Bug Bytes #214 – We launch a course, bug hunters go full time and the $20k bug

BY TRAVISINTIGRITI · OCTOBER 17, 2023 · LAST UPDATED ON APRIL 4, 2025

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

This issue covers the week from October 2nd to October 15th

Click here to subscribe

Intigriti News

- Practical Bug Bounty Course Announcement with Intigriti
- Top 4 recon tools for bug bounty!
- We're hosting an Open Port event in our offices in Antwerp and you can be there!
- What is the secret to finding more high-severity vulnerabilities?
- Top 4 labs to practice RCE vulnerabilities

From my notebook

Today I've chosen to highlight video creators, some of these are faces you've heard before but are experiementing with new content, others are smaller creators who deserve some love!

1. Bug Bounty Hunting Full Time
2. The $200 Million Crypto Hack on Mixin & more
3. REDACTED 01: Featuring @hacker_
4. My $20,000 S3 bug that leaked everyone's attachments – S3 bucket misconfig of pre-signed URLs
5. Understanding prototype pollution vulnerability

- HashiConf 2023: Everything revealed in 15 Minutes
- HackTheBox – Intentions
- Brute-Forcing File Read with MD5s [HackTheBox Intentions]
- 3 Real API Bugs I got a bounty for
- How I Became a Hacker (and What I'd Do Differently)
- Create Your Own Dark Web Website
- Website Vulnerabilities to Fully Hacked Server
- Phishing, Smishing, and Vishing Explained – 2023
- This image Can Hack You (The .webp Exploit)
- Enter the World of Haiku and Learn Hacking Through Video Games
- Looking into the Looney Tunable Linux Privesc CVE-2023-4911
- Here are 3 bugs I've Found with Recon (and how I hacked them)
- How to Study Effectively | Cybersecurity and Hacking
- 5 Skills to Level Up Your Cloud Hacking
- Hacking Netgear Wi-Fi Router Default Passwords
- Hackers Are Exploiting Critical Vulnerabilities in File Transfer Software
- My SECRET Server Room Project
- SQL Injecting Beyond Strict Filters – Union Without Comma
- 23andMe Hacked! Ashkenazi Jews Targeted.

- They Took Control of His Phone (and His Life) With a Single Text Message Ep. 97: The Pizza Problem
- One More Reason to NEVER Answer Your Phone Darknet Diaries Ep. 138: The Mimics of Punjab
- A Small Town Hack Became a Secret Service Forensics Investigation Ep. 96 The Police Station Incident
- The Art of Web Architectures (Ep. 39)

- Bug Bounty Mentorships (Ep. 40)
- Web Application Pentesting and the Importance of Specialization with Tib3rius
- We accidentally Leaked AWS access Keys on Github
- 218 – A Chrome RCE, WebP 0day, and glibc LPE
- 217 – Insecure Firewalls, MyBB, and Winning with WinRAR
- Importance of Fundamentals and Home Labs with Kevin Apolinario
- EP141 Cloud Security Coast to Coast: From 2015 to 2023, What's Changed and What's the Same?

- Beginner
  - Why Appropriate Content-Type Header Matters In REST API Security: Ft. JSON XSS
  - Exploiting Insecure Firestore Database!
  - Best Ways to Find XSS in Web App Penetration Testing
  - CSRF Hunting Methodology: Basics
  - Bypassing CSRF token validation—CSRF | part—1
- Intermediate
  - [HTB Blog] Exploiting Looney Tunables
  - Web Application Vulnerabilities: CRLF Injection and Beyond
  - Out-of-Band Exfiltration Tools
  - A Beginner's Guide to AJP Proxy: Bridging Apache and Tomcat

- Security Research
  - Looking for CVE-2023-43261 in the Real World – Blog

- An analysis of an in-the-wild iOS Safari WebContent to GPU Process exploit
- LLM Security Series – Prompt Injection
- Not Your Stdout Bug
- RedTeam Pentesting – Blog – Better dSAFER than Sorry – An Attacker's Overview of Ghostscript
- Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days
- Critically close to zero (day): Exploiting Microsoft Kernel streaming service
- How I made a heap overflow in curl
- Finding a POP chain on a common Symfony bundle : part 2
- HTTP/2 Rapid Reset: deconstructing the record-breaking attack
- D-Link DAP-X1860: Remote Command Injection
- Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products – Amnesty International Security Lab
- Yet More Unauth Remote Command Execution Vulns in Firewalls

- Bugs
  - Apache HTTP Server /server-status information disclosure
  - Exploring the Upper() Method in Python: Uncovering Vulnerabilities
  - CVE-2023–39308: User Feedback <=1.0.7 — Unauthenticated Stored XSS
  - Hunting for Hidden Treasures: Unveiling the 403 Bypass Bug Bounty Adventure
  - SSTI -Bypassing Single Quotes Filter
  - My First 2 Paid Bugs in the Wonderful World of Bug Bounty
  - How I Found Information Disclosure Just Using Google
  - The Domino Effect: How Multiple Bugs Lead to Account Takeover
  - How can I obtain a $2k bounty solely based on curiosity?
  - I was able to find SQL injection in military website.
  - Sensitive Information Leak via Forgotten .DS_Store File on redacted.com
  - Hacking the government—The attack on GOV.UK domains
  - Exploit CVE-2023–36845-RCE-By CTRL
  - Security report Write-up (CORS) | Logo URL Bypass leads to IP stealing |Bounty—€400
  - Unauthorized Email Address Change Blocks User Account Access—$200
  - NHS—The multitude of Security flaws
  - Account Takeover [Via Host Header Injection]
  - My First Bug for 300$
  - Unauthorized Access to Admin Panel & SQL Injection

- AWS API exposure—What they don't tell you about the wild
- how to dig deep to found a tricky xss via 0auth redirect in blockchain platform and get $700
- How I Uncovered a Stored XSS in octenium.com
- Uncovering Security Vulnerabilities: A Deep Dive into an Eye-Opening Git Discovery
- OTP Bypass through Response Manipulation | A Case of Insecure Design/Implementation; Part 1
- $1120: ATO Bug in Twitter's
- SQL Injection Attack : $$$ Bounty in just an hour.
- Email HTML Injection? How I did it
- Exploring XXE Vulnerabilities in GraphQL APIs
- P1 XSS?
- Multiple Organization Full account Take-over via privilege escalation
- Page admin disclosure via facebook profile link embedded in instagram
- Google Dorking can reward us $$$$
- Account Takeover
- 403 Forbidden? No Problem, Here's a POST XSS
- XSS Steal Cookies
- Critical SQL Injection Vulnerability in Login Page CVE-2023–44970
- Bug Bounty Hunter—Captcha Bypass #Response-to-this-Request
- Beyond Error Messages: Super Admin Deletion due to Broken Access Control (€€€)
- How I Found Information Disclosure as the First Bug
- Privilege escalation lets manager promote the user as admin
- nOAuth: Account Takeover via Microsoft Oauth

- CTF challenges
  - NahamCon CTF23
  - When NTLM Falls: Mastering Kerberos Authentication on Kali: An iCSI CTF
  - Mastering PicoCTF: Your Ultimate Registration Guide!
  - HTB: PC

- Release v1.0.1 · cado-security/cloudgrep · GitHub
- GitHub – ErikWynter/CVE-2023-22515-Scan: Scanner for CVE-2023-22515 – Broken Access Control Vulnerability in Atlassian Confluence
- A web small tool to consolidate the latest publicly listed Bug Bounty programs.
- What is new about AMASS

- How to make great custom wordlists for a large-scope target
- For accessing the environment file
- Tip: Always try GitHub Dorking because it can lead to the discovery of sensitive data leaks, as well as endpoints for vulnerabilities such as SQLi, XSS, and IDOR.
- Misconfiguration issue on one of the target i previously worked Found that it was vulnerable.