Bug Bytes #151 – The one where the Internet is on fire

BY ANNA HAMMOND · DECEMBER 15, 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 December 6 to 13.

Intigriti news

How Intigriti responded to the Log4j vulnerability

Our favorite 5 hacking items

1. Vulnerability of the week

Log4Shell a.k.a CVE-2021-44228

I came back to work from a long weekend only to find a deluge of information on this incredibly impactful RCE in Log4j.

For a quick introduction to the vulnerability, I recommended starting with this lunasec.io article and the first 15 minutes of this SANS video.
If you want more technical details, here is a list of resources I posted on GitHub: pentesterland/Log4Shell.

2. Vulnerability² of the week

CVE-2021-43798 – Path Traversal Vulnerability In Grafana, Grafana update & How to Identify and Exploit it

@j0v0x0 just published a writeup on how he discovered CVE-2021-43798 using source code review and Web fuzzing. It is a great read to understand the context behind the vulnerability.
If you're more interested in looking for it in pentest targets or bug bounty programs, check out @nahamsec's awesome video tutorial.

3. Writeup of the week

Don't Reply: A Clever Phishing Method In Apple's Mail App (Apple, $5,000)

$5k for a bug bounty report on *phishing*, that's not so common! It is understandable though. @jon_bottarini got a hint from @samwcyo that it was possible (at the time) to load PHP files inside `<img>` tags. This behavior could be exploited to create extremely credible phishing emails targetting Apple Mail.

4. Video of the week

How hackers pollute your code.

@PwnFunction is back with a new video on prototype pollution. As usual, a very informative and clear explanation of an interesting bug class.

5. Webinar of the week

Ed Theory for Hackers: What a Teacher Wants Infosec to Know | Michael Taggart

If you're struggling with the high learning curve in InfoSec, you will find this webinar enlightening. It is about learning how to learn, creating a learning plan, and common pitfalls that might be hindering your progress.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- I opened on a malicious email attachment.. and this is what happened!
- Command injection vulnerability in source code & Blog post
- Update requests with rotated session after user logs out | Burp Suite Pro | Cookies & Authorization
- #MentorshipMondays | Mental Health for Hackers!

Webinars

- Cracking Android PINs

Tutorials

- XMPP: An Under-appreciated Attack Surface
- Introduction to Request Smuggling
- Practical Introduction to CodeQL
- Common vulnerabilities in Java and how to fix them
- Developing with VBA for Script Kiddies — TrustedSec

Writeups

Challenge writeups

- Cyber Santa is Coming to Town – Hacking Party
- How to search for IDORs!, What is Clickjacking? & Exploiting an SSRF vulnerability
- Metasploit Community CTF 2021 WriteUp
- HackTheBox – Writer

Responsible(ish) disclosure writeups

- The Hacker Recipes: sAMAccountName spoofing, CVE-2021-42287/CVE-2021-42278 Weaponisation, noPac & WazeHell/sam-the-admin
- ModSecurity DoS Vulnerability in JSON Parsing (CVE-2021-42717)
- Bypassing Box's Time-based One-Time Password MFA

Bug bounty writeups

- A phishing document signed by Microsoft – part 1 (Microsoft)
- Bypass a fix for report #708013 (Login bruteforce) (Shopify, $3,500)
- My mindset while hunting on Yandex and my SSRF (Yandex)

See more writeups on The list of bug bounty writeups.

Tools

- HeySerial & Intro: Systematically Hunting for Deserialization Exploits
- whoc: A container image that exfiltrates the underlying container runtime to a remote server
- SAPP (Static Analysis Post Processor): Takes the raw results of Facebook's static analysis tool Pysa, and makes them explorable both through a CLI and a web UI

- Dependency Combobulator: Open-Source, modular and extensible framework to detect and prevent dependency confusion leakage and potential attacks
- GoTestWAF: Golang project to test different WAFs for detection logic and bypasses

Tips & Tweets

- Springboot >2.2.6.RELEASE behavior that can be used to bypass path traversal allowlists
- JSON payload blocked by WAF? Change the Content-Type!
- If a server reflects the Connection or Keep-Alive header over HTTP/2, it might be used for cache-poisoning DoS against Safari
- Certified Practitioner exam prep tips
- Using fff to quickly fetch a list of URLs in CLI, while adding them to Burp
- Some things to look for in JavaScript files

Misc. pentest & bug bounty resources

- Cloud Service Provider security mistakes
- RegexLearn
- WiFi Penetration Testing Cheat Sheet
- Awesome-Cloud-PenTest

Articles

- Microsoft and GitHub OAuth Implementation Vulnerabilities Lead to Redirection Attacks
- How Acunetix addresses HTTP/2 vulnerabilities
- The hidden side of Seclogon part 2: Abusing leaked handles to dump LSASS memory

Challenges

- h1-ctf (ends on December 23)
- KringleCon 2021
- Cracked Flask Lab & Walkthrough

Bug bounty & Pentest news

- Bug bounty
  - Visma's Bug Bounty Christmas campaign

    - WebAssembly and Back Again: Fine-Grained Sandboxing in Firefox 95
- Cybersecurity
    - OSCP Exam Change
    - OWASP ModSecurity Core Rule Set sandbox launched to help security researchers test new CVEs
- Tool updates
    - Second Order v3.0 & v3.1 (major rewrite)
    - pimps/JNDI-Exploit-Kit
    - Ghidra 10.1

Non technical

- Cognitive Biases and Penetration Testing
- Graph Theory for an Ethical Hacker