Bug Bytes #145 – How to Make a Million in 4 Years, CookieMonster & Threats to CI/CD Pipelines

BY ANNA HAMMOND · NOVEMBER 3, 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 October 25 to November 1.

Our favorite 5 hacking items

1. Resource of the week

Common Threat Matrix for CI/CD Pipeline & Attacking and Securing CI/CD Pipeline

We've seen some amazing writeups involving CI/DC pipelines recently. Their attack surface is large, they are trendy, and they can lead to serious suppy chain attacks which makes them a good target for attackers.
So, if you want to learn about CI/DC security (from both a defender and attacker standpoints), this new threat matrix by @rung is a great resource.

2. Writeup of the week

Tortellini in Brodobuf

While testing Web apps, you might encounter strings that seem to be base64 encoded but can't be decoded properly because they're actually Protobuf serialized data that is encoded in Base64. Not knowing about this serialization format can make you miss critical vulnerabilities.
That's what this writeup is all about: An excellent introduction to Protobuf, how to decode and deserialize Protobuf data, exploit this entry point for SQL injection and how to create a SQLmap tamper script to automate the process.

3. Tools of the week

CookieMonster & Intro
jolokia-exploitation-toolkit (JET) & Tutorial

CookieMonster is a Go tool/API that automates testing for vulnerabilities in stateless authentication. It supports several frameworks and helped @iangcarroll find bugs in many large bug bounty programs.
If you want to automate your testing even further and mass-scan targets, @naglinagli suggests combining it with his Cookies-extractor.

@TheLaluka released Jolokia Exploitation Toolkit, a Python tool that helps exploit exposed Jolokia endpoints. The accompanying article goes over detail on how to use it to get RCE on a Tomcat/Catalina server. This can be handy if you want to escalate an SSRF that allows to reach an internal Jolokia endpoint, to RCE.

4. Tutorial of the week

Android security checklist: WebView

This is a great tutorial on how to attack and protext WebView on Android. It includes different exploitation techniques, ways to increase the impact of attacks, and lots of details.

5. Non technical items of the week

How to Start Bug Bounties 101 & How to Make a Million in 4 Years
Creativity, Self-Doubt & Doing Remarkable Work

If you wonder how hackers like @ozgur_bbh and @s0md3v do their magic, I recommend reading these articles they wrote.
The TL;DR is *there is no magic*, "Just work.". However, it is still interesting to hear what they have to say on the topic, the mindset and steps they took that made all the difference.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Hack The Box Hacking Battlegrounds Streamed Tournament #2 – Commentated by IppSec and John Hammond
- HackerSploit: Red Team Security Series Part 1: Caldera, Reconnaissance, Luckystrike & PowerShell Empire & Part 2

Webinars

- BHIS | Hack for Show, Report For Dough: Part 2 w/ BB King

Conferences

- Hacking AWS end-to-end – remastered
- Texas Cyber Summit & Spanish track

Tutorials

Medium to advanced

- 5 Ways to Exploit a Domain Takeover Vulnerability
- Create a proxy DLL with artifact kit
- Utilizing Programmatic Identifiers (ProgIDs) for UAC Bypasses

Beginners corner

- Analyzing Java Heap Dumps via OQL queries
- What can I do with Open Redirect with OAuth?
- Defeating Android Certificate Pinning with Frida & frida-android-unpinning

Writeups

Challenge writeups

- Browser, what are you doing?! Solution to October '21 XSS Challenge
- [ECW] Red Team Challenge Write Up
- HTB: Explore (The first Android box on HTB)
- This bug doesn't exist on x86: Exploiting an ARM-only race condition
- How to search for XXE!
- Photographer Walkthrough with S1REN

Pentest writeups

- Finding Gadgets Like It's 2015: Part 2

Responsible(ish) disclosure writeups

- Sitecore Experience Platform Pre-Auth RCE #Web #CodeReview
- Agent 007: Pre-Auth Takeover of Build Pipelines in GoCD #CI/CD #Web
- Finding An Unauthenticated RCE Vulnerability In MovableType :: CVE-2021-20837/JVN#41119755 #Web #Perl #CodeReview
- 50 Shades of SolarWinds Orion (Patch Manager) Deserialization (Final Part: CVE-2021–35218) #Web
- 1,000,000 Sites Affected by OptinMonster Vulnerabilities #Web #CodeReview
- Zimbra "nginx" Local Root Exploit & Zimbra "zmslapd" Local Root Exploit. #Linux #LPE

N-day vulnerabilities

- CVE-2021-22205: Rapid7 analysis & Nuclei template #Web (the Gitlab / Exiftool RCE thought to be unauthenticated is actually a pre-auth RCE)

- NGINX Custom Snippets CVE-2021-25742 #Kubernetes
- Unauthenticated Remote Code Execution (RCE) vulnerability in Hikvision IP camera/NVR firmware (CVE-2021-36260) & Nuclei template #IoT

Bug bounty writeups

- Apple XAR – Arbitrary File Write (CVE-2021-30833) (Apple)
- A journey from XML External Entity (XXE) to NTLM hashes!
- Write Up – XSS Stored In api.media.atlassian.com Via Doc File (iOS) (Atlassian)
- Microsoft finds new macOS vulnerability, Shrootless, that could bypass System Integrity Protection (Apple)
- This is how i was able to Permanently Crash all Mapillary users within minutes
- Use-After-Free in Voice Control: CVE-2021-30902 Write-up (Apple)
- Image queue default key of 'None' and GraphQL unhandled type exception (Reddit, $500)

See more writeups on The list of bug bounty writeups.

Tools

- Web Cache Vulnerability Scanner (WCVS) & Intro: Go tool for testing for web cache poisoning
- Quiet Riot & Intro: A Scalable AWS Enumeration and Footprinting Tool
- Frogy: Subdomain enum tool

Tips & Tweets

- If you have trouble reversing Hermes bytecode in a React Native Android app, check the iOS version instead
- Some useful Burp hotkeys
- How to load an openapi.json file (based on v3 specification) into Burp & Useful converters
- Did you know you can do WHOIS lookups on IP addresses and ASN numbers, not just domain names?
- Hackvertor AMF tags

Misc. pentest & bug bounty resources

- Mobile Application Penetration Testing (TCM Academy course) ($29.99)
- Privilege Escalation Techniques: Learn the art of exploiting Windows and Linux systems & Introductory video (Starting at $31.19)

- Offensive-Resources V2
- GoSecure's Presentation Material
- XXE – XML External Entity Attack flyer

Challenges

- Air pollution challenge
- Damn Vulnerable NodeJS Application
- DUNGEON – BSides Ahmedabad CTF 2021 (November 6-7)

Articles

- Bypassing ModSecurity WAF
- Attacking Azure & Azure AD, Part II
- Enumerating Services in AWS Accounts in an Anonymous and Unauthenticated Manner
- Cracking WiFi at Scale with One Simple Trick
- From Zero to Domain Admin

Bug bounty & Pentest news

- Bug bounty
  - @MrTuxracer's inspiring bug bounty October stats
  - Polygon pays out record $2 million bug bounty reward for critical vulnerability
  - Google: Trick & Treat! Paying Leets and Sweets for Linux Kernel privescs and k8s escapes
  - Gitlab: Our 3rd annual bug bounty contest: the swagtastic sequel to the sequel
- Upcoming events
  - Blackhoodie at GreHack 2021 – Virtual (Novemver 10)
  - Announcing the DEF CON 30 Call For Contests & Events!
- Tool updates
  - Improvements to Burp Suite authenticated scanning & DOM Invader improvements + Line wrapping support added
  - Impacket v0.9.24 Released

Non technical

- Formalized Curiosity

- How to start reviewing code?
- The polar bear method: How to find bugs, only source and windbg