# A Bug Hunter's Journey from CTFs to Cash: Shifting to the Bug Bounty Hunter's Methodology

**Ads Dawson (@GangGreenTemperTatum   )**



Ads x BugCrowd x UNB

Nov 1, 2025

# whoami

**Ads Dawson
(@GangGreenTemperTatum / @0xmoose)**
Harnessing code to conjure creative chaos.. think evil;
do good.

Staff AI Security Researcher @ Dreadnode

Bug bounty hunter & bench penetration tester

BugCrowd Hacker Advisory Board member

Caido hacker ambassador

BugCrowd ITMOAH 2024

OWASP chapter and project lead

Ads Dawson (hacker) - 2025 - @GangGreenTemperTatum
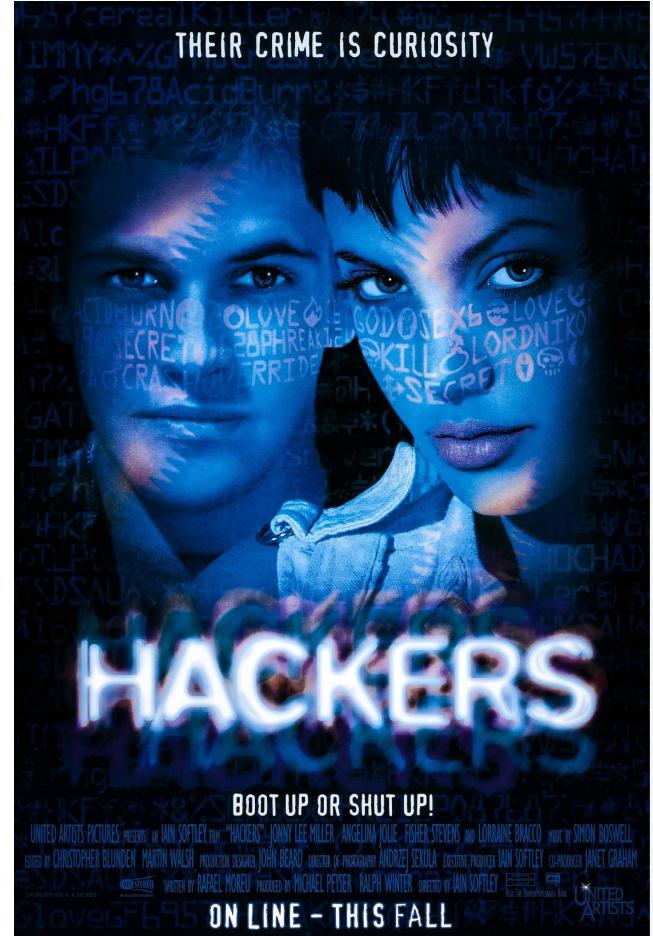
# My journey

**School**
**Dropout**

**Network intern**
**Student and sleepless nights**

**Web apps and OWASP**
**Hunger, curiosity and addiction**

**AI + AppSec**
**Breaking and using cutting edge tech**

I started my journey in tech with a hands-on apprenticeship, choosing practical experience over a traditional academic path.

My early career was dedicated to mastering network engineering at an advanced level with Cisco, where I built the foundational skills for a future in cybersecurity.

I transitioned into application security, leading chapters at OWASP, contributing to global standards like ASVS, and becoming an addicted bug bounty hunter.

Leading AI security research at Dreadnode, I now use bleeding-edge techniques to break next-gen AI and architect autonomous offensive security systems.

# Hacker DNA

- Someone who breaks things just to see how they work

- Someone who fixes things only to break them again in a different way.

- Someone who refuses to accept *"that's just how it's done"* as an answer

- The ones who refuse to think in straight lines

- They see patterns others miss, anticipate failures before they happen

- Hack the planet



THEIR CRIME IS CURIOSITY

HACKERS

BOOT UP OR SHUT UP!

UNITED ARTISTS PICTURES PRESENTS AN IAIN SOFTLEY FILM "HACKERS" JONNY LEE MILLER, ANGELINA JOLIE, FISHER STEVENS AND LORRAINE BRACCO MUSIC BY SIMON BOSWELL
EDITED BY CHRISTOPHER BLUNDEN, MARTIN WALSH PRODUCTION DESIGNER JOHN BEARD DIRECTOR OF PHOTOGRAPHY ANDRZEJ SEKULA EXECUTIVE PRODUCER IAIN SOFTLEY CO-PRODUCER JANET GRAHAM
WRITTEN BY RAFAEL MOREU PRODUCED BY MICHAEL PEYSER · RALPH WINTER DIRECTED BY IAIN SOFTLEY UNITED ARTISTS

ON LINE – THIS FALL

https://medium.com/@gonzo-hacks/the-hacker-mindset-humanitys-best-defense-a25d3e8b580e

# Hacker mindset: Bounty, or VDP?

## Bounties

**Pro**: You get paid cash rewards for valid findings, directly monetizing your hacking skills.

**Con**: The high competition often leads to duplicate findings, making it difficult to get your first payout.

## VDPs

**Pro**: Less competitive environment to find your first real-world vulnerabilities and build a public track record through acknowledgments.

**Con**: You won't receive any monetary payment, as the reward, limited to experience and public recognition.

## Red pill or blue pill

Welcome to the real world homie. Alright, so you've been grinding away at CTFs, you know how to pop a shell, and you're comfortable with the tools. So, which one do you take?

# Shifting from CTF to bounty: Threat Modelling

- Put yourself in the shoes of the company who owns this application, or any customer/stakeholder

  and ask yourself:
    - What brings risk to stakeholder of this application?
    - What is and isn't "allowed" from a users perspective?
    - Are there any warnings from the application that state the above
- Understand the attack surface, focus on business logic and think about chaining vulnerabilities with

  this in mind
- Become a power-user of the application, record your steps and observe those network requests

  being made
- Don't jump right into breaking it, understand these fundamentals first

https://projectdiscovery.io/blog/bug-bounty-etiquette-2-what-not-to-do

Ads Dawson (hacker) - 2025 - @GangGreenTemperTatum

# First: RTFM
## Program and Developer Docs

The scope document is your contract. Ignoring it is the fastest way to get your reports closed as Not Applicable and waste weeks of your time

Developer docs are sometimes the secret weapon that most hunters ignore. The developer and API documentation is a treasure map written by the people who built the fort

**1**

**What's in-scope and out of scope explicitly?**

**2**

**Read the developer docs to understand the inner and outer workings**

**3**

**Recon the tech stack and look for "focus areas" in the program**

**4**

**Are there any known issues?**

BugBoss v3:
https://www.youtube.com/watch?v=zlodGMqAuD8



RTFM OR

YOU'RE GONNA HAVE A BAD TIME

makeameme.org

# Pick your battles

- "*Spray and pray*" vs. sniping: In CTFs, you're rewarded spraying at every possible vulnerability to grab flags

- In bug bounties, you get paid to be a sniper, patiently finding that one, unique, high-impact shot that no one else saw

- Low noise, high signal is key - the vulnerabilities that have a real business impact and make a company go, "Oh, that's bad."

- Don't be a swole doge

- The "One-Trick" Cheems is a lie

- It's about depth, not just breadth of testing

- INVEST IN YOUR OWN PAYLOADS / *"I see this is being reflected in the DOM, could I use that payload from the other program?"*

I hunt for every bug
bro RCE, CSRF, SSRF, XSS...

0 $
reward

imgflip.com

1 trick
XSS

10K $
reward

# Save dem' payloads.

`` `t"/><iframe src="//evil.com"> (10200001)` ``

# Sell your submissions

- The anatomy of a good report first demonstrates immediate impact without over inflating

- Title is the first thing a triager sees. Make it count. It should be a concise summary of the vulnerability and its

  impact.

  - Bad Title: "XSS Bug Found"

  - Good Title: "Stored XSS in User Profile Page Leading to Admin Session Hijacking"

- Provide clear, numbered steps

- Use screenshots, GIFs, or even a short video for every key action.

- Include the full request and response payloads.

- Avoid AI slop

- PoC needs to be foolproof

  - Bad: "*An attacker can steal cookies.*"

  - Good: "*By stealing an administrator's session cookie, an attacker can gain full administrative*

    *access, allowing them to view, modify, or delete any user's data on the platform.*"
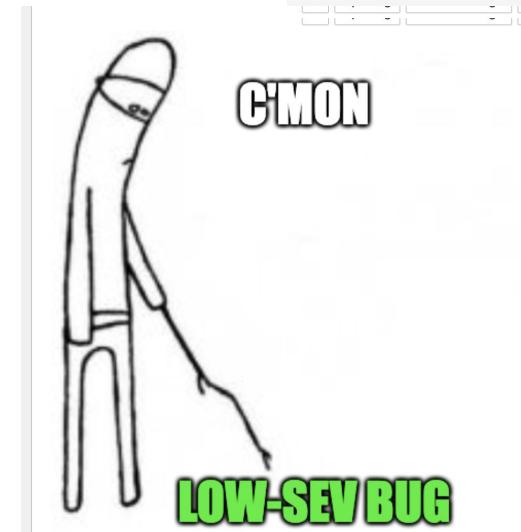
https://medium.com/@pm_/guide-crafting-a-neat-and-valuable-le-bug-bounty-report-0bf1bc933bdc

Ads sample report: https://gist.github.com/GangGreenTemperTatum/4699f7503fe3eb2dcf7e35dd0dd63a22
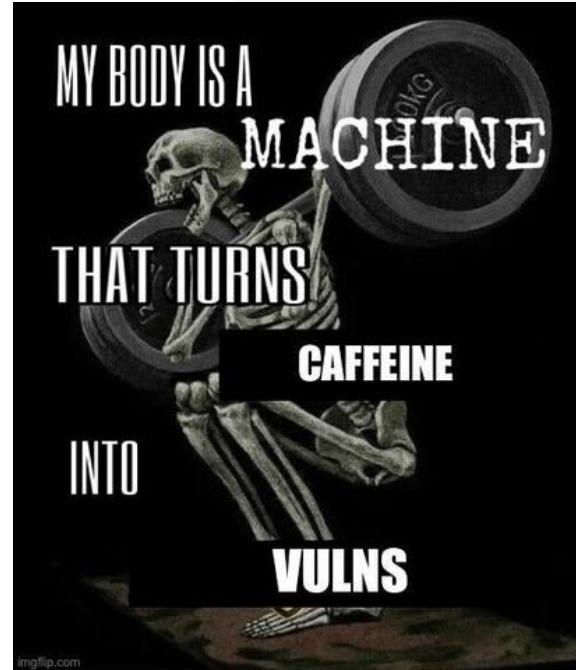
# Case study: @ads P3->P1 ATO CHAIN YOUR BUGS

- Password reset current password bypass - so what?

- IDOR - can we perform that action on another user account?

- Need cookies - where can we inject data into the app to steal

   another users cookies?

- Chain these bugs == full account takeover of all users

# LOVE what you do.

- Surround yourself with others in the same mindset

- Shiny rocks are awesome

- Share wins with friends, celebrate and root for your homies

- It's OK if you aren't this way and isn't for everyone

# Hacker psyche

- Welcome the challenge, real world programs aren't preloaded with flags

- Some devs are VERY good but don't test the simple stuff

- Embrace failure, don't be shy or scared

- Failure is an opportunity to learn

- Reach out to friends, don't suffer alone

- Speak up, say something

- Get that first bug under your belt

- If you don't understand a vulnerability class, research it and become a frickin expert at it

- There's no secret recipe to time spent on program vs vuln, find what works for you



GONNA BURN THIS ODAY

...AAAAND IT'S PATCHED

imgflip.com
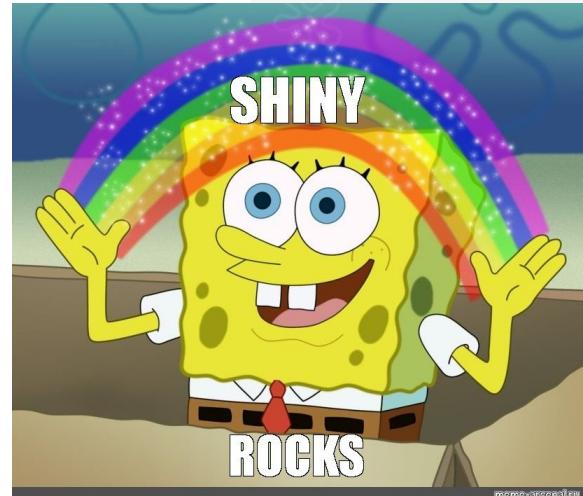
# Imposter syndrome is real

- Imposter syndrome thrives in environments where skill and achievement are central

- The more you learn about a complex field, the more you become aware of how much you don't know

- The highlight reel effect

- Track Your achievements and keep a running list of your successes, big or small

- Reframe Your Thoughts: Instead of thinking, "I got lucky," try thinking, "*my hard work paid off*"

- Speak up, share your feelings with a trusted friend, mentor, or colleague

- Embrace "Good Enough" and don't strive for perfection

- Aim for progress and completion rather than an impossible

# Never give up or leave any shiny rock unturned

- Why did my submission get declined/de-escalated?

- How can I further demonstrate impact?

- Does my report/submission read well, can I understand it?

- Can I chain this bug with something more meaningful?

- Store observations and bugs into RAM or take notes for later use

# Community is king

When you hit a wall, someone in the community has a ladder

Bugs and payouts are temporary, but a strong network is the most valuable asset you'll ever build in this industry

**1**
**When you hit a wall, someone in the community has a ladder**

**2**
**This industry is full of awesome people
Those awesome people want to see you succeed**

**3**
**Follow researchers, join discussions, and absorb information**

**4**
**Found something? Share the win with others and educate**

Ads Dawson (hacker) - 2025 - @GangGreenTemperTatum

# Collaboration: Sometimes the recipe for success

- Pair programming, but for pwnage

- You learn their perspective: You'll see how they approach a target, the unique tricks they use, and the logic they apply. It's like getting hands-on training for free

- You share your own skills: Teaching someone else your techniques is one of the best ways to solidify your own knowledge

- You get fresh eyes on the target: When you've been staring at an endpoint for six hours, you go blind to the obvious. A hacking buddy can look at it for five minutes and spot the simple mistake you were making

- Sharing wins with friends is awesome

# Stay hungry - never lose the student mindset

**BugCrowd University**

https://www.bugcrowd.com/resources/levelup/introduction-to-bugcrowd-university/

**Public Submissions**

Public writeups and submissions are a great way to understand how to shift your creative ways

**Critical Thinking**

https://www.criticalthinkingpodcast.io

**PortSwigger Labs**

https://portswigger.net/web-security

**Researcher' blogs**

https://jameskettle.com/, https://blog.orange.tw/ and more

**YouTube**

@JHaddix (Bug Bounty Hunter's Methodology), @NahamSec, @Medusa0xf, @AmrSecOfficial and more

Ads Dawson (hacker) - 2025 - @GangGreenTemperTatum
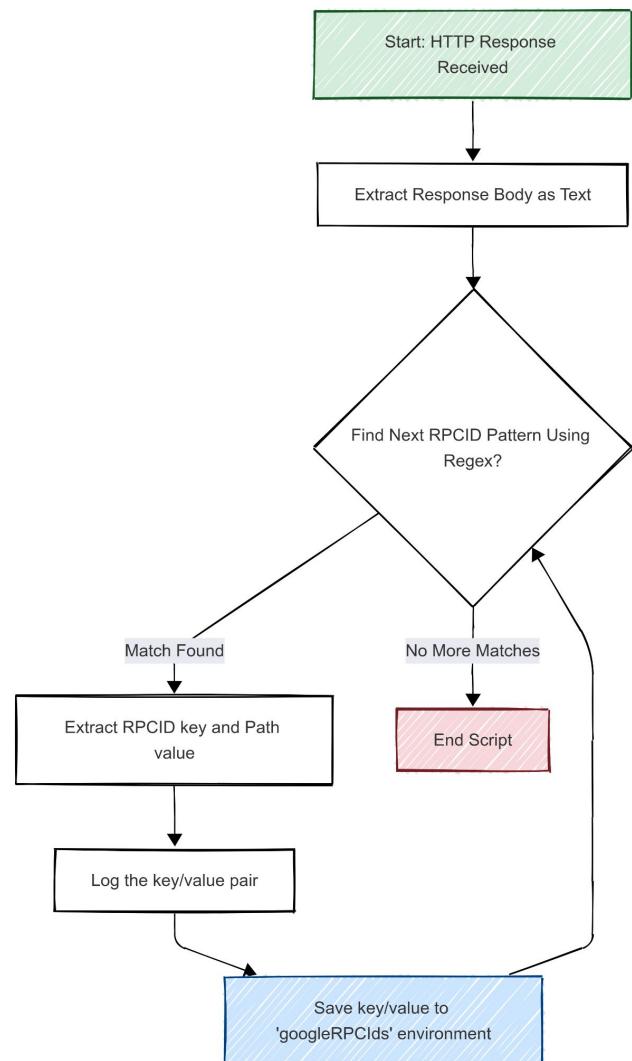
# Case Study

## Hacker Mindset - Do your homework

## Google Bard RPC ID's - WTF? = Caido workflow

- Credit: @Rhynorater
- **Problem**: Google Bard's API uses RPC cipher IDs for services
- **Why**: It's painful for us as hackers to understand what RPC ID is what service - we don't know what endpoints or services we are trying to exploit
- **Hacker mindset & solution**: The process begins when an HTTP response is received, and the script immediately starts looping through the response's text, using a Regular Expression to hunt for a specific code pattern.
- Each time a match is found, the script extracts the key (the rpcid) and the value (the descriptive path) and saves the pair into a shared environment, continuing this loop until no more matches exist in the file.

# Case Study

**Hacker Mindset** (watch video up until ~4:30mins)



**My First Bug Bounty Experience (It Was a Mess!) - Credit: @CyberFlow**
https://www.youtube.com/watch?v=lV9skVPlbnA

# Report Write Up Reviews

Live demonstration of public writeups