Bug Bytes #157 – Daily bug bounty recaps, Reading other bug hunter's reports & Hacking Google Drive integrations

BY ANNA HAMMOND · FEBRUARY 2, 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 January 24 to 31, 2022.

Intigriti news

Nullcon Berlin Student Scholarship (Sponsored by Intigriti)

Our favorite 5 hacking items

1. Vulnerability of the week

pwnkit: Local Privilege Escalation in polkit's pkexec (CVE-2021-4034)

PwnKit or CVE-2021-4034 is a Local Privilege Escalation in polkit's pkexec that was discovered by Qualys researchers.
It is noteworthy because it affects all major Linux distributions by default and all pkexec versions since 2009. Actually, @ryiron blogged about the root cause behind it in 2013.
Also, the vulnerability is exploitable reliably even though it is a memory corruption bug.

To practice, there is a free TryHackMe room, and some exploits by the community:

- PoC ("ctf quality exploit")

- PwnKit-Hunter
- berdav/CVE-2021-4034

2. Writeups of the week

Hacking Google Drive Integrations (Dropbox, $17,576)
How I could have read your confidential bug reports by simple mail? (Microsoft)
A story of leaking uninitialized memory from Fastly (Fastly)

These are three entirely different types of findings but all very impressive and worth reading: @rootxharsh found a full read SSRF on Google Drive integrations in Drobox, @Sudhakarmuthu04 found a way to read other bug hunters' reports on the Microsoft research portal, and @emil_lerner discovered a memory leak in the QUIC (HTTP/3) implementation of the H2O webserver.

3. Conference of the week

Black Hat Europe 2021

Recordings from Black Hat Europe 2021 were just released! Need I say more?
Maybe only that slides and whitepapers can be found here, and @albinowax really recommends @_dannielthatcher's talk "Practical HTTP Header Smuggling: Sneaking Past Reverse Proxies to Attack AWS and Beyond".

4. Video of the week

__Bug Bounty Recap__ January 20-26

I'm really enjoying these daily bug bounty recaps by @PinkDraconian. They are crisp and easy to digest, a fun way to stay up-to-date or get clarifications on writeups you're struggling to understand.

5. Tools of the week

Har Har Har Viewer
CodExt

CodExt is both a CLI tool and Python library for encoding/decoding anything. It extends the Python coded library with 120+ new codecs and has a "guess mode".
I know there are many tools that do the same thing, but if you prefer the CLI and need support for both Bash and Python, this is a handy alternative.

Har Har Har Viewer is another useful tool. Like its name suggests it is a HAR viewer, worth bookmarking for the next time you need to handle HAR files.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Fuzzing Java to Find Log4j Vulnerability – CVE-2021-45046
- Escalating Your Bugs With GDPR Impact
- Web App Pentesting – HTTP Headers & Methods & Web App Pentesting – Setting Up OWASP bWAPP With Docker
- Enumerating 100 targets at once! Meg – Hacker Tools & Blog post
- Kiosk Breakout & HOW TO Install Windows 11: VMware Workstation

Podcasts / Audio

- Bug Bounty Community Chats #1

Webinars

- AppSec Triage: Finding Needles in the Application Haystack
- Fixing OSS Security Vulnerabilities at Scale!
- A Master Class on Offensive MSBuild

Conferences

- HEK.SI 2022 – Bypassing UAC With UACMe
- Attacking Modern Environments Series: Attack Vectors on Terraform Environments

Slides & Workshop material

- State of DNS Rebinding (via @HolyBugx)

Tutorials

Medium to advanced

- Password spraying and MFA bypasses in the modern security landscape
- How To Extract Credentials from Azure Kubernetes Service (AKS)
- How to disable XXE processing? #BlueTeam
- RBCD WebClient attack

Beginners corner

- Vulnerabilities that aren't. Cross Site Tracing / XST
- Advanced URL And JavaScript Enumeration
- A Tale of DOM-based XSS!
- How To Get Started Hacking Django Based Applications
- The shades of tunneling

Writeups

Challenge writeups

- HackTheBox – Anubis
- Open Redirect Leading to OAuth Access Token Disclosure!
- Healthcare with S1REN!
- ATM/Kiosk Hacking

Pentest writeups

- My SQLi adventure or: why you should make sure your WAF is configured properly
- The Organization, Vendor & Application Security
- AD CS: weaponizing the ESC7 attack

Responsible(ish) disclosure writeups

- Paranoids' Vulnerability Research: PrinterLogic Issues Security Alert #Printer
- Bypassing Little Snitch Firewall with Empty TCP Packets #MacOS
- Don't Trust This Title: Abusing Terminal Emulators with ANSI Escape Characters #CLI
- CVE-2022-23968: Xerox vulnerability allows unauthenticated users to remotely brick network printers (UPDATED) #Printer

Bug bounty writeups

- Moodle: Blind SQL Injection (CVE-2021-36393) and Broken Access Control (CVE-2021-36397) (Moodle)
- The Story of a RCE on a Java Web Application
- Bypassing SSRF Protection to Exfiltrate AWS Metadata from LarkSuite (Lark Technologies)
- Microsoft OneDrive For Macos Local Privilege Escalation (Microsoft)

- CVE-2020-0696 – Microsoft Outlook Security Feature Bypass Vulnerability (Microsoft)
- WPA2-Enterprise/EAP Subject Matching Vulnerability (Google Chromium, $3000)
- CVE-2022-0185 – Winning a $31337 Bounty after Pwning Ubuntu and Escaping Google's KCTF Containers (Google, $31,337)

See more writeups on The list of bug bounty writeups.

Tools

- pty4all & Intro: Persistent multi reverse pty handler
- PurplePanda: Identify privilege escalation paths within and across different clouds
- LDAP Relay Scan: Check for LDAP protections regarding the relay of NTLM authentication

Tips & Tweets

- HTML injection in PDF generators
- Try random stuff, get random results
- A couple of "fun" GitHub behaviors
- Updates to PortSwigger's XSS cheat sheet: 1, 2, 3 & 4
- Did you know that local files in Windows can be accessed with `drive://` (e.g. `f://`)?

Misc. pentest & bug bounty resources

- Awesome WebSockets Security & WebSockets Playground
- Trickest Log4j & Collaboration with @Six2dez1 to automate updating OneListForAll
- Frida HandBook (learnfrida.info)
- RTCSec newsletter – STIR/SHAKEN DoS, Cisco phone passwords, Zoom and Yealink
- Stratus Red team: Granular, Actionable Adversary Emulation for the Cloud (like "Atomic Red Team™" for the cloud)

Articles

- Recovering redacted information from pixelated videos
- .NET Remoting Revisited
- Unauthenticated Dumping of Usernames via Cisco Unified Call Manager (CUCM)
- ldd arbitrary code execution

- Evolved phishing: Device registration trick adds to phishers' toolbox for victims without MFA
- Delegate to KRBTGT service

Challenges

- A list for free Penetration Testing & Red Teaming Labs to build locally
- A free HTB machine added every month to the Starting Point Track

Bug bounty & Pentest news

- Bug bounty
  - Android security tool APKLeaks patches critical vulnerability #Web
  - No smoke without fire? 'Critical' Loguru security flaw turns out to be non-issue & CVE-2022-0329 and the problems with automated vulnerability management
- Cybersecurity
  - OffSec Standalone Course Pricing Changes
  - UK government plans to release Nmap scripts for finding vulnerabilities
  - Cracking A $2 Million Crypto Wallet & Video
- Jobs
  - GitHub is looking for junior security researchers to help secure OSS using CodeQL
- Upcoming events
  - OAuth 2.0 Hacking for Beginners with Farah Hawa (February 6)
  - Nullcon Berlin Student Scholarship (Apply before March 10)
- Updates
  - SecLists 2022.1
  - New on HackTricks: GCP – Abuse GCP Permissions

Non technical

- Thought Process Behind Creating the Box Delivery
- What I learnt from reading 220* IDOR bug reports.
- From Marine Jarhead to Hacker, the Chuck Woolson Story