Bug Bytes #218 – Advent of Cyber, RCEs and hacking poems

BY TRAVISINTIGRITI · DECEMBER 6, 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 weeks from November 19th to December 3rd

Intigriti News

- Attending Blackhat EU 2023, we're going to be there!
- We're launching our Researcher API- Dec 6 2023
- Top 3 Tools to create your own personalized wordlists to discover more content & find more vulnerabilities
- Few spots left for our next ONSITE Meetup and last of 2023 in our amazing London Offices.
- We've launched the teaser videos for the Knights of Elektron live hacking event, a groundbreaking collaboration between IntelSecurity ProjectCircuitBreaker & Intigriti, volume one and volume two

From my notebook

1. TryHackMe! Advent of Cyber 2023 Kick-Off – Advent of Cyber is a free daily security challenge and walkthrough every day through December in collaboration with a ton of cyber security content creators, but we start off with John Hammond!
2. Where are all the RCEs? RCE case study – Another indepth case study by Bug Bounty Reports Explained, he dives deep into RCEs, I love his data driven approach
3. My Confusion Over Local File Inclusion – This write up is presented as a poem, it's fun and creative
4. Autonomous Hacking of PHP Web Applications at the Bytecode Level – Very interesting unique look at PHP by looking at the Bytecode
5. Episode 403 – Does the government banning apps work? – No but it does prompt an interesting discussion around threat modelling!

Videos 

- Hacking when all the bugs have been found?
- Hacking PyJWT for Algorithm Confusion Attack [HackTheBox CyberMonday]
- Building YOUR CyberSecurity Resume
- Can ChatGPT Find Smart Contract Vulnerabilities
- A Random $10,000 bug #bugbounty #bugbountytips #bugbountyhunter (shorts)
- What is a Container Escape? (shorts)
- Time spent on a target feat. @rhynorater #bugbounty #bugbountytips #bugbountyhunter (shorts)
- Monitoring JS files to know first about new features feat. @rhynorater #bugbounty #bugbountytips (shorts)
- Testing e-commerce? Here's what to look for (shorts)
- Giving Yourself the Best Opportunity to Find a Bug
- Setting Up My Home Lab For Docker OR Kubernetes!
- Everything about full-time bug bounty – Justin "rhynorater" Gardner from @criticalthinkingpodcast
- Reinventing Web Security
- Bug Bounty Target Deep Dive

Podcasts

- At 17, He Made $10K a Month Printing Fake IDs, But Paid a Much Higher Price Ep. 104: Arya
- Katie Paxton-Fear: The Importance of Content Creation in Cybersecurity Careers
- The SAML Ramble (Ep. 46)

- The Secret Message Hackers Left Deep Inside Their Malware Darknet Diaries Ep. 103: Cloud Hopper
- Maxie Reynolds: From hacker to underwater data center entrepeneur
- Episode 47: CSP Research, Iframe Hopping, and Client-side Shenanigans
- 228 – Hypervisor Bugs and a FAR-out iOS bug
- 227 – Kubernetes Code Exec and There Is No Spoon
- EP150 Taming the AI Beast: Threat Modeling for Modern AI Systems with Gary McGraw
- Ransomware gang reports its own crime, and what happened at OpenAI?
- 226 – A Heap of Linux Bugs

- Beginner
  - Part 03 | What To Do After Choosing a Target? | Post Recon |Bug Bounty
  - Easy Bug Hunting: HTML Injection Explained Step by Step
  - Subdomain Enumeration
  - The Bug Hunter's Methodology Live Course Review
  - 5 thing most new bug bounty hunters do wrong
- Intermediate
  - Everything I know on Recon
  - Remote Code Execution (RCE)
  - Mastering API Penetration Testing: A Comprehensive Guide for Security Pentesters
  - XSS – Weaponization ATO
  - Understanding XML External Entity (XXE) Vulnerabilities
  - CSRF Bug Hunting Methodology: Intermediate
  - A Thrilling Expedition into AWS Security
  - Semi-Automating IDORs: A Practical Approach to Working Smarter, Not Harder
  - Epic Bug Hunting Failures-2
  - Vulnerabilities in Python Serialization: Pickle
- Advanced

- HTTP/2 Request Smuggling
- Dive into Single Packet Attack
- Mass Hunting XSS vulnerabilities

- Security Research
  - Gadget chain in WordPress
  - Building Immune Authorization: AppSec in Healthcare Apps
  - Using Chaos Engineering To Hack An API
- Bugs
  - My First Valid Bug!!!
  - Business Logic Vulnerability: Payment bypass
  - The story of how I finally got my first money from hacking
  - How I Found My First Website Vulnerability as a Web Pentester
  - My first and simple ATO in a private program
  - Verification Bypass via “Mass Assignment”
  - Race Condition – A cURL Chaos
  - Fat GET Authorization Bypass
  - CRLF to XSS
  - PII Disclosure Worth $750
  - Hall of Fame at NASA
  - Writeup Bugcrowd—Private program—QR codes
  - Default Credentials, P1 with $$$$ Reward in a Bug Bounty Program
  - Waybackurls leads to pwned Admin Panel
  - How i get my first Logic Bug and how to find them
  - Critical misconfiguration in Firebase-Bug bounty
  - $20,000 Paid For A Bug That No One Has Ever Expected
  - First massive bug: Noise’s AWS Bucket Misconfiguration
  - How I Made $$$ Using Open-Redirect

    - How i hacked a router (embedded system)
    - SAML authentication bypass leads to account takeover
    - Google dorking is one of the best method | Hall of fame from XXX.gov
    - 200$ bounty for CRLF injection Attack
    - How I found a vulnerability in a Trillion Dollar Company, Amazon!
    - CRITICAL BUG Alert: How I HACKED into a company's DATABASE
    - CVE-2023–47837: ARMember ≤= 4.0.10 — Bypass Membership Plan
    - Chaining CORS by Reflected XSS to Steal Sensitive Data
    - Vulnerability Exploiting Privilege Escalation Discovered in WordPress [CVE-2023–32243]
    - Budget Change: IDOR 1000$ Bug
- CTF challenges
    - HackTheBox – CyberMonday
    - HTB: CyberMonday
    - Capture the Flag: Hacking Yet Another Markup Language
    - HackTheBox – Pilgrimage
    - VulnLab — SQLi Injection series — Bypass Login
    - HackTheBox — Web Attacks: XXE with Blind Exfiltration Data, HackTheBox — Web Attacks: Error Based XXE to exfiltrate data, HackTheBox — Web Attacks: From XXE Injection to Advanced Local File Disclosure

- Porch-Pirate – The Most Comprehensive Postman Recon / OSINT Client And Framework That Facilitates The Automated Discovery And Exploitation Of API Endpoints And Secrets Committed To Workspaces, Collections, Requests, Users And Teams
- Pentest Muse: an Open Source AI-Powered Tool for Ethical Hacking
- @pdiscoveryio's Katana for Bug Bounty.