Bug Bytes #199 – Hacking LLMs, Bug Chains and Hackers Chat in LA

BY TRAVISINTIGRITI · MAY 10, 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 1st to May 7th

Click here to subscribe

Intigriti News

- The intigriti YouTube channel has officially passed the 15k milestone!
- Top 5 Web Extensions for bug bounty hunting (for Chrome & Firefox)!

From my notebook

1. Offensive Security w/Olivia Gallucci
2. Dependabot Confusion: Gaining Access to Private GitHub Repositories using Dependabot
3. Privilege Escalations through Integrations
4. A smorgasbord of a bug chain: postMessage, JSONP, WAF bypass, DOM-based XSS, CORS, CSRF...
5. HackAPrompt is a prompt hacking competition aimed at enhancing AI safety and education by challenging participants to outsmart large language models (e.g. ChatGPT, GPT-3). – Prompt injection explained

Other Amazing Things

- ChatGPT tries a BASIC Capture The Flag (CTF) Challenge
- Asset Discovery Using Shodan + Giveaway! // Bug Bounty Recon

- Hunt for Hackers with Velociraptor
- Static Malware Analysis using PEStudio
- Here are 3 FREE web hacking resources to learn web hacking! (shorts)
- Hack The Box – Juggling Facts (Easy) – Live Walkthrough
- InfoSec Unnplugged: Queen of Purple Team with Maril Vernon
- Dangerous Codes: SQLi (shorts)
- Facebook's TOP1 bounty hunter about how to not be replaced by AI (shorts)
- How long does Facebook's TOP1 hunter stay on one target (shorts)
- What Facebook's TOP1 bounty hunter does differently (shorts)
- Stored, Blind, Reflected and DOM – Everything Cross–Site Scripting
- Portswigger Web Academy – Server-Side Template Injection (SSTI)
- How I am learning Web3! (Smart Contracts, Security, Bug Bounty)
- Hacking an organization with one of the most stealthy and dangerous web attacks
- Inside the Mind of the TOP1 Facebook Bug Bounty Hunter
- TryHackMe – OWASP Top 10 (2021) – Live Walkthrough

- EP119 RSA 2023 – What We Saw, What We Learned, and What We're Excited About
- The Reason You Don't Have Data Privacy
- NO. 380 — LLM-Mind-Reading, Automated War, Rusty Sudo, Eliezer Bitterness Theory
- 207 – Git Config Injection and a Sophos Pre-Auth RCE
- SN 921: OSB OMG and Other News! – Age verification, Google Authenticator E2EE, VirusTotal AI, cURL
- Risky Business #704 — Why LLMs aren't an exploit bonanza
- 208 – A Timing Side-Channel for Kernel Exploitation and VR in the wake of Rust
- Episode 374 – The event we called left-pad, Episode 77 remaster part 1

- 133: I'm the Real Connor
- Episode 17: LA Live Chat with Five Legendary Hackers

- Could you pass the turing test?
- Last year, @Jhaddix, @bscarvell, @seanyeoh and I found a pre-auth RCE in Oracle Opera – CVE-2023-21932. This product holds the PII of every guest (including credit cards)
- I seek from my fellow hacker friends to invest wisely their bounties and earnings to be able to rest a few years from now
- To bug bounty hunters, where do you store your recon data and your test data in general
- I really really really hate call out posts against specific triagers.
- Flipperzero, very useful when you dont have your hotel room key with you!
- If you as a #bugbounty hunter buy stolen credentials off of cyber criminals and send it as a report to us in our bugbounty program, we will NOT pay, as we do not support criminal activities or engage in any activities that support criminal activities.
- Oh yeah, another funny thing about @OpenAI's new "Code Interpreter" is the way it looks super vulnerable when downloading any file from your own k8s containe

- c{api}tal walkthrough
- Achieve Maximum Protection With Minimal Effort: Beginning Your Zero Trust Journey
- Write-up of Lame—An easy-rated HTB machine.
- JAVASCRIPT PROTOTYPE POLLUTION VULNERABILITIES PART 1
- CIDR IN HACKING
- Understanding Server Side Request Forgery (SSRF): Owasp API6 | 2023
- Bypassing MPX Node Authentication—Firmware analysis

- Red Teaming: Exfiltrating Data & Command Network Nodes (Like a Ghost!)
- phpMyFAQ-3.1.12 CSV Injection
- The Art of Reconnaissance for Bug Bounty: Finding Vulnerabilities like a Pro
- Ruby Code Vulnerability Analysis: ConfirmSnsSubscription RCE
- The Art of Bug Bounty Reporting: Mastering Effective Communication and Persuasion
- "Ooo aaa uuuthh" or 2 me, OAuth ! Tips on conquering OAuth2!
- GO Code Review #1 : Hard-coded credentials are security-sensitive
- TryHackMe's WebOSINT Simple Writeup— Conducting Basic Open-source Intelligence Research
- GPT-4 – How does it work, and how do I build apps with it? – CS50 Tech Talk

- Credential Stuffing: Speeding up massive leaks databases
- Unauthorized access to the admin panel via leaked credentials on the WayBackMachine
- Researching Polymorphic Images for XSS on Google Scholar
- From blind XXE to root-level file read access
- Account Takeover Worth $100,000
- Easiest Bug To Find That Worth 200$ Bug Bounty
- Idor View To History Order Users
- Exploiting an Order of Operations Bug to Achieve RCE in Oracle Opera
- How do I Bypass Payment when a Subscription ends so I don't have to pay for my subscription
- /Metrics ; Easiest Bug To Find ,That Worth $$$ (Bug Bounty)
- Subdomain Take Over on Azurewebsite
- Vulnversity—TryHackMe Room
- OSINTorg Revealed
- Leaking Account Credentials with Excel: Hunting Vulns in Office365

- Metasploit: Meterpreter—TryHackme Simple Writeup | 2023
- Red Teaming: 0x01 Click RCE via VoIP USB
- PHP Backdoor Obfuscation
- LDAP Injection
- from self html injection to ssrf
- IDOR CHANGES DESCRIPTION ANOTHERS USERS/COMPANY
- The story of how I finally got my first money from hacking
- How I found +100 Reflected Cross Site Scripting & SQL Injection
- Accessing Admin Dashboard in 5 seconds: Hall of Fame.
- Exploiting Put Method to upload malicious file
- Simple Account Takeover Worth $9,999
- Mass Assignment leads to the victim's account being inaccessible forever
- XSS drag Drop in Google worth $6,999
- My first P3 in bug crowd (cross site scripting) xss
- Four Digit Bounty($$$$) in 10 mins
- How I Discovered and Reported a PII Disclosure Vulnerability
- How I got €50 from tag . It literally bypassed everything.(UNEXPECTED BYPASS)
- My first XSS without parentheses and semi-colons
- I got XSS in a million websites
- An Epic Account Takeover Worth $57,500
- Azure Account Takeover Worth $11,756
- IDOR to Account Takeover
- How I discovered XSS via triple URL encode
- Race Condition To Get Followers Unlimited
- 200$ Exploit On /mellon/logout?ReturnTo=
- How a simple Directory Listing leads to PII Data Leakage, Remote Code Execution and many more
- Facebook OAuth Vulnerability Worth $55,000
- Unauthorized access in GitHub worth $17,875

- Unauthenticated access to messages
- How Bug Bounty Hunters Find Complex Vulnerabilities
- Client Secret = Should be Secret
- Three Argo CD API exploits, distributed identity for modern API security

- Discover API endpoints with Feroxbuster
- Proxy Postman into Burp Suite
- Teler-Waf – A Go HTTP Middleware That Provides Teler IDS Functionality To Protect Against Web-Based Attacks
- NTLMRecon – A Tool For Performing Light Brute-Forcing Of HTTP Servers To Identify Commonly Accessible NTLM Authentication Endpoints
- Httpx and EagleEye for Hackers.
- Bypass WAF with SQLMAP and TOR
- PimpMyBurp #8 – Perform Advanced Fuzzing With Turbo Intruder
- Introducing SpiderSuite: Advance web security crawler
- Visualizing Katana crawl results using SpiderSuite.
- Discover Hidden Domains with DomainSleuth
- 10 handy practical #hacking tools I've developed over the years @hakluke
- httpx v1.3.0 update with screenshot support
- Bypass WAF / Restrictions with REcollapse

- Account Takeover checklist
- Bug bountry tips from twitter
- Did you know you can recover scrubbed metadata from a PDF that wasn't scrubbed properly?
- If you happen to find Symfony Web Framework that has Symfony profiler debug mode enabled, fuzz the following endpoints:
- Don't discount dead subdomains in bug bounty! Try enumerating them against valid target IP addresses, who knows what you might find
- My new favorite SQLi finding methodology returning some great results...
- Complete #BugBounty Recon Fundamentals
- Quick DOM-XSS Tips

- So long passwords, thanks for all the phish
- Apple Fails to Fully Reboot iOS Simulator Copyright Case (1)
- FYI: Intel BootGuard OEM private keys leak from MSI cyber heist