

# A JOURNEY FROM ALERT(1) TO P1

CARY HOOPER  
@NOPANTROOTDANCE  
//HOOPERLABS.XYZ





# AGENDA

- INTRO / GOALS
- DEMO
- THE PHISH
- SHARPENING THE AXE
- FINAL PAYLOAD (TO MAXIMIZE FUN)

# ./WHOAMI

Cary Hooper (h00p)

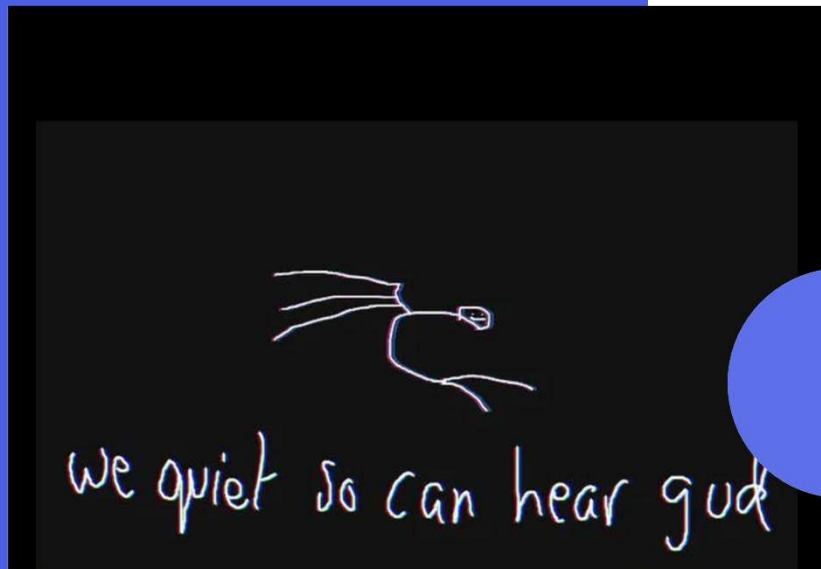
@nopantrootdance

Hacker

[www.hooperlabs.xyz](http://www.hooperlabs.xyz)

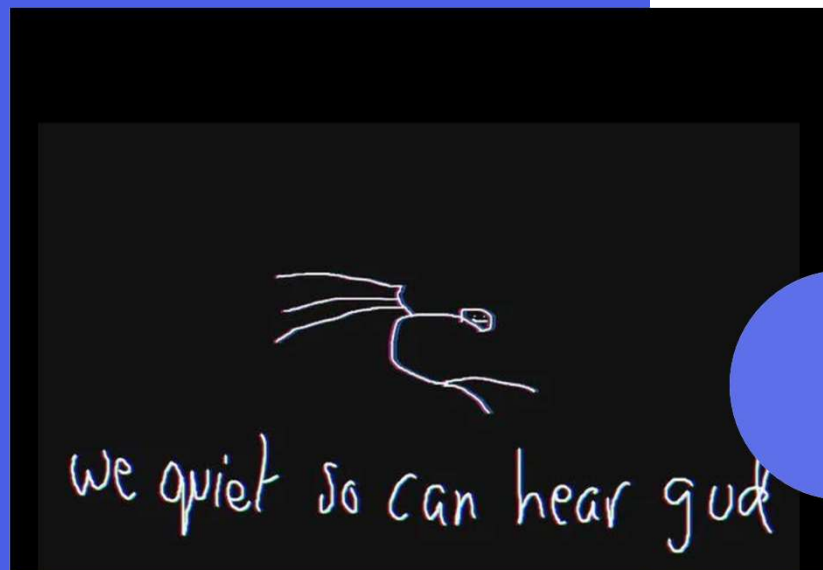


# INTRO



- + XSS Fatigue
- + Changes to Security Landscape
- + Maximize Impact
- + Maximize Fun

# INTRO



- + XSS Fatigue
- + Changes to Security Landscape
- + Maximize Impact
- + Maximize Fun
- + Cats
- + Self-Care
- + Cybering Good and Doing Other Stuff Good Too



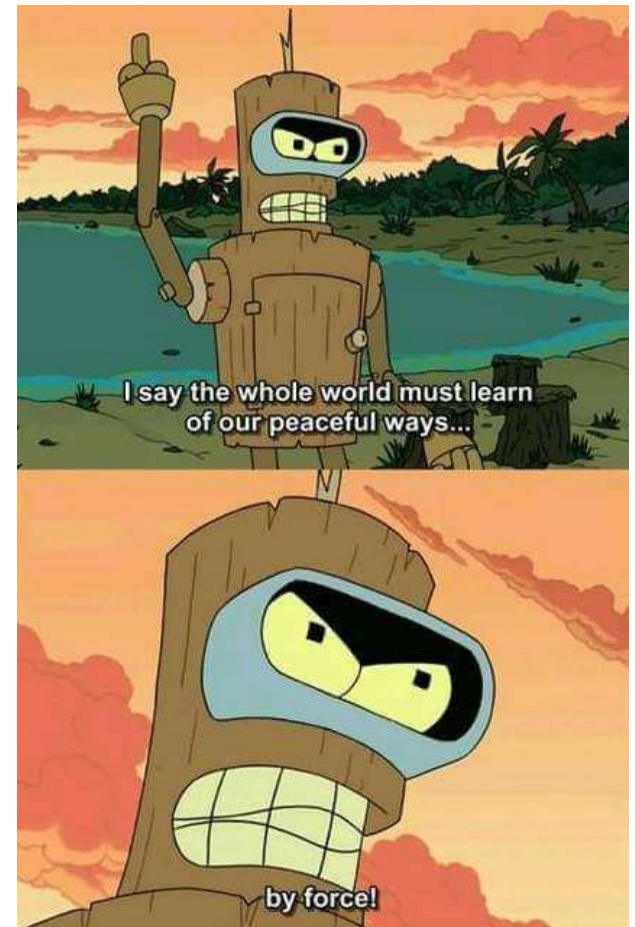



# GOALS

XSS: BEYOND ALERT(1)

NIFTY TRICKS

NETWORK ACCESS





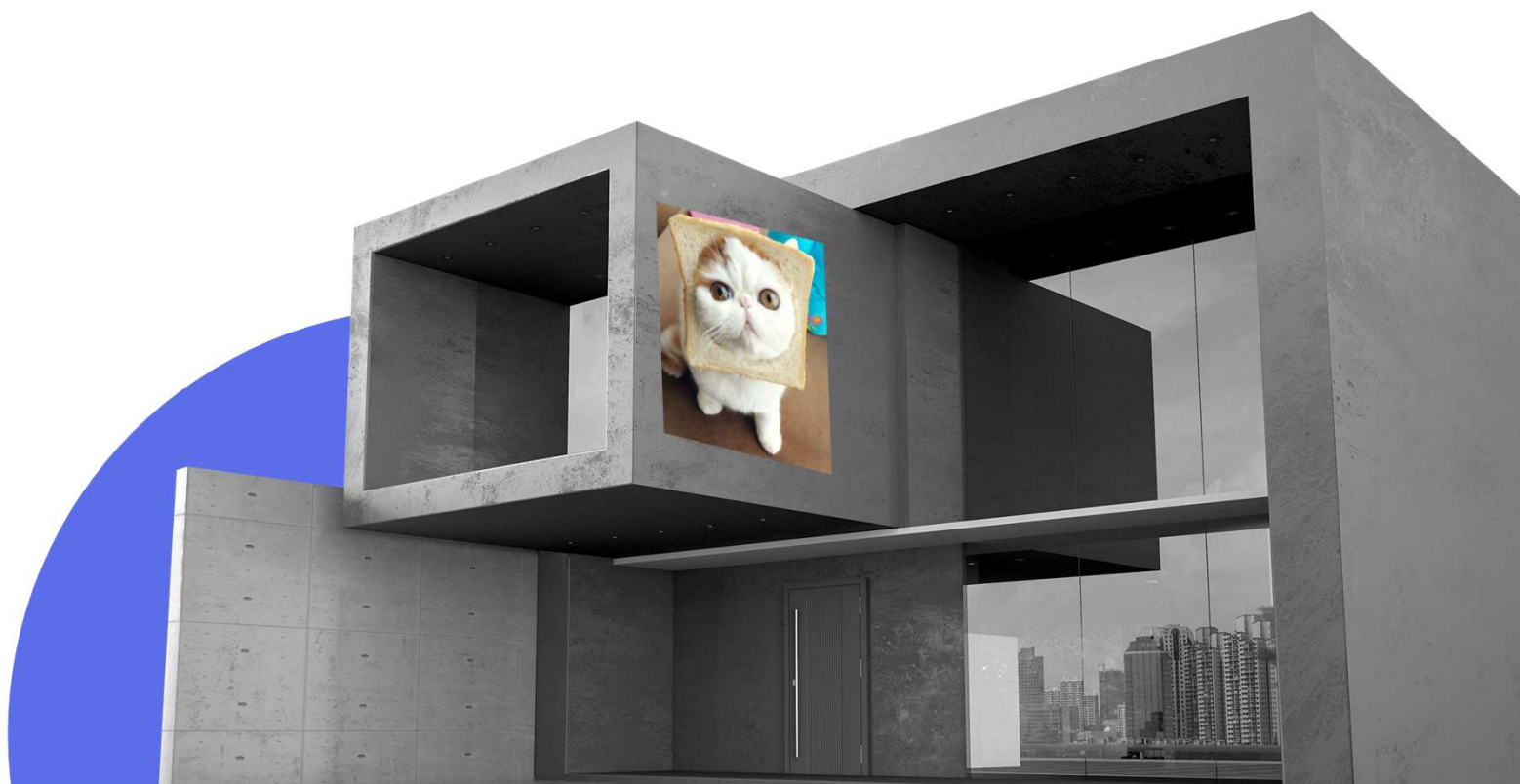
# **ALERT(1) SUCKS**

“

YOU CAN'T ARGUE WITH A ROOT SHELL

”

Felix “FX” Lindner





DEMO



# ATTACK TOOLS



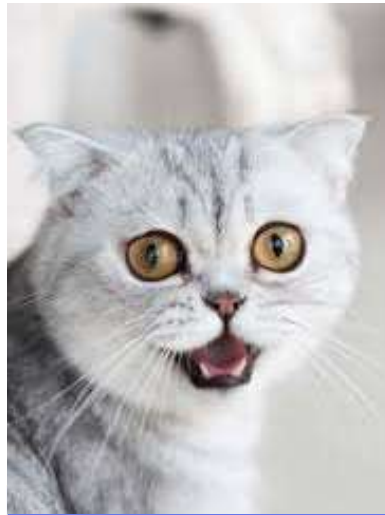
## XSS Vector

Vuln on CO Domain Site



## DOM Manipulation

(Ab)using JS like a Dev



## Cred Harvester

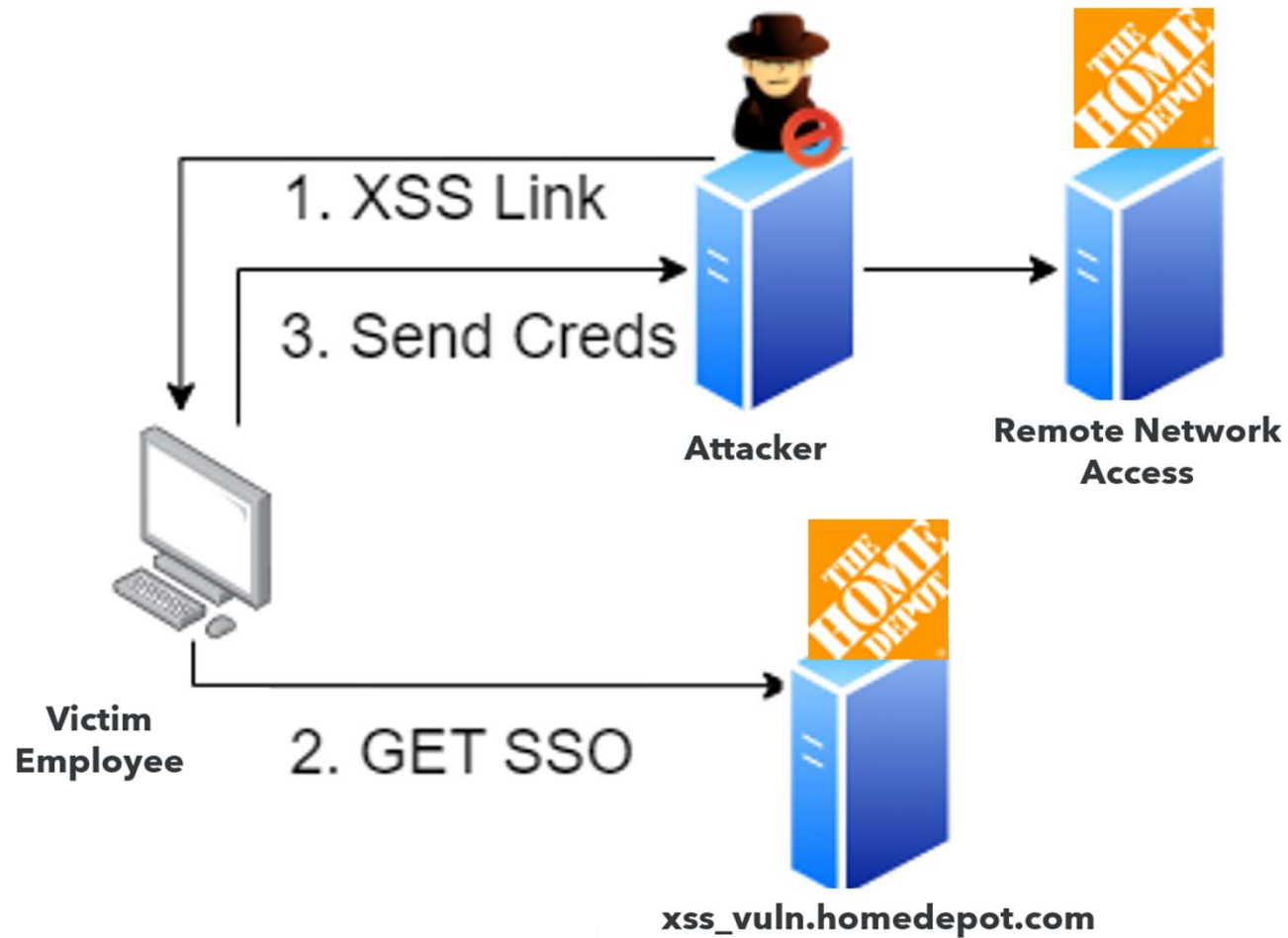
PHP File on Web Server



## Automation Script

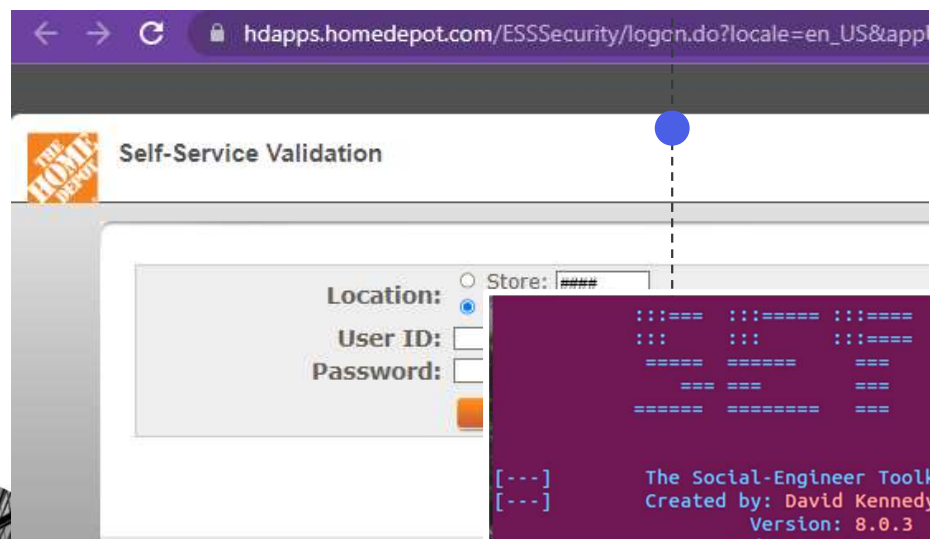
Python "requests" + "bs4"

# INFRA DIAGRAM





# SET



```

:::==  ::::==  :::==
:::  :::  :::
=====
===  ===  ===
=====

[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]              Version: 8.0.3
[---]              Codename: 'Maverick'
[---]      Follow us on Twitter: @TrustedSec      [---]
[---]      Follow me on Twitter: @HackingDave     [---]
[---]      Homepage: https://www.trustedsec.com   [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

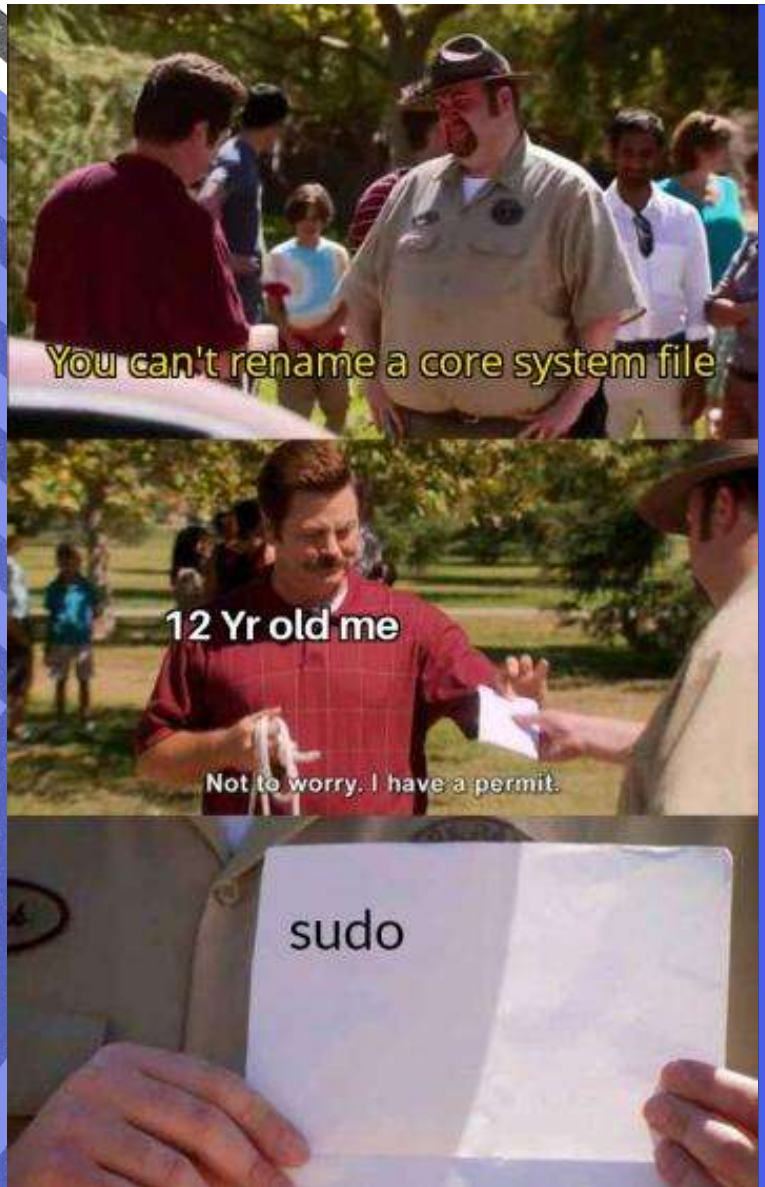
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```

DEMO





# THE PHISH

## DEVELOPING OUR OWN

- Demo to follow

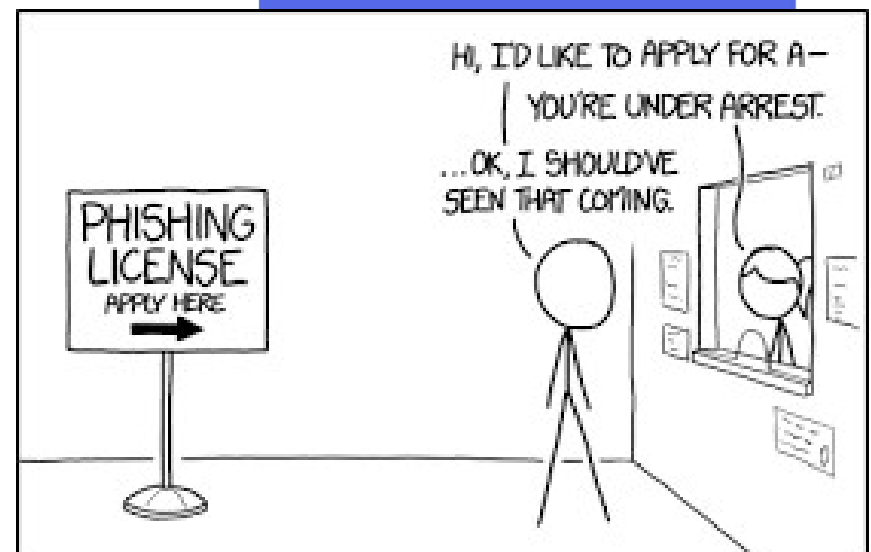
## SHARPENING THE AXE

- CSP
- HTML >> XSS
- JS

□□□□độçạêñtj□čộđỳ□îñşêstjAdkắçêñtjHỖÑL'

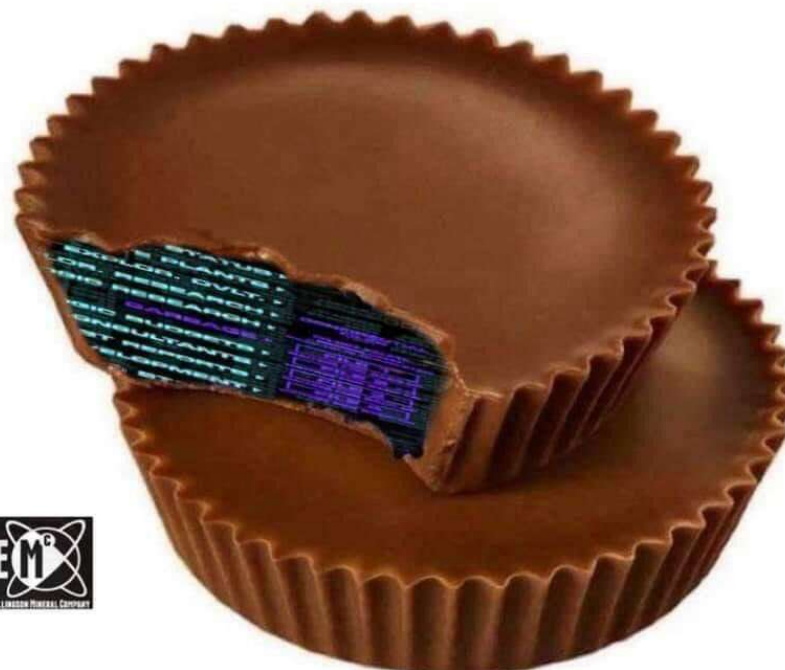
□□□□□DỒÑCộñtjêñtjLộắđêđ□□êwêñtj

□□□□çộñşộlê□lộg□□gêñtj□çsêắtjîwê□□



DEMO

be sure to check your kid's halloween candy. last year someone tried to hide an entire **Gibson Garbage File** in this reese's.



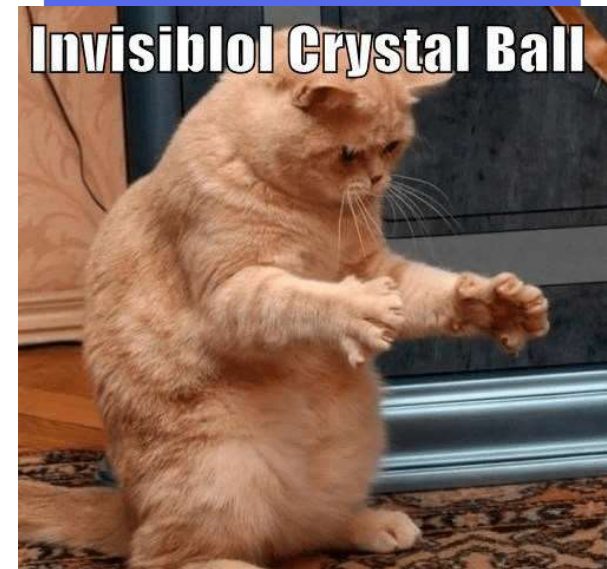
# DETECTIONS

## CAUGHT!

- Canaries... canaries everywhere
- “Failed Auth” during dev/testing
- RFC 1918 Referer

## OPPORTUNITIES

- Login from cloud IPs (non-residential/non-corporate)
- Impossible Travel Logins? (Geo-IP analysis)
- Unexpected Referrers (long tail analysis)
- Bot Detection
  - Synchronicity of Login Flow (vs browser)
  - Incomplete Logins
  - Unexpected URL-encoding in legitimate endpoints



# SUMMARY

- HTML Injection (cats)
- Manual Payloads Don't Take Long
- Script + Automate for Impact
- Creativity is Key
- Maximize Impact and FUN







# THANK YOU!

Cary Hooper

@nopantrootdance

hooperlabs.xyz