Bug Bytes #132 – RCE on 12.7% of the Internet & Why you should turn off your password manager's autofill

BY ANNA HAMMOND · JULY 21, 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 July 12 to 19.

Our favorite 5 hacking items

1. Article of the week

You should turn off autofill in your password manager

@marektoth explored the autofill function of popular password managers. The results are not reassuring: "It is possible to steal the saved login credentials from 11 of the 16 tested browsers and password managers in one mouse click.".
This is worth knowing both as users (TL;DR: disable the autofill function) and hackers (XSS can be exploited to abuse the autofill feature and steal login credentials).

2. Writeups of the week

Remote code execution in cdnjs of Cloudflare (Cloudflare)
Diving into Dependabot along with a bug in npm (GitHub, $8,117)

@ryotkak discovered a Remote Code Execution via Path traversal on Cloudflare's cdnjs CDN library. It could have allowed attackers to tamper with 12.7% of all websites on the Internet.

Another interesting finding is @tyage's SSRF on GitHub's Dependabot and RCE in npm. It reads like an investigation starting with the observation that Dependabot is enabled by default and can make commits on many repositories.

3. Tool of the week

CDN

@vortexau's CDN is a Python script that compiles a list of subnets for major CDN and WAF providers. It runs every day and outputs results into a YAML file that you can use to quickly identify whether an IP belongs to a CDN of WAF.

This is a timesaver. I love this kind of tool/repo where the work is done once and everyone benefits from it.

4. Resources of the week

BugHuntr.io

Full-time bug hunter @ajxchapman launched a new training platform for bug hunters called bughuntr.io. Currently, it has 13 attack scenarios related to Web and Container/Docker hacking. They are free and range from beginner to expert level.
This is one platform I'm keeping an eye on as more scenarios, premium content and training are planned.

5. Non technical item of the week

Should you do Bug Bounties for a Living?

@codingo_ shares some interesting questions to consider before taking the plunge into full-time bug hunting. This is must reading if you're thinking about it and want to maximize your chances of success.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- HackerSploit: Docker Security Series, Part 1 & Part 2 (starting July 23)
- Hacker Heroes #5 – @rana__khalil (Interview) & Blog version
- Hacker Tools: Aquatone – Visualize your attack surface & Blog version
- Radio Hack Ep1: Red Teaming – Ahmed Sultan (in Arabic)

Podcasts

- REvil Vanishes! – Chrome Zero-Day Vulnerability, iOS WiFi SSID Bug, Patch Tuesday Review

Webinars

- OWASP July Lightning Event Featuring Ben Sadeghipour
- How to Build a Phishing Engagement – Coding TTP's

Conferences

- ACM WiSec 2021 & Schedule #WiFi

Tutorials

Medium to advanced

- Azure Persistence and Detection
- Nim on the Attack: Process Injection Using Nim and the Windows API
- Working Around macOS Privacy Controls in Red Team Ops & Interesting macOS Chrome Browser Files

Beginners corner

- Deep Link Exploitation: Introduction & Open/unvalidated Redirection & Exploiting Android WebView Vulnerabilities
- File Upload Attacks (Part 1) & Part 2
- Transport Layer Security: What Is New

Writeups

Challenge writeups

- Empires and Deserts #Deserialization
- SQL Injection – Lab #16 Blind SQL injection with out of band data exfiltration

Responsible(ish) disclosure writeups

- Possible RCE vulnerability in fail2ban #Linux #RCE
- CVE-2021-3438: 16 Years In Hiding – Millions of Printers Worldwide Vulnerable #Printers
- Server-Side Template Injection leading to unauthenticated Remote Code Execution in SCIMono – CVE-2021-21479 #Web
- Aruba in Chains: Chaining Vulnerabilities for Fun and Profit #Router
- Analysis of Satisfyer Toys: Discovering an Authentication Bypass with r2 and Frida #Android
- Bypassing Windows Hello Without Masks or Plastic Surgery #BiometricAuth

0-day & N-day vulnerabilities

- WooCommerce Unauthenticated SQL Injection Vulnerability #Web
- Meet WiFiDemon – iOS WiFi RCE 0-Day Vulnerability, and a Zero-Click Vulnerability That Was Silently Patched #iOS
- SeriousSAM bug impacts all Windows 10 versions released in the past 2.5 years #Windows

- Google TAG: How we protect users from 0-day attacks & Root causes analyses #Web #Browser #MemoryCorruption
- How the Kaseya VSA Zero Day Exploit Worked #Web
- Windows Print Spooler has a new unpatched Local Privilege Escalation (CVE-2021-34481) (PoC will be released at DEFCON)

Bug bounty writeups

- CVE-2021-22555: Turning \x00\x00 into 10000$ (Google, $10,000)
- Account Takeover + A Bonus Vulnerability
- RFD Vulnerability And Content-Disposition Header Bypass Story!
- Stored XSS in custom emoji (GitLab, $3,000)

See more writeups on The list of bug bounty writeups.

Tools

- cent: Community edition nuclei templates, a simple tool that allows you to organize all the Nuclei templates offered by the community in one place
- ppfuzz: Rust tool to scan for prototype pollution
- requests-ip-rotator: A Python library to utilize AWS API Gateway's large IP pool as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing
- SimpleAutoBurp: Python script to run burp scans from CLI using Burp's REST API
- Lepus: Python tool for enumerating subdomains, checking for subdomain takeovers and performing port scans

Tips & Tweets

- On-Site Request Forgery to bypass SameSite cookie
- GraphQL global CSRF by changing content type
- How to use DOM Invader to find JSON data structures automatically, See if a sink is vulnerable & Find more attack surface
- That time @pry0cc and @vict0ni found out how to use IPinfo.io API for free
- From odd filesize to authentication bypass
- Undocumented API endpoint in #AWS CloudShell to export IAM credentials

Misc. pentest & bug bounty resources

- BountyTricks
- HackerOne Hacker API tools
- Idiosyncrasies of the HTML parser
- @0xAwali's methodologies for testing Settings, SSO & 2FA
- Resources for anyone just getting started into bug bounties & @isira_adithya: My Bug Bounty Journey

Challenges

- defenselessV1: Just another vulnerable web application

Articles

- On SSRF (Server Side Request Forgery) or Simple Stuff Rodolfo Found — Part I
- XLS Entanglement, Whitepaper & Repo
- Failed SSH Lockout!

Bug bounty & Pentest news

- Bug bounty
  - How The Industry's First Hacker-powered API Helps Hackers Automate Workflows
  - Facebook: Launching Payout Time Bonus
  - Microsoft: Introducing Bounty Awards for Teams Mobile Applications Security Research
  - US offers $10 million reward for info on state-sponsored hackers disrupting critical infrastructure
- Cybersecurity
  - Forensic Methodology Report: How to catch NSO Group's Pegasus & Mobile Verification Toolkit
- Upcoming events
  - OWASP Nagpur Meetup #11 (Virtual) (July 25, feat. @zseano and @JR0ch17)
  - DEF CON 29 Red Team Village CTF, Red Team Village CyberWraith & #RedTeamTips
- Tool updates
  - Hakrawler now limits crawling to current host (use -subs to include subdomains) & Source tags aren't printed by default
  - Frida 15.0 Released

- Mitmproxy 7

Non technical

- Should you do Bug Bounties for a Living?
- Sliding Bounties and Why You Should Use Them
- GitHub: Our shared common weaknesses
- You ain't got no problem, Jules. I'm on the Multifactor.

Community pick of the week

Awesome! Enjoy your well-deserved vacation alicanact60

We love seeing you enjoy your bug bounty life! If you too have wins, swag and joys to share with other Bug Bytes readers, tag us on social media.