Bug Bytes #123 – Exiftool RCE, Learn mobile hacking for free & #BurpHacksForBounties

BY ANNA HAMMOND · MAY 19, 2021 · 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 May 10 to 17.

Intigriti News

Meet the hacker: 0xkasper, CTF player, Student, and hunter

New SSRF Blanket in our swag shop

Our favorite 5 hacking items

1. Resources of the week

@reyammer's mobile security class material from MOBISEC 2020
The Missing Semester of Your CS Education

The first resource is a complete course on mobile hacking by @reyammer. It includes video recordings, slides, challenges and covers a lot of topics from basics to advanced notions.

The second course is about various tools used in Computer Science classes that are rarely introduced properly. This includes how to best use the command line, text editors, tools like tmux to access remote machines, Git, etc. These topics are actually relevant to all hackers, not only CS students.

So, hurray for two completely free, top-notch quality courses!

2. Writeups of the week

ExifTool CVE-2021-22204 – Arbitrary Code Execution (GitLab, $20,000)
CVE-2021-27651: Pega Infinity RCE
FragAttacks

Remember CVE-2021-22204, the Exiftool RCE from a couple of weeks ago? There weren't any public exploits for it at the time. @wcbowling just shared how he exploited it to get RCE on GitLab for $20k. This prompted other hackers to share articles about recreating exploits for the same bug. Here are the links if you want to do a deep dive into it: CVE-2021-22204 – Recreating a critical bug in ExifTool, no Perl smarts required. & An Image Speaks a Thousand RCEs: The Tale of Reversing an ExifTool CVE.

The second writeup is about an RCE in Pega infinity that @samwcyo's team discovered while hacking on Apple. It is interesting to see the technical details of a bug in open source software that was used for bug bounties on big targets like Apple.

The third writeup if for all of you Wi-Fi hackers. @vanhoefm found several vulnerabilities in all modern security protocols of Wi-Fi (goind back to 1997 and including WPA3!). What's most impressive is that some of them are implementation flaws but three are design flaws in the Wi-Fi standard itself.

3. Tools of the week

whey-cewler.py
Copy As FFUF

Whey CeWLer is a Burp extension by @LaNMaSteR53 that parses your already crawled SiteMap and creates a wordlist. This is a convenient method for creating target-based custom wordlists that can be used for Web fuzzing and directory bruteforce.

Copy as FFUF is also a handy Burp extension. If you often find yourself copying requests from Burp to fuzz with FFUF, this will make the process much quicker.

4. Tips of the week

#BurpHacksForBounties – @sec_r0's 30 days of Burp tips

@sec_r0 is sharing a Burp hack each day for 30 days, and they are good! If you want to level up your Burp skills make sure to follow him and apply these tips.

5. Conference of the week

Black Hat Asia 2020, BH Asia 2020 Slides & BH Asia 2021 Slides

40 videos from Black Hat Asia 2020 were just made public. There's variety of topics so each talk's description and slides will help quickly decide if you want to watch the whole talk.
If you're also curious about the Black Hat Asia 2021, the recordings aren't available yet but slides are. Some of these presentations on Web and mobile hacking are pretty interesting!

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Wanna hack zseano website and get paid? – Bounty Thursdays #28
- bsidesahmedabad AMA with Shubs
- Stealing all your passwords from LastPass due to URL parsing vulnerability – $1,000 bounty
- Q&A session with NahamSec
- Hack The Box Hacking Battlegrounds Streamed Tournament #1 – Commentated by IppSec and John Hammond
- Creating Custom Nuclei Templates and Workflows
- Free Automated Recon Using Github Actions | Ft. Project Discovery

Podcasts

- DAY[0] Episode 77 – Cross-Browser Tracking, Frag Attacks, and Malicious Rust Macros
- The WiFi Frag Attacks – DarkSide Follow-Up, DarkTracer, Patch Tuesday, The Frontiers Saga

Webinars

- OWASP May Lightning: Hacking APIs for Beginners (with Katie Paxton-Fear)
- The Tangled Web and Its Same Origin Policy (OWASP Bay Area Meetup – May 2021)

Conferences

- Bug hunter adventures | Yuvraj Dighe and Shreyas Dighe | Nullcon Security Conference March 2021

Tutorials

Medium to advanced

- Overcoming Issues Using Custom Python Scripts with Burp Suite Professional
- Upgrading XSS Hunter with a basic reverse JavaScript shell
- Deploying a Hash Cracker in Azure
- AMSI Bypass Methods

Beginners corner

- Hacker tools: Arjun – The parameter discovery tool
- The Shell..
- Privilege Escalation Attack : Attacking AWS IAM Permission Misconfigurations
- Wi-Fi Penetration Testing – Part 1

Writeups

Challenge writeups

- A tale of solving all the recent XSS challenges using chrome 1-day.

Pentest writeups

- Simple Data Exfiltration Through XSS
- SSRF in Open Distro for Elasticsearch
- Leveraging Microsoft Teams to persist and cover up Cobalt Strike traffic

Responsible(ish) disclosure writeups

- Aurelia Framework Insecure Default Allows XSS #Web
- Terminal escape injection in AWS CloudShell #RCE #Cloud
- Exploiting custom protocol handlers for cross-browser tracking in Tor, Safari, Chrome and Firefox #Browser
- CVE_2021_1079 – NVIDIA GeForce Experience Command Execution #LPE #Windows
- From theory to practice: analysis and PoC development for CVE-2020-28018 (Use-After-Free in Exim) #MemoryCorruption
- CVE-2021-31166: HTTP Protocol Stack Remote Code Execution Vulnerability #RCE

- Exploit Development: CVE-2021-21551 – Dell 'dbutil_2_3.sys' Kernel Exploit Writeup & Exploit to SYSTEM #Kernel

Bug bounty writeups

- One-click reflected XSS in www.instagram.com due to unfiltered URI schemes leads to account takeover (Facebook, $9,600)
- Auth Bypass in https://nearbydevices-pa.googleapis.com (Google, $5,000)
- Just Gopher It: Escalating a Blind SSRF to RCE for $15k ($15,000)
- CVE-2021-27075: Microsoft Azure Vulnerability Allows Privilege Escalation and Leak of Private Data (Microsoft)
- Mass Assignment exploitation in the wild – Escalating privileges in style
- Counter-Strike Global Offsets: reliable remote code execution (Valve)

See more writeups on The list of bug bounty writeups.

Tools

- Unimap
- ugly-duckling & Intro: Lighweight Web scanner
- Nozaki: HTTP fuzzer engine security oriented
- VPS-web-hacking-tools: Automatically install some web hacking/bug bounty tools
- Domain Enumeration Tool (DET) & Intro: Perform Windows domain enumeration via LDAP

Misc. pentest & bug bounty resources

- Write-up factory
- LinkShare
- DogWhisperer's SharpHound Cheat Sheet
- External Pentest Checklist

Articles

- Send My: Arbitrary data transmission via Apple's Find My network
- Semgrep: scanning unusuals extensions
- Dumping Plaintext RDP credentials from svchost.exe
- Giving Azure a REST – Expanding REST API Capabilities

- bad_actor_poc: Exfiltrating secrets with Rust macros
- The Need to Protect Public AWS SSM Documents – What the Research Shows
- Humanity wastes about 500 years per day on CAPTCHAs. It's time to end this madness & Why Cloudflare's CAPTCHA replacement with FIDO2/WebAuthn is a really bad idea

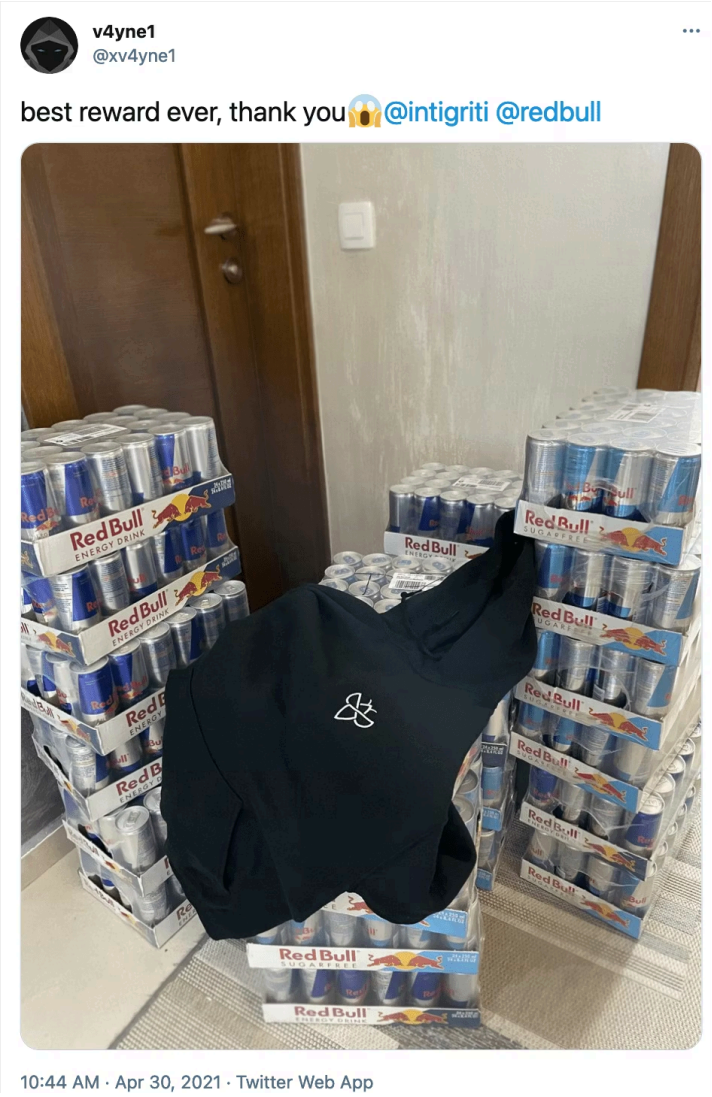
Bug bounty & Pentest news

- @nostarch Foundation Grants
- Upcoming events
  - Mayhem 2021
  - @albinowax's next talk at Black Hat USA: "HTTP/2: The Sequel is Always Worse"
- Tools updates
  - hashcat 6.2.0 update released
  - Custom tag filters added to BBRF
  - Ffuf now supports TLS SNI and Response time logging and filtering
  - mimikatz has a new command to check privileges of SCCM endpoints

Non technical

- Meet the hacker: 0xkasper, CTF player, Student, and hunter.
- Think outside the box with Satyam Gothi
- Determining Risk Less Badly

Community pick of the week



What a bug it must've been... Bravo, @xv4yne1!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!