Bug Bytes #191 – Heaps of Bugs

BY TRAVISINTIGRITI • JANUARY 25, 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 January 16th to January 22nd

CLICK HERE TO SUBSCRIBE

Intigriti News

- IDOR in 100 seconds
- This week's code review challenge and the solution
- XSS challenge
- We posted a new video on SQL injection

From my notebook

1. Chopin's Series on heap exploitation and memory
    - The toddler's introduction to Dynamic Memory Allocation
    - The toddler's introduction to Heap exploitation (Part 1)
    - The toddler's introduction to Heap exploitation (Part 2)
    - The toddler's introduction to Heap exploitation—Overflows(Part 3)
    - The toddler's introduction to Heap exploitation, Use After Free & Double free (Part 4)
    - The toddler's introduction to Heap Exploitation, FastBin Dup Consolidate (Part 4.2)
    - The toddler's introduction to Heap Exploitation, Unsafe Unlink(Part 4.3)
    - The toddler's introduction to Heap Exploitation, House of Spirit(Part 4.4)
    - The toddler's introduction to Heap Exploitation, House of Lore(Part 4.5)
2. Top 10 bugs found in C# projects in 2022
3. Microsoft bug reports lead to ranking on Microsoft MSRC Quarterly Leaderboard (Q3 2022)
4. Caido is now in public beta
5. Learn to build it, then break it

- Hacking a Car's License Plates...
- Top 3 Burp Suite Plugins for a More Collaborative Workflow
- TCP For Hackers: The Basics!
- Web Hacking Challenges EXPLAINED | with PinkDraconian
- Head in the Clouds | Cloud Hacking with panawesome
- Prototype Pollution in 60 Seconds
- Launch your cybersecurity career: IppSec's advice
- Lost 50 lakhs with sim swapping attack!
- Finding IDORs with CODE REVIEWS!
- The Billion Dollar Vulnerability Forcing a Major Fork On The Ethere...
- How to Be An Ethical Hacker: 2023 Edition
- LevelUpX – Series 14: Finding and Exploiting Hidden Functionality
- Is Subdomain Bruteforcing Worth It?!

- 179 – Client-Side Path Traversal and Hiding Your Entitlement(s)
- 180 – An iPod Nano Bug, XNU Vuln, and a WebKit UAF
- Risky Biz News: Google Search and Ads have a major malware problem
- Srsly Risky Biz: LockBit ripe for disruption, Russians throw kitchen sink at Ukraine

- found a pre-auth xss 0day today that affects over 5M hosts on the internet lol
- True greatness lies not in the attainment of knowledge, but in the eternal pursuit of it.
- Wanna collab?
- Jack Cable joins CISA
- Triaging in a single image
- CAIDO public beta

- Migration Assistant killed my terminal
- Firestore Security Testing Guide—Go Beyond *.firebaseio.com/.json
- LDAP PassBack Attacks, the docker way
- Tips for BAC and IDOR Vulnerabilities
- SSTI: The Hidden Threat to Web Application Security
- Setting up Playwright & VSCode for hacking headless browsers
- Bug Hunting 101: Multi-Factor Authentication OTP Bypass
- How to Find Compromised Credentials on Darkweb?
- Software Development Lifecycle (SDLC), DevSecOps, SAST, DAST And IAST Concepts
- Easy XSSHunter Discord Alerts
- MySQL LOAD_FILE() and INTO OUTFILE() Sql Injection
- Fuzz open source for potential bounties
- Password Cracking Technique used by Blackhat Hackers
- Privilege Escalation Attacks

- Top 10 smart contract vulnerabilities on Ethereum
- Blog 07: Misc—JSON Web Token(JWT)
- HTTP Request Smuggling—Basic CL.TE vulnerability

- Account Take Over Due To AWS Cognito Misconfiguration
- Hacking into (RCE) Government Server operated for the US Department of Energy's National Nuclear Security Administration.
- How I found 130+ Sub-domain Takeover vulnerabilities using Nuclei
- Another major flaw this time in the TransUnion that allows bypassing security by Jenya Kushnir
- OTP Leaking Through Cookie Leads to Account Takeover
- DOMAIN ADMIN Compromise in 3 HOURS | by Ignatius Michael | bug bounty
- DOM-Based XSS for fun and profit $$$! | Bug Bounty POC
- From Error_Log File(P4) To Company Account Takeover(P1) and Unauthorized Actions On API
- Full Team Takeover
- How I passed the AWS security specialty certification in 2023
- How I identified and reported vulnerabilities in Oracle and the rewards of responsible...
- How I found 40+ Directory Listing Vulnerabilities of Source Code Disclosure via Exposed WordPress
- API Misconfiguration – No Swag of SwaggerUI
- The easiest way I used to bypass an admin panel
- How I was able to hack into anyone's account on an Institute Portal
- Two Factor Authentication Bypass On Facebook
- CSRF + Stored XSS to Leading to Full Account Takeover
- Exploitation of CVE-2022–21500: Oracle E-Business Login Panel

- Reflected XSS Leads to 3,000$ Bug Bounty Rewards from Microsoft Forms
- Forget SQL Injection Have you Heard of Jwt Injections?
- How I found XSS on Admin Page without login!
- How i was able to get critical bug on google by get full access on [Google Cloud BI Hackathon]
- Bypass Facebook locked profiles Post/Information

- PimpMyBurp #7: How HaE Burp Suite extension can help you in your daily hunting session
- Hacking with cURL: Unleash the CLI beast
- Weaponised XSS Payloads – XSS payloads designed to turn alert(1) into P1.
- CyberChef – A web app for encryption, encoding, compression and data analysis.
- MagicRecon – A powerful shell script to maximize the recon and data collection process.
- LeakLooker-X – Discover, browse and monitor database/source code leaks.

- Broken Authentication and Session Management
- Creating your own tools to hunt bugs, a power often neglected
- Easy information disclosure P4
- Godfather Orwa's tips
- The best way to succeed in bounties and research is knowing the tech
- Increase the RAM allocated to Burp Suite
- Fingerprinting what tech stack a bug bounty target is using

- Create a privilege matrix

- Manipulating the WebSocket handshake to exploit vulnerabilities
- eLFI already solved it, better get going #BUGCROWD Challenge Walkthrough
- Learning Web-Sec – Day 13 – Authentication Vulnerabilities
- JWT authentication bypass via unverified signature—Portswigger Simple Solution Writeup | 2023
- Cross-site WebSocket hijacking
- Hack File Inclusion in DVWA: A Full Walkthrough
- Easy Peasy-TryHackMe-Writeup
- Basic server-side template injection (code context) | 2023
- HTB: UpDown
- Simple Web Challenge on HTB | Templated