# Bug Bytes #209 – The only graphQL wordlist you need, ML bug hunting and VDP submissions

BY TRAVISINTIGRITI · AUGUST 23, 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 14th – August 20th

Intigriti News

- Our August Challenge
- inQL GraphQL testing tip!
- XXE Automation Tools

From my notebook

1. Episode 32: The Great Write-up Low-down
2. graphql-wordlist – The only graphql wordlists you'll ever need.
3. Episode 388 – Video game vulnerabilities
4. Google Online Security Blog: AI-Powered Fuzzing: Breaking the Bug Hunting Barrier
5. Weaponizing ML models for red teams and bounty hunters


- How to get started in cybersecurity: HTB Academy – Episode #1, Episode #2, Episode #3
- Not All ZIP Files Are Equal
- Spoof Your Computer
- The Discovery of Zenbleed ft. Tavis Ormandy

- Hacking the Police
- Tracing Automations in HackTheBox Mailroom [Beyond Root]
- 2023 Roadmap To Your First Cybersecurity Job
- The Great Anonymous Scam
- DetectDee
- Bug Bounty: What is VDP and Why submit FREE BUGS?!


- DEFCON 31
  - DEF CON 31 Recon Village Interview (shorts), Red Team Village Interview (shorts), Car Hacking Village Interview, Hack the Box Interview, Voting Village Interview
  - DEF CON 31 Apple TV Spoof – video team (shorts)
  - Crashing AI at the AI Village | DEF CON 31
  - Hack in a Box at Hack The Box | DEF CON 31
  - Hacking the Badge at Hardware Hacking Village | DEF CON 31
  - the Password Cracking Village | DEF CON 31
  - Behind the Scenes at QM | DEF CON 31


- A Conversation about Hack Red Con with Dan and Ken
- Risky Biz News: PowerShell's official package repo is a supply chain mess
- AI versus AI.
- AI chat wars, and hacker passwords exposed
- NO. 394 — Vegas Recap, CISA MS Alert, China/US AI Fight, Deceased Kid AI, Following vs. Leading

- SN 935: “Topics” Arrives – Firefox multi-account containers, DuckDuckGo email alias, satellite crowding
- EP134 How to Prioritize UX and Security in the Cloud: UX as a Security Capability


- Beginner
  - My top 5 bookmarks that I consistently use for bug bounty and penetration testing.
  - Exploring Burp Suite’s Features: A Detailed Overview
  - How i escalate P5 to P3
  - How to Get Unique Subdomains on Large scope
  - Web Scraping Made Easy in 10 Minutes
  - Reconnaissance Strategy and Techniques
  - AppSec Tales XVI | File Inclusion
  - Primer on HTTP Security Headers
- Intermediate
  - Reversing WordPress CVEs: Baby Steps
  - Bypassing XSS Filters: Techniques and Solutions
  - Security Automation 101
  - AppSec Tales XVII | SSRF
  - Bug Hunting on Autopilot, Free VPS Setup
  - Unlocking the Secrets of Network Security: Advanced Nmap Commands for Effective Penetration Testing
  - Defending AWS Assets through Email alerts.
  - Mastering the Realm of GraphQL Exploitation
  - Types of RCE in Brief: Exploring Remote Code Execution Vulnerabilities—7| 2023
- Advanced
  - iOS Pentesting Series Part 3- The Ceasefire
  - NoSQL Injection Redis
  - The Overflowing Cookie Jar: A Fun Tech Adventure
  - Unveiling Vulnerabilities: Host-header injection in OAuth Functionality

- Journey into Windows Kernel Exploitation: The Basics


- Security Research
  - Injecting backdoor into ML model
  - CVE-2023–32315—Path Traversal in Openfire leads to RCE
  - SQL injection in Apache Airflow MySQL provider (CVE-2023–22884)—PoC + exploit
  - Podman API service listening on TCP can be used from websites
  - The Shellcode Compiler Was Right There All Along... (Part 1)
  - LABRAT: Stealthy Cryptojacking and Proxyjacking Campaign Targeting GitLab
  - Third-Party GitHub Actions: Effects of an Opt-Out Permission Model
  - SAP Security: Vulnerability Analysis By RedRays
  - LLM Security Series: Nuts and Bolts
  - A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS: Synology DS920+ Edition
  - Creating Fully Undetectable JavaScript Payloads to Evade Next-Generation Firewalls
  - NetModule Router Software Race Condition Leads to Remote Code Execution – Pentest Blog
  - A phishing attempt on Steam that became a Qrljacking research
  - emptynebuli/StealthBunny: Gadget IoC removal from HAK5's BashBunny
  - Istio outboundTrafficPolicy Egress Control Bypass
- Bugs
  - Hijacking Broken Links for $$$
  - The Ticket Hack: Free travel by hacking the Chennai Metro Rail.
  - My first Bounty Worth $$$$
  - Escaping Input Sanitization By Using Bulk Import Features
  - Change Any User Data on NFT Marketplace crosea.io
  - An IDOR leads join any group makes me $2,500
  - Findings in Swiggy's Codebase: Memory Leak and Google Maps API Key Exposure.
  - SQLi – US Gov Datadump
  - Endpoint Allows for Multiple Account Creation

    - Exploit in /mellon/logout?ReturnTo= : 50$~200$
    - Reflected XSS At U.S. Government
    - My first Bug finding in Apple website
    - Stored XSS Filter Bypass in the Skills section
    - How i earned my first 1000$ in Bug Bounty
    - Easy 500$ Bug
    - Exposed .git to bitbucket account owner's all repository access!
    - A Journey Close to RCE in Nokia
    - Critical XSS Vulnerability in Workflowy
- CTF challenges
    - Lab: SQL injection vulnerability allowing login bypass—2 | 2023
    - HTB: Mailroom
    - Keeper Writeup—HackTheBox—By Amdjed Zerrougui
    - Templates TryHackMe Write-Up


- VEnum—Subdomain Enumeration Tool
- Commix—Command Injection Exploiter
- Intern Showcase: Anonymizing Logs Made Easy with LogLicker
- Xsubfind3R – A CLI Utility To Find Domain'S Known Subdomains From Curated Passive Online Sources
- HackBot – A Simple Cli Chatbot Having Llama2 As Its Backend Chat AI
- Redeye – A Tool Intended To Help You Manage Your Data During A Pentest Operation
- InfoHound – An OSINT To Extract A Large Amount Of Data Given A Web Domain Name