Bug Bytes #210 – Zenbleed, Interview Questions, Challenge Coins and SQL Injections

BY TRAVISINTIGRITI · SEPTEMBER 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 week from August 28th – September 3rd

Intigriti News

- Oda has just launched their public bug bounty program paying up to €4,000 for valid vulnerabilities!
- What's the first payload you try to test for SSTI
- What payload would work in the following vulnerable code snippet?
- Do you want to start bug bounty, but struggle to find the right program to hack on?
- Intigriti's August Challenge is over!
- 3 Labs to practice SQL Injections

From my notebook

1. Zenbleed (CVE-2023-20593)
2. Fake bug bounty writeup exposed (shorts)
3. Web AppSec Interview Questions
4. Initgriti Challenge Coin BSidesLV/DefCon 2023
5. Getting into AWS cloud security research as a n00bcake

- Turning SQL injection in MySQL into file read (shorts)
- Your Computer is For Sale on the Dark Web
- The FBI Disrupted a HUGE Malware Strain
- How to turn an SQL injection into an RCE? (shorts)
- how do you ACTUALLY find a computer's location?
- It's Okay to Take a Break From it All
- $30,000 blind SQL injection chained with blind XSS (shorts)
- Trick Hackers with a Fake User
- Balancing Bytes and Well-Being: Navigating the World of Young Hackers
- Its Okay to Quit
- Local SQL injection in Zoom allowed to spy on people (shorts)
- HackTheBox – MonitorsTwo
- NahamCon CTF 2023 – Museum (Medium) Walkthrough
- Ligolo-ng: Pivoting Your Way Through Complex Networks!
- Hacker vs Program Manager – $50 is NOT enough for a retest, especially when 1 week+ has passed... (shorts)
- Hacker vs Program Manager – Should 0-Days get paid? (shorts)
- Exploit Blind SSRF with Out-of-Band Detection
- Bug Bounty: 9 Tips to Writing Good Bug Bounty Reports
- Chat w/ Charlie Eriksen, Creator of Jswzl! (Bug Bounty, Cyber, Automation, etc.)

- DEFCON 31
  - DEF CON 31 – Demystifying (& Bypassing) macOS's Background Task
  - DEF CON 31 – SODA Machine with DualD
  - DEF CON 31 – The Internals of Veilid

- Episode 34: Program vs Hacker Debate
- Srsly Risky Biz: The UK snoopers' charter won't stop security patches
- SN 937: The Man in the Middle – WinRAR v6.23, fake flash drives, Voyager2 antenna, Google Topics
- The Power of Community: A Conversation with Kevin Johnson
- No. 396 – Elon's Doxxing FSD, ATHI AI Threat Modeling Framework, Cardboard Drones, and GPT Enterprise
- Encore: cross-site scripting (noun) [Word Notes]
- EP136 Next 2023 Special: Building AI-powered Security Tools – How We Do It?

- Beginner
  - S3 Bucket Recon
  - Still exists! Subdomain takeover via surge.sh
  - Enhancing Bug Bounty Workflow with Advanced Google Dorks
  - Bug Bounty—Hacking with Subfinder the Right Way
  - GitHub Dorks: Simplified
  - Unraveling the IDOR Vulnerability: A Comprehensive Guide to Understanding and Testing
  - How does Kerberos work – an introduction for beginner.
- Intermediate
  - Exploit Analysis: Request-Baskets v1.2.1 Server-side Request Forgery (SSRF)
  - Exploring Server-Side Request Forgery (SSRF) within WordPress
  - How to Exploit a WordPress Plugin Vulnerability: A Case Study of TheCartPress
  - Defending AWS Assets through Email alerts.
  - Reverse Engineering: Injection Series Part 4—Blue Team Labs
  - What is GraphQL?

    - How to connect wazuh and discord: a Step-By-Step Guide.
- Advanced
    - Creating the perfect bug bounty automation
    - Machine Learning Vulnerabilities
    - Mastering Ffuf: Basic and Advanced Commands
    - Extending Burp Suite for fun and profit – The Montoya way – Part 4 – hn security

- Security Research
    - Spraying the Microsoft Cloud
    - WinRAR RCE CVE-2023-38831 Zeroday Latest
    - Leaking File Contents with a Blind File Oracle in Flarum
    - GDB Baby Step 4: Decoding Multiplication in Assembly with GDB — StackZero
    - Decoding the Enigma: A Journey into Minesweeper's Reverse Engineering
    - Navigating Uncharted Waters: The Cybersecurity Implications of Maritime Vessel Hacking
    - Unlocking Potential: Exploring Frida & Objection on Non-Jailbroken Devices without Application
    - Game Hacking: Hex Editing Save Files for Unlimited Cash
    - SSD Advisory – File History Service (fhsvc.dll) Elevation of Privilege – SSD Secure Disclosure
    - Secure FastAPI with eBPF
    - Introducing Session Hijacking Visual Exploitation (SHVE): An Innovative Open-Source Tool for XSS Exploitation · Doyensec's Blog
    - Mashing Enter to bypass full disk encryption with TPM, Clevis, dracut and systemd
    - Unpinnable Actions: How Malicious Code Can Sneak into Your GitHub Actions Workflows
    - Converting Tokens to Session Cookies for Outlook Web Application
    - Contain Yourself: Staying Undetected Using the Windows Container Isolation Framework
    - Analysis of Obfuscations Found in Apple FairPlay
    - Diving into Starlink's User Terminal Firmware
    - Thousands of Organizations Vulnerable to Subdomain Hijacking

    - Google Cloud Functions are Secure, only if you know how to use them!
- Bugs
    - A Year of Hunting into Vulnerability Disclosure programs (VDPs)
    - Bypass WAF by a simple trick gained $1000 bounty
    - RCE on Tracking Application's Admin panel
    - Webinar Pro or Not: The $500 Access Control Bug
    - Lenskart Data Leak: Unveiling Critical Security Breach in Spring Boot Configuration
    - How to install Foundry to debug smart contracts
    - Exposing Critical Vulnerabilities in Grafana
    - Real World Bug Hunting: Information Disclosure in Error Messages
    - Host Header Injection / Redirect on Spotify—Bounty $200
    - Ability to delete other user's companies
    - The story of how I was added to the Microsoft Hall of Fame
    - How I was able to find the P4 vulnerability in the United States Department of Agriculture by phone.
    - $100 under 1 hour: Subdomain takeover via firstpromoter.com
    - how I was able to find information disclosed by reading my old report and understanding the website
    - Ability to Deny Subaccounts feature for all users
    - Exploiting Maltrail v0.53—Unauthenticated Remote Code Execution (RCE)
    - How I could view any Facebook Groups Notes media, and they paid me a $10,000
    - From P4 to P3 using one additional step
    - I was able to see all user information by manipulating parameters on the website.
    - How I was able to modify and delete any user's data file (filestack API)
    - PII at Your Fingertips: How I Stumbled Upon an Easy-to-Find Data Leakage Vulnerability @ Swisscom
    - rate-limit Bypass led to 2FA Bypass using brute-force
    - Exploring the User Registration & Login and User Management System v3.0 SQL Injection Exploit
    - Finding Reflected XSS + WAF Bypass As My first Bug!
    - Account takeover hidden in Javascript files plus some extra work? my type.
    - Series of Web Exploits: From Discovery to Disclosure—XSS fun
    - Uncovering Vulnerabilities: Security Flaws Discovered on the Indian Prime Minister's Website
- CTF challenges
    - Zipping (Intended + unintended way)— HackTheBox Medium machine—By Amdjed Zerrougu

- HTB: MonitorsTwo
- Authentication Bypass TryHackMe Write-Up
- Mailroom HTB | Gitea | XSS | NoSqli | RCE | Exploit Development | Strace
- Devel writeup | Hack the box

- r3volved/CVEAggregate: Build a CVE library with aggregated CISA, EPSS and CVSS data
- What Are They and How Do They Work · HotCakeX/Harden-Windows-Security Wiki
- Snawoot/dtlspipe: Generic DTLS wrapper for UDP sessions
- Noir – An Attack Surface Detector Form Source Code
- DNSWatch – DNS Traffic Sniffer and Analyzer
- Poastal – The Email OSINT Tool
- Tiny_Tracer – A Pin Tool For Tracing API Calls Etc

- You've heard of SSRF. You've heard of IDOR. But have you heard of SSRDOR?
- Exploited a tricky XSS yesterday
- Exploiting the unexploitable with lesser known browser tricks
- FYI, if you're testing for SQL injection against apps using MySQL (and its variants), be wary of these injections:
- Just popped another crazy XSS. Check this one out
- If you use the command line tool "llm" by@simonw, this is fun 1-liner
- 10 tips for crushing bug bounties

- Stop Studying Hacking