Bug Bytes #188 – Hello 2023!

BY TRAVISINTIGRITI · JANUARY 3, 2023 · LAST UPDATED ON MARCH 6, 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 December 26th until January 1st.

CLICK HERE TO SUBSCRIBE

Intigriti News

- Code review challenge and the solution
- We welcome the new year
- Please follow us on Twitter

From my notebook

Happy 2023! As hackers around the world rang in the new year we saw many recap their 2022 or look towards 2023 with new goals. With that in mind I've brought together some resources on the theme of learning new skills in the new year, for me I really want to develop new technical skills, at are you looking to learn in 2023?

1. Chrome Browser Exploitation Part 1, Part 2 and Part 3
2. JNDI Injection Series: RMI Vector—1, JNDI Injection Series: RMI Vector—Dynamic Class Loading From Remote URL
3. Turning Google smart speakers into wiretaps for $100k
4. Difficulty of Reproducing Old Exploits and Difficulty of Reproducing Old Exploits (Part Two)
5. Corben shares his favourite hacking stories

Other Amazing Things

- SSRF Hacking With Yuvraj | Hacker2Hacker | SSRF
- How To Bypass Website File Upload Restrictions
- The Ultimate Sock Puppets Guide for OSINT
- Can ChatGPT Solve Cyber Capture The Flag Puzzles? (Live Event Testing)
- How Alissa Knight is Taking Cybersecurity To The Next Level
- How to Proxy Command Execution: "Living Off The Land" Hacks
- LFI to RCE using PHP Filters!
- Pivoting into Internal network – SSHUTTLE
- Computer Networking (Deepdive)
- How I scale my containerized bug bounty automation! (Automation Series)
- ChatGPT for Security Researchers
- Web3 Security Learning Resources

- How Netflix Learned Cloud Security [ML B-Side]
- 131: Welcome to Video
- Episode 356 – LastPass ducked up, now what?

- Rhynorater and 0xteknogeek start a bug bounty podcast
- More tools added to offsec.tools
- What advice would you give your younger self about cyber security
- MrTuxracer's Bug Bounty recap, mcipekci's recap, harshbothra reviews his educational resources and another from haxor31337

- Why isn't bug bounty like esports
- Best bug found in 2022?, what type of bugs did you find in 2022 and what is going to be big in 2023
- The Mind Behind Nuclei, Demo w/ Sandeep Singh Jan 11

- Endpoint Security: The Protection Mechanism of Web Application and Networks
- Understanding Memcache Injection
- Bug Bounty Recon: Content Discovery (Efficiency pays $)
- How to test for JWT attacks?
- XXE (XML EXTERNAL ENTITY) Injection
- Efficient methodology to get P2 level – subdomain takeover vulnerability
- The Big Danger With Laravel (.env file)
- Out Of Band Command Injection
- Hacking Basics
- How I Design My Prefect Bug Bounty Automation (1), How I Design My Prefect Bug Bounty Automation(2) and How I Design My Prefect Bug Bounty Automation(3)
- !00 Complex terms related to Bug Bounty Explained for a Newbie
- how to have an effective recon?
- Exploiting XSS with Javascript/JPEG Polyglot
- Setting up your bug bounty scripts with Python and Bash
- Navigating the World of Directory Traversal
- Cypher Injection Cheat Sheet
- Spice up your persistence: loading PHP extensions from memory

- Diving into an Old Exploit Chain and Discovering 3 new SIP-Bypass Vulnerabilities
- CSRF: The Silent Web Attack
- Tautulli 2.1.9 version; Cross-Site Request Forgery (ShutDown) and Denial of Service (Metasploit)
- Stored XSS vulnerability in Microsoft booking
- LDAP anonymous login story of my 3 simple P3 findings in DHS
- How I Earned My First Bug Bounty Reward of $1000
- Unauthorized Sign-up on Subdomain of Subdomain leading to Organization takeover worth $2000
- How Capabilities actually Work ? | Exploitation | Privilege Escalation
- $350 XSS in 15 minutes
- How I got a Bug At Apple that lead's to takeover accounts of any user who view my profile
- Account Takeover Due to Cognito Misconfiguration Earns Me €xxxx
- OSINT Case Study: Validating a website if its fraud or legit
- CVE-2022-38627: A journey through SQLite Injection to compromise the whole enterprise building
- $500 in 5 minutes
- My report on how the admin panel took over and I got X, $500 bounty from my report Hello hackers,

- clif – Application fuzzer wfuzz/ffuf for applications
- SubOver – A Powerful Subdomain Takeover Tool

- Autowasp – Burp Suite extension that integrates Burp issues logging, with OWASP Web Security Testing Guide (WSTG)
- Understanding the Scapy Module: Its Use in Cyber Security
- Understanding the NumPy Module: Its Use in Cyber Security

- Read the documentation!
- ramsexy's goals have been the same since 2020: Being happy and having fun
- Unsafe logger for code injection
- Default passwords oops
- nuclei scan tip
- BlindXSS made easy with this chrome extension
- log4shell is still a problem

- Advent of Cyber 2022 [Day 1—Day 24] All Challenges Walkthrough and Writeups with Answers
- DOM XSS Using Web Messages (Practioner)—Portswigger Lab 1 | Solution and Approach
- Safe Opener—Reverse Engineering | PicoCTF 2022 Writeup
- OWASAP juice shop lab setup
- Compromising a vulnerable GCP, INE-Labs GCPGoat walkthrough. Part-1 / Compromising a vulnerable GCP, INE-Labs GCPGoat walkthrough. Part-2

Bug bounty/Pentest news 

- LastPass Breach
- Cyber attacks set to become ‘uninsurable’, says Zurich chief