Bug Bytes #202 – CAIDO, Finding your first bug, and OAuth

BY TRAVISINTIGRITI · MAY 31, 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 May 22nd to May 28th

Click here to subscribe

Intigriti News

- Every quarter, we create a portrait of the top hackers in our community! Here they are! Congrats to @0xdln @haylayyyff and Sklon
- May challenge is over! Were you a winner?
- Exploiting file upload vulnerabilities
- 3 Tools to help you automate file upload vulnerabilities
- Web Shell Upload via Obfuscated File Extension

From my notebook

This week I've been thinking a lot about developing a specialism for hacking, being the kind of hacker who can find a bug anywhere because they're an expert in a specific class or type of vulnerability, so here are some resources around that theme from my bookmarks!

1. Web Hacking with Caido – CAIDO is the new Burp replacement everyone is talking about
2. jq Injection [Jason – Hacky Easter 2023] – Really cool injection bug, demonstrated on a CTF
3. Bluetooth device hacking reading list – My number 1 suggestion if you're feeling stuck with your hacking, get a specialism! Maybe bluetooth and IoT could be yours?
4. Narrative over numbers: Andreessen Horowitz's State of Crypto report – This is a great look at why crypto and web3 have slowed down a bit and if it's all hype
5. Google Fuzzing Forum – tutorials, examples, discussions, research proposals, and other resources related to fuzzing. – Another great specialism and a whole bunch of resources to learn it

Videos

- Web Apps Hack and Learn “Let’s Play” Live with Teacher Gerald Auger.
- My YouTube Financials – The Future of LiveOverflow
- Finding Your First Bug
- The Ultimate Panel to Attending a Cybersecurity Conference
- Why You Shouldn’t Be An Ethical Hacker Part 3, Why You Shouldn’t Be An Ethical Hacker Part 4 (shorts)
- Raspberry Pi Malware uses IRC Remote Access Trojan (RAT)
- Building a Password Cracker in Rust
- Learn how I pick locks during physical pentesting work.
- Moise: Transitioning from Big4 to Web3 Security

Podcasts

- Cameron Vincent on Both Sides of Bug Hunting
- James Forshaw on Writing Your Own Tools
- David Weston on the Importance of Security Research
- 298-OSINT Maintenance
- Episode 20: Hacker Brain Hacks – Overcoming Bug Bounty’s Mental Tolls
- 214 – Exploiting VMware Workstation and the Return of CSG0-Days
- 213 – Jellyfin Exploits and TOCTOU Spellcasting
- EP122 Firewalls in the Cloud: How to Implement Trust Boundaries for Access Control
- Episode 376 – Open Source Summit, who built your open source, and AI

- 100 (very) short bug bounty rules
- OWASP LLM Top Ten v.1
- There have been hundreds of thousands of FOSS vuln check rules created.
- Jhaddix talks about his personal brand
- Burp Suite has been solid for me, especially Intruder/autorize/autorepeater for automating custom attacks.
- OSCP got upgrades! But are they good?
- My controversial #BugBounty opinion

- Beginner
  - Unveiling Hidden Bugs in Web Apps: Unique Tips!
  - Malicious File Upload Checklist
  - Introduction to SQL Injection Attacks
  - Subdomain Takeover vulnerability and how to find it using a simple technique
  - Information Disclosure: A Crucial Aspect in Bug Bounty Hunting | 2023
  - What is /etc/passwd group shadow file in Linux
- Intermediate
  - The power of chaining ethical hacking tools such as burp suite, OWASP ZAP, SQLmap and others
  - How to write a perfect Bugbounty report.
  - Analyzing JavaScript Files To Find Bugs
- Advanced
  - How to TraceBack a Spoofed IP in Real-Time Digital Forensics Case.

- Security Research
  - CVE-2023-26818 – Bypass TCC with Telegram in macOS
  - CVE-2023-31070 Broadcom BCM47xx SDK EMF slab-out-of-bounds write
  - Blog – What if we had the SockPuppet vulnerability in iOS 16? – Apple Security Research
  - CVE-2023-33617 Writeup
  - A new OAuth vulnerability may impact hundreds of online services
  - Rooting with root cause: finding a variant of a Project Zero bug | The GitHub Blog
  - Dig Discovers Vulnerability in GCP CloudSQL Leads to Data Exposure
  - State of DNS Rebinding in 2023
- Bugs
  - Azure DNS Takeover @ Swisscom
  - Exploring the Infamous 51% Attack: A Comprehensive Analysis of Blockchain Vulnerabilities | 2023
  - How i managed to get an Easy $$$$ hacking learning website
  - The 30000$ Bounty Affair.
  - Got Access To Server through SQL Injection.
  - IDOR ON EVERYWHERE
  - Simple Bugs—Buying Everything for Free!!!
  - How I was able to find Job by discovering a vulnerability
  - Stored Cross Site Scripting (XSS) via Cross Site Request Forgery (CSRF)
  - First Bug: Backup file Found
  - A Unique Tale Of P1: Exposed GraphQL Leads to Mass User Account Takeovers
  - Utilizing Historical URLs of an Organization to successfully execute SQL queries—Blind SQLi
  - From Broken Object Level Authorization to the Massive Financial Attack
  - Price Manipulation Vulnerability: Potential Exploitation in Dating Website
  - Finding a Unique Kind of IDOR
  - OTP bypass via response manipulation
  - XSS Via Qr Code

    - How I found Reflected XSS in Users login page on Public Program ?
    - How I was able to access data of other users [Insecure Direct Object Reference]
    - Unveiling the Hidden Gems: A Bug Bounty Journey of Multiple Discoveries
    - I helped the top Indian health benefits management platform from major PII leak
    - 2FA Bypass Using Custom Cookie Parameter
- CTF challenges
    - HTB: Absolute
    - Secure the Web: Exploring Defense Strategies for Web Realistic Levels 1–4 CTF Challenges
    - OverTheWire Bandit: Solving Level 5

- GitHub – mthbernardes/codeexplain.nvim: GPT powered nvim plugin that helps you understand code.
- All-Time Best Tools for Bug Hunting
- PentestGPT – A GPT-empowered Penetration Testing Tool
- rebindMultiA – Tool To Perform a Multiple A Record Rebind Attack
- Jsfinder – Fetches JavaScript Files Quickly And Comprehensively
- katoolin3 – Get your favourite Kali Linux tools on Debian/Ubuntu/Linux Mint
- espionage – Collects informations related to domains whois, history, dns records and more
- wgen.io – Generate rich wordlists for targeted attacks online

- 10 (very) short tips for bug bounty
- You can now attach notes to requests via the new ‘Organizer’ tab

- My list of resources for beginner hackers!
- LFI in misconfigured rails application
- When hunting for Blind XSS, remember to use a unique identifier for each payload and log your steps meticulously
- A guide to SSRF vulnerabilities and where to find them

- Tesla Whistleblower Leaks 100GB of Data, Revealing Safety Complaints
- Google Cloud Bug Allows Server Takeover From CloudSQL Service