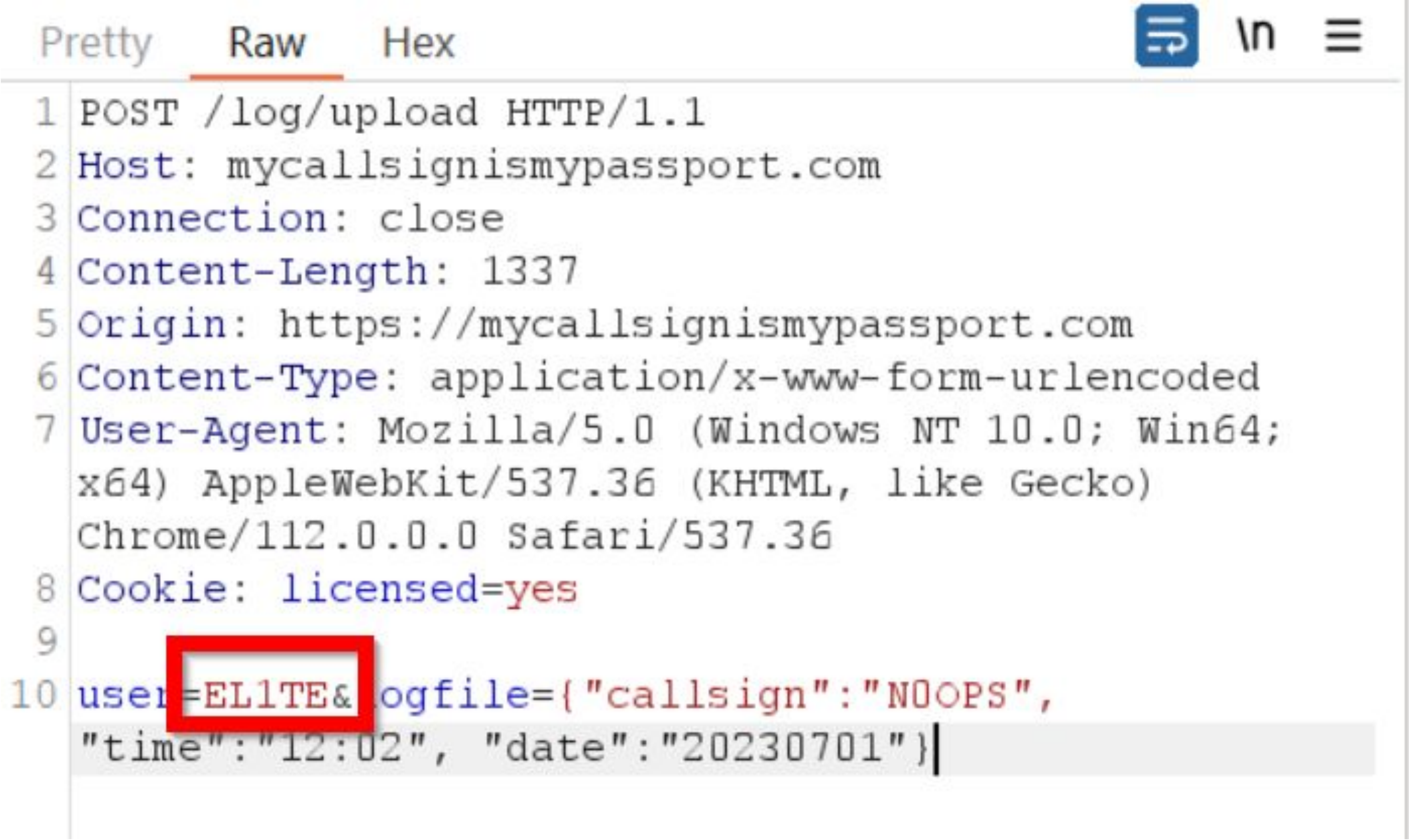
What We Found



```
POST /log/upload HTTP/1.1
Host: mycallsignismypassport.com
Connection: close
Content-Length: 1337
Origin: https://mycallsignismypassport.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Cookie: licensed=yes

user=W0BDP&logfile={"callsign":"N0OPS", "time":"12:02", "date":"20230701"}
```

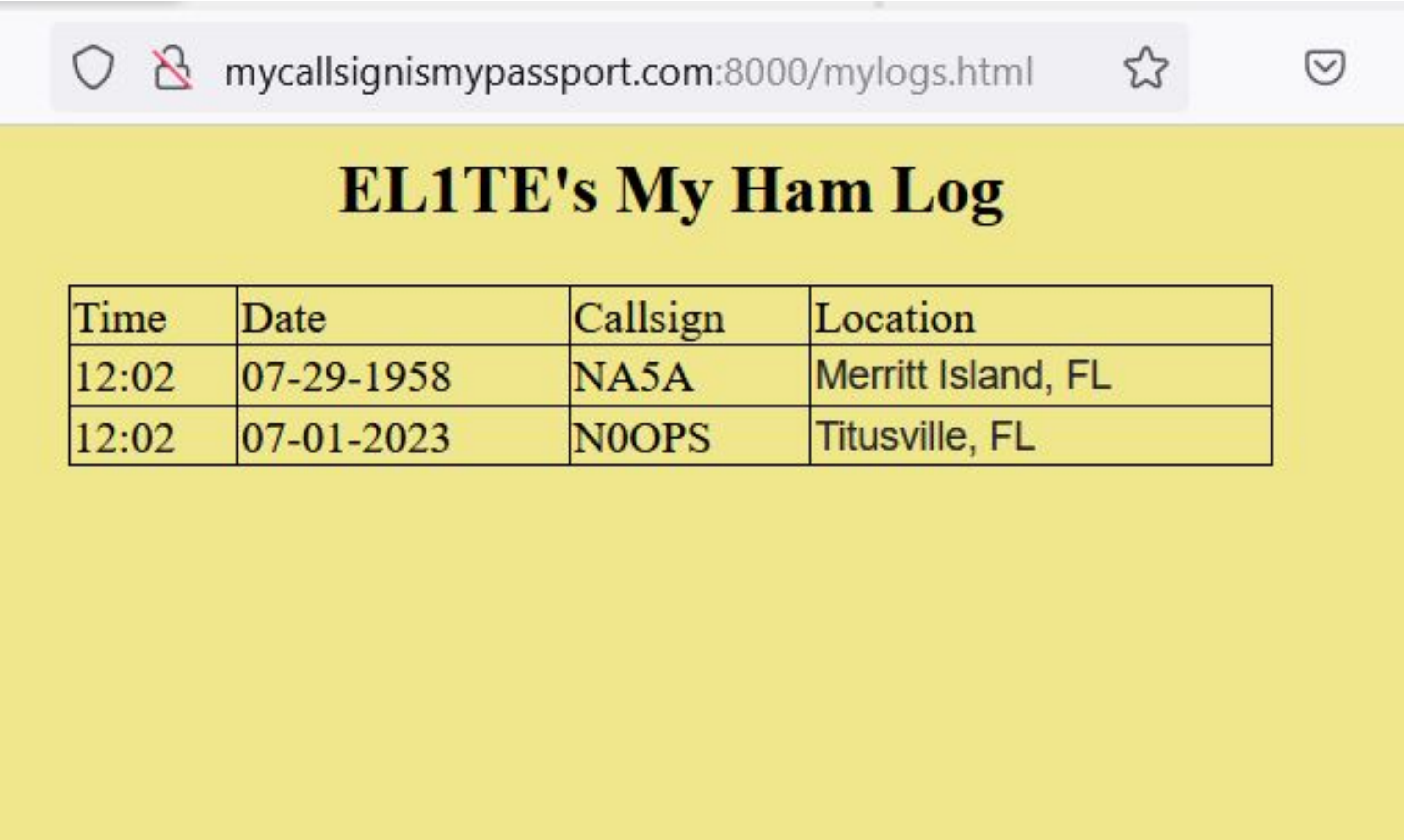
What We Found - IDOR



```
POST /log/upload HTTP/1.1
Host: mycallsignismypassport.com
Connection: close
Content-Length: 1337
Origin: https://mycallsignismypassport.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.0.0 Safari/537.36
Cookie: licensed=yes

user=EL1TE&logfile={"callsign":"N0OPS",
"time":"12:02", "date":"20230701"}
```

What We Found - IDOR

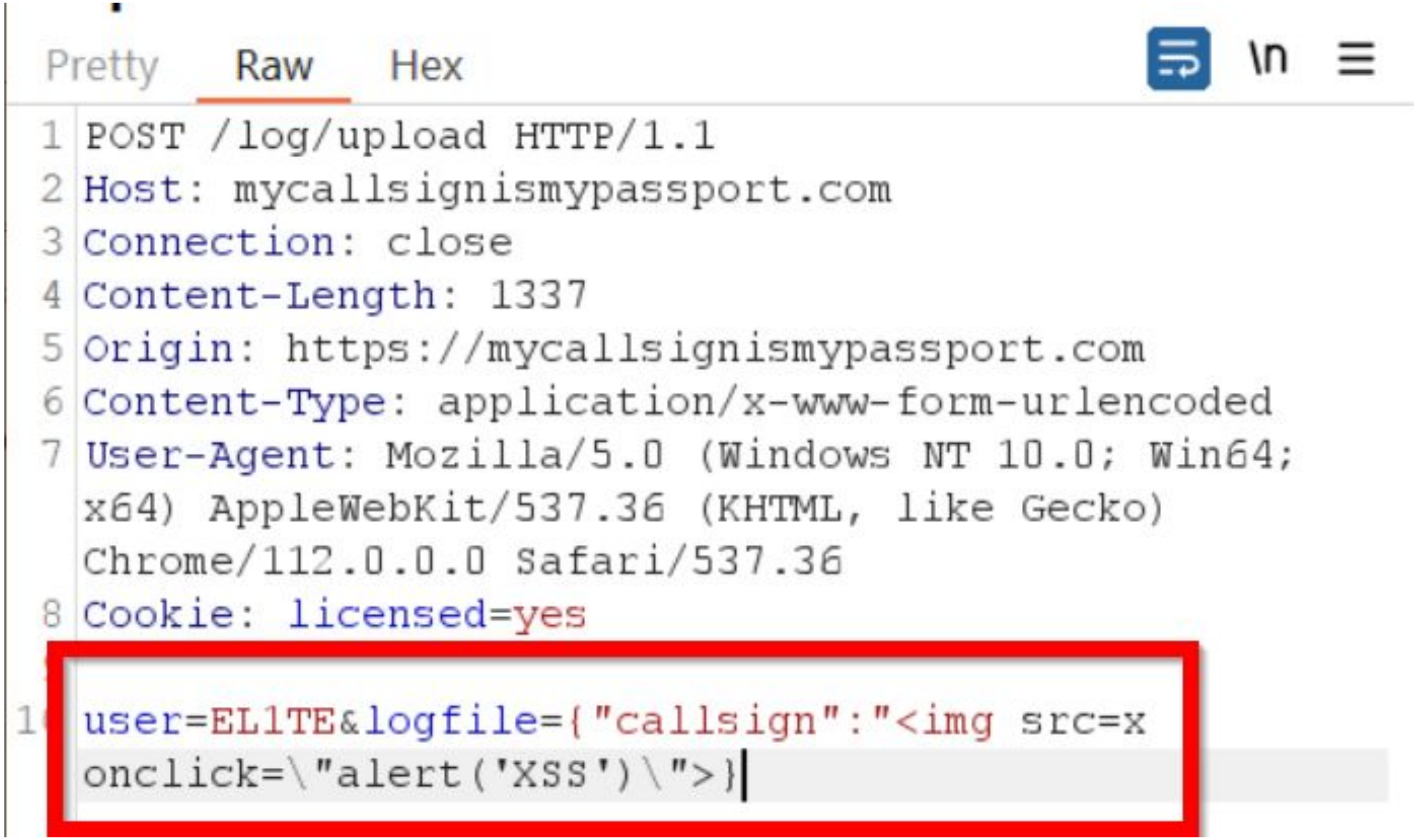


mycallsignismypassport.com:8000/mylogs.html

EL1TE's My Ham Log

Time	Date	Callsign	Location
12:02	07-29-1958	NA5A	Merritt Island, FL
12:02	07-01-2023	N0OPS	Titusville, FL

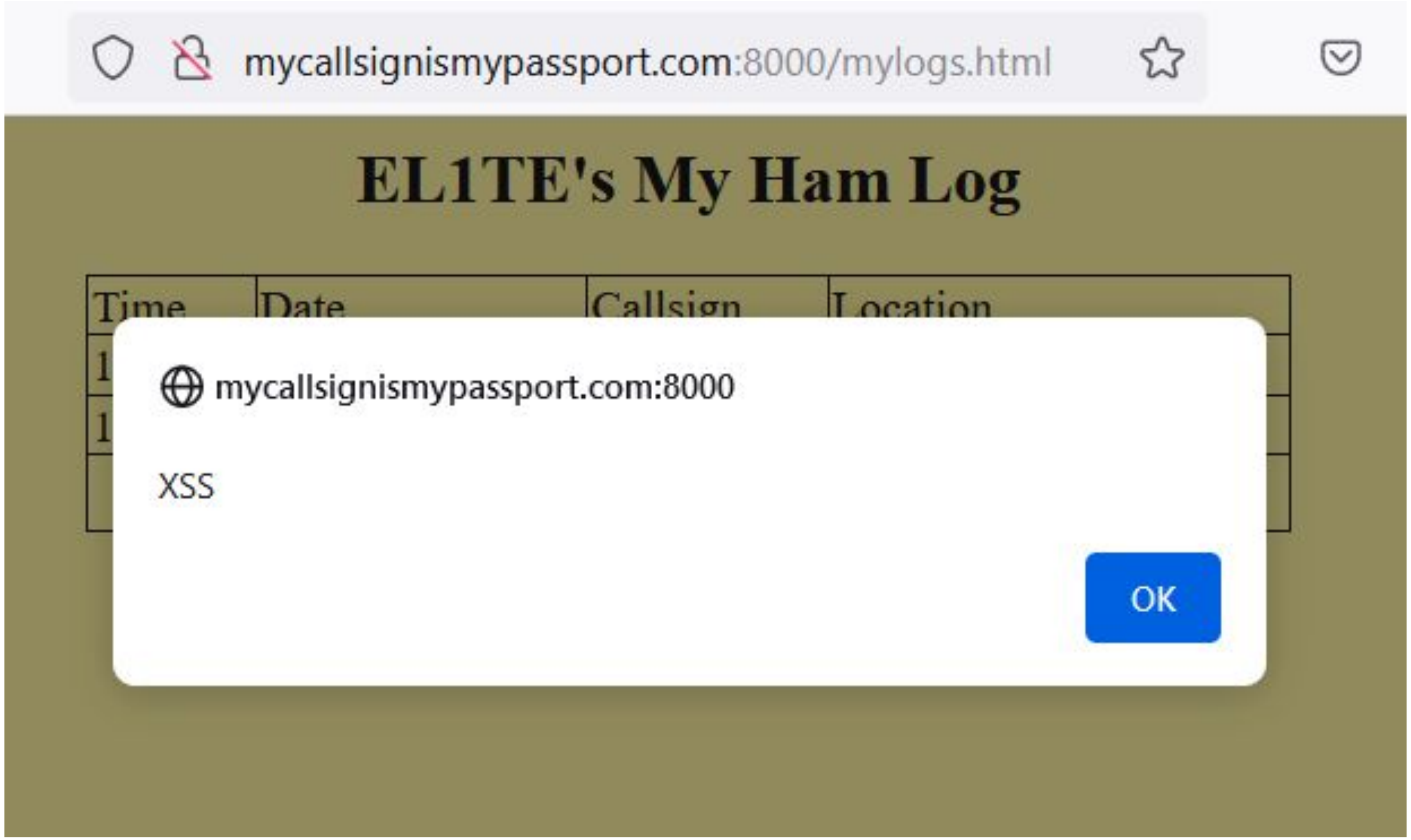
What We Found - XSS



```
POST /log/upload HTTP/1.1
Host: mycallsignismypassport.com
Connection: close
Content-Length: 1337
Origin: https://mycallsignismypassport.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Cookie: licensed=yes

user=EL1TE&logfile={"callsign":"<img src=x onclick=\"alert('XSS')\">}
```

What We Found - IDOR + XSS



EL1TE's My Ham Log

Time	Date	Callsign	Location
1			
1			

mycallsignismypassport.com:8000

XSS

I HATE TLS FINDINGS

No Pentest Report is Complete Without TLS

- TLS certificate in use had an annual cost of over $200
- Recommended replacing with LetsEncrypt.org
- Provided the correct installation instructions for the infrastructure

How prevalent is the problem?

There appears to be deficiencies

- Quick Shodan search of ~20 ham radio websites found suboptimal patterns
  - What’s a firewall?
    - 40% have excessive exposed services
  - Patching is sporadic
  - Single-tier architectures

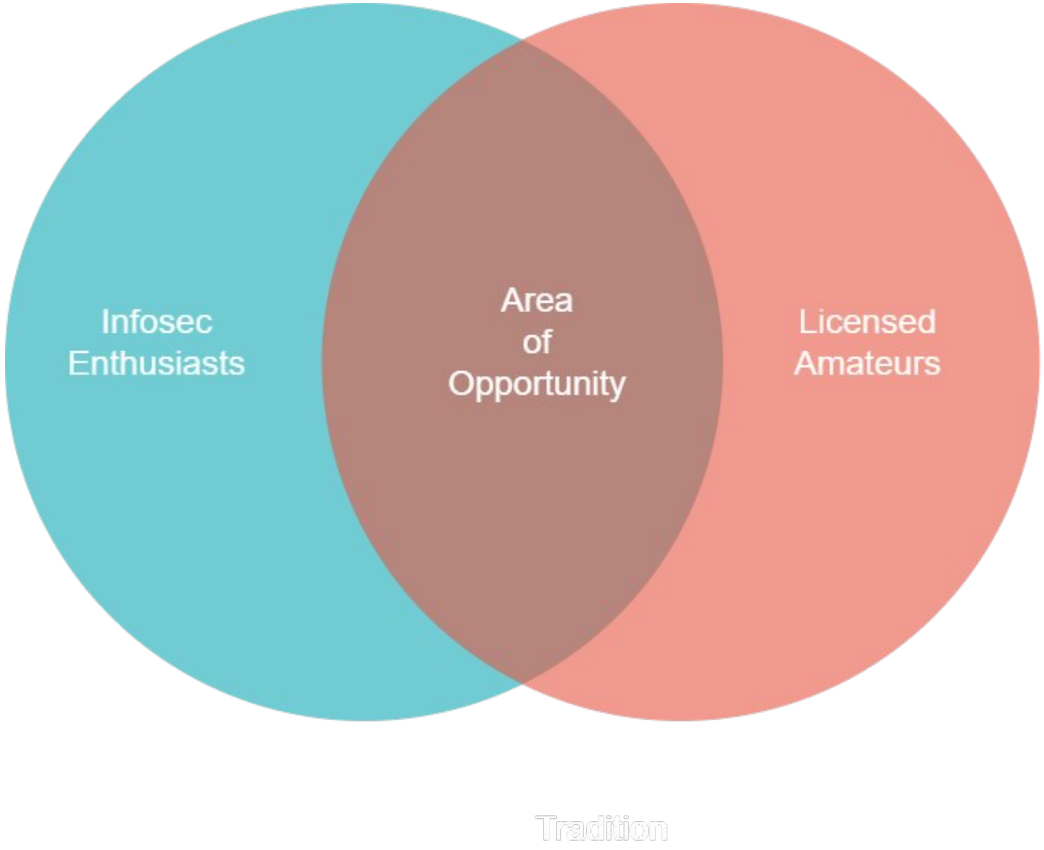
What can we do about it?

The Approach

- If we could do it, why can’t other hams in the infosec community apply our strategy?

- **Callsign = Identification ~ Trust**

- Reach out to your favorite sites, identify yourself as a ham involved in infosec, provide your callsign, and request permission



Draft Rules of Engagement

- **Get permission from site owner**
- “Friend-DA” is the name of the game
  - Honor the scope and constraints originally agreed to
    - No legal protections
    - Avoid destructive testing
    - Don’t disclose what you were asked to keep private
  - Treat like a Prod env regardless

Draft Rules of Engagement

- Focus on identifying issues and recommending solutions
- Offer to help with fixing if so inclined
  - Consider actual remediation to be a bonus
    - Understand many sites will have limited resources to implement fixes
- In the spirit of amateur radio licensing
  - Foster a collaborative dialogue vs an adversarial one

DFIU

- Know your limits
  - We are trying to help, not generate stress for the site owners
  - Stick to what you know
  - Treat every system like it’s Prod and under SLA
    - Skip the Low Orbit Ion Cannon
  - Know when to stop
  - Potential Computer Fraud and Abuse Act (CFAA) violations

Example solutions to the common themes

- System Issues
  - Limit attack surface
    - Network Firewall
    - Shut off services
  - Segment logical functions
  - Patch systems
- App Issues
  - OWASP Secure Coding Guide
  - WAF

Who Can Help?

- Something for everyone!
  - Red teamers - test for active vulns
  - AppDev background - check for OWASP Top 10
  - General tech industry - help with remediation and infrastructure review
  - Audit background - map current config against framework like CIS Benchmarks or Cybersecurity Framework (CSF)

What needs more thought?

- Just trying to start the conversation
- There’s obviously a need
- How to handle unmotivated / unresponsive (or worse) site owners?
    - Kinda back to where the broader tech industry was with responsible disclosure 20 years ago
- Should typical responsible disclosure timelines be part of this?
    - Is the data on these sites important enough to warrant it?

Looking Down the Road

- Legalese that could provide some actual protection
    - SOW-like paper trail could be beneficial
- “Bug Bounty”
    - Paid program a non-starter, paper awards a la Worked All States (WAS)?
- Develop a community-sourced testing methodology
    - “These are the top things we should look for on every site”
    - Standardize community report templates
    - Other supporting references

References

- Security Research Threats
  - threats.disclose.io
- OWASP Secure Coding Practices Quick Reference
  - https://owasp.org/www-project-secure-coding-practices-quick-reference-guide
- NIST Cybersecurity Framework (CSF)
  - https://www.nist.gov/cyberframework
- CIS Benchmarks
  - https://www.cisecurity.org/cis-benchmarks

Contact Info

Lucas

n0ops@protonmail.com

qrz.com/db/n0ops

Dan

dannorte@protonmail.com

qrz.com/db/w0bdp

Slide deck will be posted at github.com/mycallsignismypassport

Thank You