Bug Bytes #176 – Deepfake dangers, @rhynorater's SSRF magic, recon techniques everyone misses & more!

BY ANNA HAMMOND · OCTOBER 5, 2022 · LAST UPDATED ON MARCH 6, 2025

Welcome back everyone to Bug Bytes, the weekly newsletter curated by members of the Bug Bounty community!

As you may have read in the last issue the previous author of Bug Bytes, Mariem / PentesterLand, left Intigriti and the torch of Bug Bytes to whomever would take it up.

Every week she kept us all up to date with comprehensive list of write-ups, tools, tutorials and resources, some big boots to fill!

We can now announce that this torch and boots will be filled by InsiderPhD.

This issue covers the weeks from September 26th until October 1st.

CLICK HERE TO SUBSCRIBE

Introduction to InsiderPhD

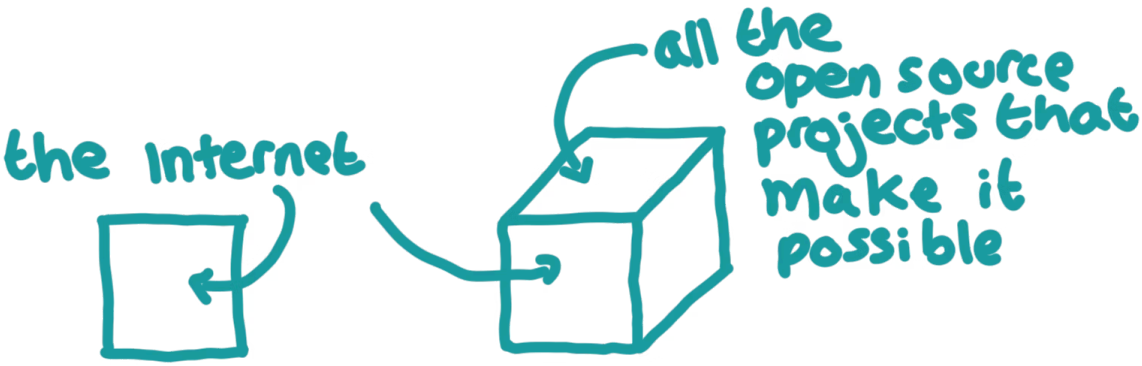
Hello, my name is Katie aka InsiderPhD, you may know me from my YouTube videos on getting started in Bug Bounty or through my talks on API hacking. I'm also a lecturer at a university in cyber security. I was a

huge fan of Bug Bytes from back before it was on Intigriti, so it feels like a big role for me to fill. Hopefully I can add my own flair onto your usual newsletter expectations. I'm still figuring this out so please do tag me on blogs or videos you'd like me to see and give me some feedback on how I could improve things.

Intigriti News

- Inti De Ceukelaire will be speaking at IWCON2022
- You can now edit and remove messages on the platform
- Our monthly challenge is over! Check out the results and write-ups

From my notebook



This week, open-source security has really been on my radar, thanks to an article in the New Yorker about how the internet keeps to time. Open source is neat like that it's like the bass in music, you know when it's missing but otherwise it's in the background. For bug hunting this is really interesting because behind every app there's a slew of open-source projects keeping it together, and these are often full of vulnerabilities, especially if they are out of date. So, I've included some recent open-source security links as well as some links from the archive on open-source security and code review.

What's on your radar this week? What kind of vulnerabilities are you reading about?

- The Thorny Problem of Keeping the Internet's Time
- Stargazers Github stargazers information gathering tool
- Finding Security Vulnerabilities through Code Review OWASP DevSlop and How to Analyse Code for Vulnerabilities
- Intigriti hosted an open source programme on behalf of the EU commission you can read about it here
- CVEs are flaws that affect software that lots of people use, so think about every company that uses Microsoft products or open source, CVENew on twitter is a great way to keep up to date on recent CVEs and here is a video showing a CVE that affects the open source web server Apache by Ran$ome as an example
- As for tooling we have to give a shoutout to Nuclei who implement automatic scanning for a bunch of CVEs in open source tools https://github.com/projectdiscovery/nuclei – remember when using a

vulnerability scanner to read the targets scope, check the request rate and confirm any vulnerability with a manual test!

Other Amazing Things

- IppSec HTB Scrambled
- CryptoCat HTB Tier 0 Starting Point Walkthrough
- LevelUp X 8 ways to (Almost) never get a dupe again
- My First Year in Cyber – Cyber Warrior Studios
- H1 702 recap Nahamsec
- Creepy OSINT – Forgot Password tips

- Live Recon – Rhynorater Talks About Grafana SSRF, Picking Bug Bounty Targets, and His Favorite Hacking Tools!
- Cybersecurity and Cloud Podcast
- SecurityNow Darknet Politics
- SmashingSecurity 291: Deepfake dangers, AI image opt out ansd controlling your urges
- Risky Business 680 Uber, Rockstar Games hacker arrested
- Hacking Humans – A cryptoqueen on the run and the cons she got away with
- Malicious Life – What's it like to fight Lulzsec
- Breaching the wirefall with community OWASP podcast

- Best recon tools by ShreKy
- I hacked a gaming company this year, here's how I did it by Corben Leo
- Thoughts on infosec mentoring by hacks4pancakes
- Testing/Recon methodology by @ManieshNeupane
- Full time hunters share their thoughts of existential crisis
- JWT by @sec_r0

- BSides London 9-10/12/2022
- CyberWarCon 10/11/2022
- AWS Community Days 2022 (India 10/11/2022)

- Investigating webshells
- Cool Recon techniques every hacker misses! Episode 2
- IDOR on Apple
- How To Attack Admin Panels Successfully
- How I abused the file upload function to get a high severity vulnerability in Bug Bounty
- Monitoring your targets for bug bounties

- Short write up on dirsearch
- Orange Arbitary Command Execution

- Nginxpwner (a simple tool to look for common Nginx misconfigurations and vulnerabilities)
- Dnsx v1.1.1 released
- ASNmap

- GDPR
- Shodan
- cURL

- 0day RCE In Microsoft Exchange
- Willful Security Ignorance: Are you Exposed to Old Vulnerabilities
- Major Database Security Threats
- An attacker's guide to AWS Access Keys

Challenges

- TryHackMe free challenge corridor
- H4CK1NG Google
- Phoenix CTF – Charity CTF

Bug bounty/Pentest news

- HackTheBox launches certified penetration testing certification
- Snyk launches code checker

Non-technical

- I spent 2000 hours learning how to learn
- Optus under $1million extortion threat
- IOS16 Security and Privacy Features Firewalls Don't Stop Dragons