Bug Bytes #163 – Uber Eats payment bypass, Mystery lab challenge & 1337Up livestream

BY ANNA HAMMOND · MARCH 16, 2022 · LAST UPDATED ON JULY 31, 2025

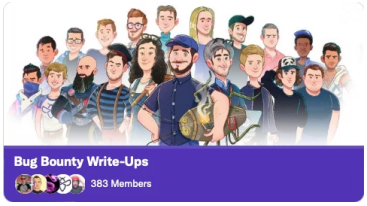
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from March 7 to 14.

Intigriti news

"Bug Bounty Write-Ups" community



We have a brand new Twitter community!

It is a place where you can share with us your bug bounty writeups, and stay informed of the latest and most informative writeups.

Join now

Our favorite 5 hacking items

1. Vulnerability of the week

What caused the Uber Eats glitch that allowed ordering free food for a weekend in India?

@GergelyOrosz explains a bug in Uber Eats that allowed students in India to order around $14,000 of food for free. All because of a small change in an API endpoint related to idempotency...

2. Resource of the week

PortSwigger: Introducing the mystery lab challenge

If you've completed all Web Security Academy challenges and wondered what's next, you will love this! PortSwigger introduced a new functionality, the "Mystery lab challenge", that can generates realistic labs where the bug type is not known beforehand.

3. Conferences of the week

Amazon Cognito (Mis)Configurations – BSides Ahmedabad 2021
1337UP LIVE Conference (livestream)

The first talk is a walkthrough of Amazon Cognito misconfigurations by @sheth_kavisha. She goes over how AWS Cognito works and common attack vectors. To go further, here are other resources recommended by @yassineaboukir.

Another conference worth your time is Intigriti's 1337UP LIVE Conference. The livestream is up on Youtube and is a fantastic opportunity to learn about topics like how to find your first bug, 2FA vulnerabilities, creating bug bounty tools, mobile app hacking, OSINT in bug bounty, a cool red teaming story and more.

4. Article of the week

Finding Gadgets Like It's 2022 & QLinspector

@hugow_vincent shares a new methodology to find deserialization gadget chains in Java apps using CodeQL.
It has some limitations like the necessity to have the app's source code and being able to compile it, but it can help when tools like Yoserial and gadget inspector fail to find valid chains.

5. Tutorial of the week

iOS Hacking – A Beginner's Guide to Hacking iOS Apps [2022 Edition]

A lot of mobile hacking tutorials show only the first steps to set up your testing environment and stop there. This one goes further, explaining not only jailbreaking and seting up your environment with Linux as a host, but also how to actually start testing iOS apps using both static and dynamic analysis.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty Redacted #1: Exposed Redis and HAProxy
- ey! Look for patterns
- Cross-Origin Resource Sharing (CORS) | Complete Guide
- How to Use Bug Bounty to Help Your Career!

- Exploring bash Reverse Shell
- First time hacking with Burp Suite be like.
- Common Active Directory Misconfiguration | Tech Talk #1, 2022
- MentorshipMondays | How to Communicate and Write a Report, Meet Chris Evans, HackerOne's Chief Hacking Officer & How To Pick A Target

Webinars

- Stranger Danger: Your JavaScript Attack Surface Just Got Bigger!
- Breaking and Entering: A Hacker's Field Manual for Physical Access – Tyler Robinson

Slides & Workshop material

- Rules to Hack By

Tutorials

- Common Cloud Security Issues – AWS Edition v1.0
- Recon Weekly #3: Find More Subdomains using Permutations
- Bypassing CSRF token protection by abusing a misconfigured CORS policy

Writeups

Challenge writeups

- UHC – Ransom & Blog post
- HackTheBox – Devzat & Blog post
- Bypassing Basic PHP WAF to Read Files [DefCamp CTF 2022]

Responsible(ish) disclosure writeups

- Securing Developer Tools: Package Managers #Web #CodeReview
- Pascom: The story of 3 bugs that lead to unauthed RCE. #Web #LPE
- JBoss EAP / AS <= 6.X RCE 0day #Web
- Multiple vulnerabilities in FortiManager version 6.4.5 #Web
- CVE-2022-21831: Overview of the security issues we found in Rails's image processing API #Web
- Redis Lua Sandbox Escape && RCE (CVE-2022-0543) #Linux
- CVE-2022-26143: TP240PhoneHome reflection/amplification DDoS attack vector #VoIP #DDoS

- The Discovery and Exploitation of CVE-2022-25636 #Linux #MemoryCorruption

Known vulnerabilities

- Making Sense of the Dirty Pipe Vulnerability (CVE-2022-0847), Video tutorial by @HackerSploit & Max Kellermann's exploit modified (to overwrite root's password in /etc/passwd)
- CVE-2022-22005 Microsoft Sharepoint RCE
- CVE-2022-0185: A Case Study

Bug bounty writeups

- From Recon via Censys and DNSdumpster, to Getting P1 by Login Using Weak Password – "password" ($2,500)
- How I bypassed disable_functions in php to get a remote shell
- SQL Injection at Spotify (Spotify)
- Oracle Access Manager Pre-Auth RCE (CVE-2021–35587 Analysis)
- Container Escape to Shadow Admin: GKE Autopilot Vulnerabilities (Google)
- Escalating from Logic App Contributor to Root Owner in Azure (Microsoft)
- SSD Advisory – NETGEAR DGND3700v2 PreAuth Root Access (Netgear)

See more writeups on The list of bug bounty writeups.

Tools

- bypass-url-parser: Bash script that tests many URL bypass techniques to reach a 40X protected pages
- reflector: A crawler that tests HTML forms for reflection (based on hakrawler)
- tew: A quick 'n dirty nmap parser written in Golang to convert nmap xml to IP:Port notation
- GraphQL Cop: Security Auditor Utility for GraphQL APIs
- scant3r: Module based Bug Bounty Automation Tool
- swaggerHole: A python3 script searching for secret on SwaggerHub

Tips & Tweets

- SSRF via PDF export using meta tag with refresh time "0"
- Increase your luck when bruteforcing directories/endpoints on webservers like Express, Rails, Flask, Django, etc
- Can't decide what to attack first?

- Recover deleted files on Linux with dd
- A thread about starting and building your cybersecurity career

Misc. pentest & bug bounty resources

- waf-bypass.com
- Payloads to identify OOB RCE on hardened systems
- Rust By Practice
- exploitalert.com
- Cloud 9: Top Cloud Penetration Testing Tools
- Educational Heap Exploitation

Articles

- Hijacking AWS API calls
- Abusing Kerberos Constrained Delegation without Protocol Transition
- Revisiting Phishing Simulations
- Put an io_uring on it: Exploiting the Linux Kernel

Challenges

- picoCTF 2022 (March 15 – 29)
- zer0pts CTF 2022 (March 19 – 20)

Bug bounty & Pentest news

- Bug bounty
  - 1Password increases bug bounty reward to $1 million
  - @MrTuxracer on crossing the $1 million bug bounties mark
- Upcoming events
  - Bounty Thursday's ON-AIR (March 17 at 16:00 CET)
  - NahamCon2022 (April 30)
- Cybersecurity
  - Microsoft starts killing off WMIC in Windows, will thwart attacks
- Tool updates

- Burp Professional / Community 2022.2.3 (for those who “miss the speed/simplicity of the Spider from Burp Suite 1.7”)
- Sharpener v1.09
- Axiom is transitioning to Docker modules
- reconFTW v2.2.1
- Introducing the InternetDB API

Non technical

- Interview with Ippsec
- Not All MFA is Equal, and the Differences Matter a Lot
- Celebrate tiny learning milestones
- 6 Valuable Lessons I Learned Working For A Cybersecurity Startup