Bug Bytes #194 – Google's highest bounty of 2022, making extensions and Chaos goes into beta

BY TRAVISINTIGRITI · FEBRUARY 28, 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 February 20th to February 26th

CLICK HERE TO SUBSCRIBE

Intigriti News

- Congrats to the hackers who topped our monthly leaderboard!
- We did some game hacking
- And challenged you to find the vulnerability in our code snippet, here's the solution if you missed it!
- Digging into some Web3 security

From my notebook

This week Google reflected on it's vulnerability management program, which is their bug bounty program. So the first two links are their blogpost and a podcast episode which gives a little more context. Number 3 is a great introduction to how chrome extensions are created and particularly the kind of permissions you give them when you install it. Finally, the last 2 are about some specialist skills, first of hardware tools for IoT/physical device security and then a look at version control using .git and how that became an RCE.

1. Vulnerability Reward Program: 2022 Year in Review
2. EP109 How Google Does Vulnerability Management: The Not So Secret Secrets!
3. Let's build a Chrome extension that steals everything
4. Unlocking the Secrets of IoT Security: A Comprehensive Guide to Using Hardware Tools for Bug...
5. $10.000 bounty for exposed .git to RCE

Other Amazing Things

Videos 

- Can You Find Where a Picture was Taken?
- Hack The Box – Shoppy (Easy) – Live Walkthrough
- Active Engagement: Cybersecurity Research with Kody Kinzie
- Get a cybersecurity job just by doing this
- Russian Missile Alert System Hacked
- awk Injection via JWT Forgery [HackTheBox – Awkward]
- Playing With Idors With @IAmRenganathan | Hacker2Hacker
- 2FA Bypassing Techniques

Podcasts 

- 190 – Fuzzing cURL, Netatalk, and an Emulator Escape
- Episode 8: PostMessage Bugs, CSS Injection, and Bug Drops
- NO. 370 | GoDaddy Hack, EU Chinese APTs, Hacking with ChatGPT
- 189 – Compromising Azure, Password Verification Fails, and Readline Crime
- 290-Extreme Privacy: Mobile Devices
- Episode 363 – Joylynn Kirui from Microsoft on DevSecOps

Tweets 

- How long did it take you to start getting bug bounties?

- Jetty CVEs
- Recon is a trap
- Learning Rust? Donut has a suggestion
- Generic University is now on TryHackMe
- Pancakes Con schedule on March 19th
- Call to Delhi based hackers!
- The most exciting notification
- Apple pay vs Google pay
- Bug bounty /pentest tool notes (teaser)

- ChatGPT for Bug Bounty: Faster Hunting and Reporting
- Nuclei: Automating Web Application and Network Service Testing [Cheat Sheet]
- Bug Bounty Manual Recon Guide
- Exploring the Dangers of SQL Injection and Cross-Site Scripting
- Getting Started with Frida: Setting up on an Emulator
- Exploiting XXE to retrieve files
- Mastering/understanding the Crawler Indexing Before Osint
- Getting Started with Google Cloud Platform
- Bug Bounty Hunting 101: WAF Evasion
- Understanding SSL—Secure Socket Layer | 2023
- Bypass FreeRASP's Mobile Security Measures in Flutter
- Exploiting Remote Command Execution Vulnerability in EasyNAS
- USB Forensics 101

- WordPress Plugins Security Analysis
- My First Un-Expected $$$$ Digit Bounty for an Un-Expected Vulnerability
- The Vulnerability That Exposed an UN Website to Remote Code Execution
- Interesting Stored XSS in sandboxed environment to Full Account Takeover
- How i was able to find Django Misconfiguration using Shodan.
- RCE Writeups
- Account Takeover worth of $5
- How did I found RCE on SHAREit which rewarded $$$ bounty
- How To Attack Admin Panels Successfully Part 3
- Bypassing CORS configurations to produce an Account Takeover for Fun and Profit
- Easy bounties and Hall of fame
- Little bug, Big impact. 25k bounty
- Blind XSS fired on Admin panel worth $2000
- How I Used JS files inspection and Fuzzing to do admins/supports stuff
- How do I take over another user subdomain name worth $$$$
- With a single request, you can kill any Gitea server
- Html Injection On One Of The Indian Government's Official Domain
- How I Bypassed The OTP By Different Method (Part-1)
- HubSpot Full Account Takeover in Bug Bounty
- Business logic flaw, the enemy of scanners
- XSS and chicken biryani got along.
- How I got into Nokia HOF in 5 Mins
- Information Disclosure Vulnerability in Adobe Experience Manager affecting multiple companies...

- My first finding XSS,IDOR
- Using the “World’s Worst Fuzzer” To Find A Kernel Bug In The FiiO M6
- SQL Injection + RCE | How I got a shell on my university website
- [1500$ Worth—Slack] vulnerability, bypass invite accept process
- The ‘U Up?’ Files with Joran Honig
- Bypassing SSO Authentication from the Login Without Password Feature Lead to Account Takeover
- Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS
- How I was able to Turn a XSS into A Account Takeover
- Leaked tokens on personal GitHub repositories

- FavFreak: A Penetration Testing Tool for Favicon Analysis and Subdomain Enumeration [Cheat Sheet]
- APKHunt – Comprehensive Static Code Analysis Tool For Android Apps That Is Based On The OWASP MASVS Framework
- SXDork – A Powerful Tool That Utilizes The Technique Of Google Dorking To Search For Specific Information On The Internet
- Probable_Subdomains – Subdomains Analysis And Generation Tool. Reveal The Hidden!
- Leaky Paths – A collection of special paths linked to major web CVEs, known juicy APIs, misconfigurations
- Project Discovery’s Chaos goes into beta – Recon data for Public Bug Bounty Programs
- FilePursuit – lists files available on the internet from open directories

- IDOR tip for uuid based APIs
- More uuid tips
- Checkout flow business logic error tip
- Secure code review thread of tips
- Shodan dorking, example on splunk
- XSS filter bypass
- Open Redirect to XSS
- GraphQL tips
- Leaked keys with regex
- Angular extract API endpoints one-liner
- Account takeover with JWTs