Bug Bytes #217 – how to submit vulnerabilities, writing a great writeup and 2 years of bug bounty

BY TRAVISINTIGRITI · NOVEMBER 22, 2023 · LAST UPDATED ON JULY 14, 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 6th to November 19th

Intigriti News

- Check out the interview with @eckert_madeline from @Microsoft explaining the importance & differences between #BugBounty & #VDP, and how you can partner with them!
- Were you one of the 10 teams who solved the #1337UPLIVE game hacking challenge, "Dark Secrets"? If not, here's a walkthrough from @_CryptoCat
- The #1337UPLIVE 2023 CTF is OVER!! Massive congratulations to the winning teams
- Intigriti's October Challenge is over!!

From my notebook

1. where do you ACTUALLY submit vulnerabilities?
2. Dan Rearden | The Write-Ups & Downs To Making A Great Write-Up | Simply Cyber Con 23
3. Bug bounty: year 2 – 0days, a $20k bounty and... laziness – bounty vlog #5
4. Easy $500 Vulnerabilities! // How To Bug Bounty
5. Biden's 8 Rules for AI Usage & What it Means For You

- Potential vulnerability in AI chatbots feat. @rez0 #bugbounty #bugbountytips #bugbountyhunter (shorts)

- Watch out for API use theft when implementing AI chatbots feat. @rez0 #bugbounty #bugbountytips (shorts)
- Wow! Sam Altman fired from OpenAI! #ai #chatgpt (shorts)
- How to Use DOM Invader in 2023
- How to monetise a scalable 0day in bug bounty? #bugbounty #bugbountytips #bugbountyhunter (shorts)
- What are clients REALLY asking? | Soft Skills for Hackers
- NoSQLi Tutorial Using PortSwigger (with labs)
- $3,200 client-side DoS in PayPal #bugbounty #bugbountytips #bugbountyhunter (shorts)
- What types of DoS bugs will get you a bounty? Case study of 138 DoS bug bounty reports
- Another Cisco 0-day discovered #cybersecurity #cisco (shorts)
- Getting Started with CTF's
- Bug Bounty Stories: HACKING REDBULL again! (Tomcat + Jolokia Walkthrough)

- The OG Bug Bounty King – Frans Rosen (Ep. 45)
- URL Parsing & Auth Bypass Magic (Ep. 44)
- It Wasn't Easy to Print $250 Million of Counterfeit Cash Darknet Diaries Ep. 102: Money Maker
- Phillip Wylie Show with Olivia Gallucci
- One Click, $9 Million In Student Debt Erased Darknet Diaries Ep. 139: D3f4ult
- Why Was Puerto Rico's Lottery Leaking Millions of Dollars a Month? Darknet Diaries Ep 101: Lotería

- Beginner

- Master JSON in 8 Minutes
- Access control vulnerabilities
- Let's together dive deep into information disclosure
- Broken Access Control and Privilege Escalation: What You Need to Know

- Intermediate
  - OpenCart Static Code Injection in common/security.admin
  - Hacking Microsoft IIS : Enumerating IIS for V
  - AppSec Tales XXIII | XPathI
  - How to find vulnerabilities in a web page in 10 minutes
  - How I Automatically Generate XSS Payload & Automate Reflected XSS
  - #4 Session Fixation—Secure Code Explain
  - What is Kerberoasting?? How it works
  - A Pentester's Approach to Kubernetes Security—Part 1

- Advanced
  - Exploiting Blind XXE: Going Out of Band
  - Exploiting Parallels Plesk Panels With Shodan
  - Unveiling Sensitive Information Exposure: IIS Tilde Enumeration Vulnerability
  - Janus Vulnerability (CVE-2017–13156)
  - Escalating Blind SSRF to a Remote Code Execution
  - Akamai Bypass! Advanced XSS.
  - Decoding Advanced XSS Payload Chaining Tactics

- Security Research
  - Process stomping and loading beacon with sRDI
  - Building a free Burp Collaborator with Cloudflare Workers
  - Visual Studio Code Security: Markdown Vulnerabilities in Third-Party Extensions (2/3)
  - Plundering Postman with Porch Pirate

- protectai/ai-exploits: A collection of real world AI/ML exploits for responsibly disclosed vulnerabilities
- I analyzed stackoverflow
- CrushFTP – CVE-2023-43177 – Unauthenticated Root-Level RCE Chain
- Accessing Azure Kubernetes Service as Guest and Cross-Tenant
- Escaping the sandbox: A bug that speaks for itself
- Static Code Injections in OpenCart (CVE-2023-47444)
- Tapping into a telecommunications company's office cameras
- Denial of Pleasure: Attacking Unusual BLE Targets with a Flipper Zero
- When An AOL Coder Sold the Whole Database
- From Akamai to F5 to NTLM... with love.
- Android Kitchen Sink: Send BLE spam to iOS, Android and Windows at once using Android app
- Our Pwn2Own journey against time and randomness (part 2)
- 50 Shades of Vulnerabilities: Uncovering Flaws in Open-Source Vulnerability Disclosures
- Visual Studio Code Security: Deep Dive into Your Favorite Editor (1/3)
- PRTG Remote Code Execution
- Post-exploiting a compromised etcd – Full control over the cluster and its nodes
- Your printer is not your printer ! – Hacking Printers at Pwn2Own Part II

- Bugs
  - Privilege Escalation: Unauthorized Low-Privilege Users Creating Feature Bundles
  - Default Credentials, P1 with $$$$ Reward in a Bug Bounty Program
  - OAuth Misconfiguration Leads To Pre-Account Takeover(snapchat)
  - $1000 Bounty: How I scaled a Self-Redirect to an XSS in a web 3.0 system at Hackenproof
  - How I got a $500 reward for finding an unacclaimed bucket on GitHub
  - Riding the Waves of API Versioning: Unmasking a Stored XSS Vulnerability, CSP Bypass Using YouTube...
  - Easy Admin Access—RVDP
  - How I hacked Google's bug tracking system itself for $15,600 in bounties
  - Idor That allowed me to get access to sensitive users files and share them
  - SSRF – access to ssh keys
  - Google VRP -[IDOR] Deleted Victim Data & Leaked
  - 1200$ IDOR Flaw: Allow Attacker To Approve Project Time Tracking
  - I created posts on the newsletter page dedicated to the program administrator
  - Subdomain takeover and Text injection on a 404 error page-$100 bounty

- Unlocking Cash: Easy P1 Bug in Grafana Dashboard with Default Credentials = €€€€
- Dutch T-Shirts for Dutch Hacks: A Tale of Four Vulnerabilities!!
- Bypassing 2FA for Password Reset : By Request Manipulation 500$ Bug
- Race Conditions with pipelining
- Breaking Barriers: Unmasking the Easy Password Validation Bypass in Security Key Registration
- $1800 Bounty: Exploiting Unpredictable Data that Leads to All Users PII Exposure in an IDOR
- How I was able to find BAC on the University website leading to result dumping?
- CRITICAL BUG Alert: How I HACKED into a company's DATABASE
- Cloudflare Bypass leads to RXSS[Reflected-Cross Site Scripting] in Microsoft
- LFI to RCE—Bug bounty
- How I sent multiple payment requests on PhonePe, Paytm, and Google Pay
- Discovering and Exploiting a XML External Entity (XXE) Vulnerability in a Public Bug Bounty Program

- CTF challenges
  - HackTheBox – Sandworm
  - HTB: Sandworm
  - Exploring a Flask App with SSTI [HackTheBox Sandworm]
  - Post IR Investigation – MoveIT Exploit – HTB Sherlocks – I Like To
  - HackTheBox – Download
  - HackTheBox – Broker
  - HTB: Broker
  - SSTI bypass using CRLF (1337 UP CTF—Smarty Pants)
  - GraphQL Misconfiguration Leads to Unlimited Money Transfer (Intigriti CTF—Bug Bank)
  - JWT Intrigue: Hidden Keys within Web Applications
  - Har Har Hijack: The Okta Plunder
  - TickTock Intrusion: The Timing Attack Challenge
  - Huntress CTF 2023—Write-up
  - Jupiter | HTB | Grafana | raw SQL Query | Shadow Simulator RCE | Sattrack

- Goblob – A Fast Enumeration Tool For Publicly Exposed Azure Storage Blobs
- Forbidden-Buster – A Tool Designed To Automate Various Techniques In Order To Bypass HTTP 401 And 403 Response Codes And Gain Access To Unauthorized Areas In The System
- Afuzz – Automated Web Path Fuzzing Tool For The Bug Bounty Projects
- SSL Search—A tool to identify infrastructure and discover attack surfaces.