Bug Bytes #216 – SQL injections, Android XSS and Writing Quality Reports

BY TRAVISINTIGRITI · NOVEMBER 2, 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 October 23rd to October 29th

Intigriti News

- XSS Challenge is currently down but stay tuned for updates
- What's the least helpful advice that someone can get when starting out in bug bounty?
- Top 3 tools for automating SSRF vulnerabilities!
- Attention Belgium! Join us at our Open Port event on 2nd November! Get free swag, free food tour Intigriti's Antwerp HQ, meet and collaborate with other hackers! Wether you're beginner, intermediate or advanced level, all are welcome at the open port event

From my notebook

1. Automating Boolean SQL Injection and Evading Filters
2. Execution of Arbitrary JavaScript in Android Application
3. Cisco IOS XE CVE-2023-20198 and CVE-2023-20273: WebUI Internals, Patch Diffs, and Theory Crafting
4. Best Practices for Writing Quality Vulnerability Reports
5. How I Hacked 1000 + Tesla Cars using OSINT

- The Russian cyberattack that crippled Ukraine
- HackTheBox – Gofer & Binary Analysis of notes [HackTheBox Gofer]

- How to Use Docker in 2023
- Hacking with Haiku Part 3
- Cloud Security with Microsoft 365 Developer Tenants
- The Beginner's Guide to Blind XSS (Cross-Site Scripting)
- Did the World Bank's servers get breached?
- AWS Security Hub: Getting Started & Practical Demo
- Thousands of remote IT workers discovered to be North Korean Spies
- RagnarLocker Ransomware Seized by Law Enforcement
- Password Managers and Secure Passwords
- Let's Hack Together! Follow Along Livestream w/ Gerald Auger, PhD
- STRIDE Threat Modeling for Beginners – In 20 Minutes

- Renniepak Interview & Intigriti LHE Recap (Ep. 42)
- @Shenetworks: Leveraging Content Creation to Build a Career in Cybersecurity
- They Hired Him to Snoop a Target, but Something Felt Very Wrong Darknet Diaries Ep. 99: The Spy
- Cloud Security Tools from Cloud Pentest Lab | DeRF |Stratus Red Team
- EP149 Cloud Security: Shared Responsibility, Shared Fate, Shared Faith?
- Cyber sloppiness, and why does Google really want to hide your IP address?
- SN 945: The Power of Privilege – New cURL vulnerabilities, CVSS 10.0 Cisco Nightmare, So long VBScript!
- Risky Business #726 — Okta owned while Cisco takes a massive L
- 220 – Windows Kernel Bugs, Safari Integer Underflow, and CONSTIFY

- Beginner
  - Simple Tips for Bug Bounty Beginners: Finding Open Redirect Bugs
  - Looking for Broken Access Control Vulnerabilities in websites
  - What To Do After Choosing a Target? Part 01 | Bug Bounty
  - Mastering SQL Injection on DVWA Low Security with Burp Suite: A Comprehensive Guide— StackZero
  - How to Crack Windows Passwords with John the Ripper
  - A Guide to LFI Discovery: Uncover Vulnerabilities and Enhance Web Security | Bug bounty
- Intermediate
  - On Path Attacks: File Transfer Capture with Ettercap and Wireshark
  - Broken Object Level Authorization Vs. Broken Functionality Level Authorization | API Hacking |
  - Reverse SSH SOCKS proxy via Alpine image
  - Delving into the Depths of NoSQL Injection: A Research Odyssey
  - Bypass Android Applications Debug and Root Detection via debugger.
  - Bug Hunting: An Extension that Makes the Job Easier
  - Exploring Host Header Vulnerabilities with headi
- Advanced
  - EC2 User-data to RCE
  - Akamai Bypass! Advanced XSS
  - Secure Code Review #1: Basics (Getting Started)
  - Unleashing Memcached: The Double-Edged Sword of Speed and Vulnerability

- Security Research

    - 3 new NGINX ingress controller Kubernetes related vulnerabilities
    - Compromising F5 BIGIP with Request Smuggling
    - Threat Hunting: Detecting Browser Credential Stealing [T1555.003]
    - Citrix Bleed: Leaking Session Tokens with CVE-2023-4966
    - RCE in Progress WS_FTP Ad Hoc via IIS HTTP Modules (CVE-2023-40044)
    - CVE-2023-33466 – Exploiting Healthcare Servers with Polyglot Files
    - CVE-2021-27198
- Bugs
    - A Quick Price Manipulation
    - $1120: ATO Bug in Twitter's
    - XSS on the Oauth callback URL with CSP bypass leading to zero-click account takeover
    - How I got Access to Auth0 Management API !!
    - BBP#1 (BugBountyProgram Story) Zolo
    - $1000 Bug using simple Graphql Introspection query
    - Beyond Error Messages: Super Admin Deletion due to Broken Access Control (€€€)
    - Budget Change: IDOR 1000$ Bug
    - Open redirect & rXSS via profile image
    - Business Logic Errors on a Local VDP program
    - Admin Panel Bypass Using Google Password Manager
    - One Bug at a Time: Patent Pirating using IDOR | RE'ing US Patent and Trademark Office for fun
    - A web cache deception chained to a CSRF, the recipe
    - Securing Data: How I Quickly Accessed 3000 Student Records in under 5 Minutes
    - Business Logic Errors on a Porn Site—$$$$ Bounty
    - The Story of How I Hacked My Favorite Coffee Shop
- CTF challenges
    - Tryhackme: Brooklyn Nine Nine Walkthrough
    - SQL Injection by Default in Grafana (HTB—Jupiter)
    - Aero HTB | Windows 11 RCE & PrivESC | Themebleed | CLFS
    - HTB: Gofer
    - QueryQuake: Shaking Grafana through Postgres!

- Fadi002/de4py: toolkit for python reverse engineering
- foozzi/discoshell: a simple discovery script that uses popular tools like subfinder, amass, puredns, alterx, massdns and others
- Hakky54/certificate-ripper: A CLI tool to extract server certificates
- fin3ss3g0d/CosmicRakp: CVE-2013-4786 Go exploitation tool
- PatchaPalooza – A Comprehensive Tool That Provides An Insightful Analysis Of Microsoft's Monthly Security Updates
- CloudPulse – AWS Cloud Landscape Search Engine
- Arsenal – Just A Quick Inventory And Launcher For Hacking Programs
- LooneyPwner – Exploit Tool For CVE-2023-4911, Targeting The 'Looney Tunables' Glibc Vulnerability In Various Linux Distributions
- PathFinder – Tool That Provides Information About A Website
- Puncia – Subdomain And Exploit Hunter Powered By AI
- PostLeaks Tool that searches for sensitive data in public Postman API assets

- Have you found a WordPress that the home page redirects to an authentication page? It could be used by Internal teams as a CMS, knowledge sharing, etc
- I often find IDORs by searching in JS Files for interesting endpoints
- Forgotten assets =
- If you find a framework that uses Cargo 4.1.1 version
- If you discover a node.js template area, you should try triggerable node payload

- Saw 403's > Read JS files > Collected endpoints via GAP/Scripts + heavy OSINT > Tested further for Access Control issues > Exposed PII/Confidential content