Bug Bytes #160 – Invisible SQL Injection, Reading redacted text & Coinbase's largest-ever bug bounty

BY ANNA HAMMOND · FEBRUARY 23, 2022 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from February 14 to 21.

Intigriti news

Ethical Hacker Survey 2022

Our favorite 5 hacking items

1. Vulnerability of the week

@Tree_of_Alpha on Coinbase's "largest-ever bug bounty", Coinbase's Retrospective & A 60s explanation by @Farah_Hawaa ($250,000)

@Tree_of_Alpha shares how they discovered a business logic issue on Coinbase and was rewarded a quarter-million-dollar bounty.
The wild part is that it didn't involve any Web3 hacking. The root cause was a missing logic validation check in an API endpoint, which allowed selling Bitcoin and other cryptocurrencies without owning them.

2. Writeup of the week

Finding an unseen SQL Injection by bypassing escape functions in mysqljs/mysql

This is about an escape function in mysqljs/mysql that is commonly misunderstood and misused. It causes many Node.js projects that use this package to be vulnerable to SQL injection.

According to the author, @stereotype32, this vulnerability has been known to many web security researchers but most SQL injection scanners miss it.

3. Tool of the week

Unredacter & Never, Ever, Ever Use Pixelation for Redacting Text

@2600AltF4 released a new tool for uncovering redacted pixelated text. It solves some limitations that another similar tool, Depix, has.
Two useful takeways for pentesters / bug hunters: The only way to securely redact text is to use black bars. And if you find redacted documents or screenshots that may contain sensitive information, try reading it with Unredacter.

4. Video of the week

BOUNTY THURSDAYS – LIVE #1 (SVG-XML/Redirects/OOB servers and Community Questions)

Do you know what's better than a Bounty Thursdays episode? A LIVE Bounty Thursday episode!
This is an amazing opportunity to be part of the show, interact with @stokfredrik and his co-host @Jhaddix, and stay up-to-date with bug bounty news in a fun way.
It's supposed to be a bi-weekly show, so keep an eye on the channel.

5. Challenge of the week

Javascript reverse engineering challenge & Video walkthrough

This is a good challenge to test your JavaScript deobfuscating and reverse engineering skills. The video shows how to solve it using dynamic analysis with DevTools.
So even if you're not interested in reverse engineering per se, it may teach you some useful tricks on DevTools and how to approach big JavaScript files when doing client-side code review.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Is clicking a link bad in 2022? & Part 2
- Bug Bounty Recap February 10 – 16
- The 'Million Dollar Hacker' – Tommy DeVoss AKA 'Dawgyg' & The Fearless Hacker On Learning How To Hack | Mike Padrick
- The CyberSec Show (#6) – LiveOverflow
- Exploring Python SSTI Payloads & Exploring mkfifo / nc Reverse Shell
- Reversing Assembly – Pwn Zero To Hero 0x01

- Reverse Engineering 101 – Intro to Ghidra on Linux by Reversing 5 crackmes
- Hacking Will Tear Us Apart: Hacking Battlegrounds #4

Webinars

- Attacking JSON Web Tokens with Louis Nyffenegger
- Hacking ELECTRON: JavaScript Desktop Applications w/ 7aSecurity
- Introducing PurplePanda: AUTOMATED Privilege Escalation IN THE CLOUD

Tutorials

Medium to advanced

- Healing blind injections
- SSH into your private machines from anywhere, for free, using Cloudflare Tunnel
- 10 ways of gaining control over Azure function Apps
- A primer on DCSync attack and detection
- Macrome – Excel Macro Document Reader/Writer For Red Teamers And Analysts

Beginners corner

- Did default SameSite:Lax put the nail in the coffin for CSRF? Mostly, but not always!
- What is Google Dorking?
- Avoiding Mixed Content Errors With An HTTPS Python Server
- Current MFA Fatigue Attack Campaign Targeting Microsoft Office 365 Users

Writeups

Challenge writeups

- HackTheBox – Bolt, Blog post
- XSS for beginners – Google XSS Game Levels 1 & 2
- Writeups for Hayyim Security CTF 2022
- UNION SQL Injection to Extract Data From Other Tables!

Responsible(ish) disclosure writeups

- Zabbix – A Case Study of Unsafe Session Storage #Web #CodeReview
- Horde Webmail 5.2.22 – Account Takeover via Email #Web #CodeReview

- Oh Snap! More Lemmings: Local Privilege Escalation Vulnerability Discovered in snap-confine (CVE-2021-44731) #Linux #LPE
- CVE-2022-0478 – WooCommerce Event-Manager Plugin SQL Injection #Web
- CVE-2021-44521: Exploiting Apache Cassandra User-Defined Functions for Remote Code Execution #Web #CodeReview

Known vulnerabilities

- A Samba's horror story, CVE-2021-44142 & PoC
- CVE-2021-26084 PoC write-up
- Apache: Code execution in log4j2

Bug bounty writeups

- Hunting for bugs in VMware: View Planner and vRealize Business for Cloud
- RCE in GitHub Desktop < 2.9.4 (GitHub, $2,000)
- My first report on HackerOne: A logic flaw in npm (Node.js)
- ICMAD SAP Vulnerabilities (CVE-2022-22536, CVE-2022-22532 & CVE-2022-22533) & onapsis_icmad_scanner
- Advisory: Cisco RV340 Dual WAN Gigabit VPN Router (RCE over LAN) (Cisco)

See more writeups on The list of bug bounty writeups.

Tools

- TLD:er: TLDs finder — check domain name availability across all valid top-level domains.
- OnHandlers: Script to generate Event Handlers and bypass filters
- uproot-JS/: Extract JavaScript files from burp suite project with ease
- nrich: A Rust tool to quickly analyze all IPs in a file and see which ones have open ports/ vulnerabilities
- KrbRelay: Framework for Kerberos relaying
- ltmod (Left To My Own Devices) & Intro: Fast NTCracking tool in Rust

Tips & Tweets

- Bypass 403 Forbidden with CNAME
- jid on jq – interactive JSON query tool using jq expressions & JSON diff and patch
- Always try this on GraphQL endpoints

- Getting security research ideas from RFCs & @EdOverflow's process for coming up with new security research areas
- @Frichette_n on aws_api_shapeshifter, a library they used to find XSS in the AWS Console
- Direct path to become Domain Admin if you compromise a member of the Backup Operators group

Misc. pentest & bug bounty resources

- A Practical Guide To Attacking JWT (JSON Web Tokens)
- Cursed Types: List of Trusted Types bypasses
- Subdomain enumeration statistics and wordlists from bugbounty scopes & Intro
- Nmap Cheat Sheet: Commands & Examples (2022)
- Node.js Vulnerability Cheatsheet
- Meta(Facebook) BugBounty-Writeups

Articles

- Subdomains Tools Review: a full and detailed comparison of subdomain enumeration tools
- Relaying Kerberos over DNS using krbrelayx and mitm6
- Steal Credentials & Bypass 2FA Using noVNC
- Stealing and faking Azure AD device identities
- The Death of "Please Enable Macros" and What it Means

Challenges

- Intigriti 1337UP LIVE CTF (March 11 – 12)
- picoCTF 2022 (March 15-29)
- 2 free Red Team Fundamental rooms (on THM)

Bug bounty & Pentest news

- Bug bounty
  - Jaw-dropping Coinbase security bug allowed users to steal unlimited cryptocurrency
- Upcoming events
  - ZAPCon 2022

    - NULLCON Berlin 2022 (James Kettle will keynote on “Hunting evasive vulnerabilities: finding flaws that others miss”)

- Tool updates
    - dnsx v1.0.8
    - Certipy 2.0: BloodHound, New Escalations, Shadow Credentials, Golden Certificates, and more!
    - WCFDSer-ngng (more up-to-date than the Burp BApp Store version)