Bug Bytes #162 – How to read RFCs, Param Miner doc & SSRF with browser exploitation

BY ANNA HAMMOND · MARCH 9, 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 February 28 to March 7.

Intigriti news

1337UP LIVE

CTF SIGN UP Virtual Conference

The **1337UP LIVE** event is nearing! Only 2 more days to go!

On March 11th, we will kick off with the 24-hour long CTF with challenges from web all the way to binary exploitation. Sign up right now at ctf.intigriti.io.

On March 12th, once the CTF ends, we will directly jump into the live bug bounty conference with astonishing talks by amazing speakers. Check out the line-up over here at www.intigriti.com/1337uplive!

We can't wait to see you there!

Win some swag!

We're inviting you to share your opinions!

As a community-driven platform, your feedback is extremely valuable to us. To get to know you better, we would like to ask you to fill out our five-minute survey. At the end of the survey, you will be able to participate in our raffle to win a **€50 Intigriti swag voucher (there are 20 available)**. Looking forward to hearing from you!

Take the survey

Our favorite 5 hacking items

1. Articles of the week

Reading RFCs for bug bounty hunters
The perils of the "real" client IP

@EdOverflow who knows a thing or two about RFCs (as the author of security.txt), shares some tips on reading RFCs for bug hunters.
This is actually part of a new Q&A blog series. This is a fantastic opportunity to have your bug bounty / security questions answered by a seasoned security researcher.

The second article is about how to retrieve the "real client IP address" from HTTP headers, common misconfigurations and the vulnerabilities they lead to. It is a long but excellent read if you want to explore this area of security.
Another good article on the same blog is about bypassing timing attack mitigations.
As pointed out by @albinowax, when you find a good article, make sure to browse the entire site for other gems.

2. Writeups of the week

Circumventing Browser Security Mechanisms For SSRF
AutoWarp: Critical Cross-Account Vulnerability in Microsoft Azure Automation Service
The Dirty Pipe Vulnerability & PoC

A few months ago, I saw a very intriguing tweet about a bug bounty finding that involved Web and Pwn. @iamnoooob, @rootxharsh and @S1r1u5_ just dropped the writeup, and it is indeed incredible.
The team chained an SSRF with XSS to bypass some limitations, and with a known headless Chrome RCE that didn't have any public PoC.

Another equally impressive finding is @Yanir_'s AutoWarp. He found a way to interact with an internal Azure server, which gave them access to authentication tokens of other customers and the ability to take over their accounts.

The third writeup is about a privilege escalation that Max Kellermann discovered in the Linux kernel since version 5.8. It is similar to Dirty Cow but easier to exploit.
If you are interested in this type of bugs, I highly recommend the writeup. It details everything from the indicators of vulnerability, questions the author asked themselves at each step, what worked and what didn't... just like an investigation.

3. Resource of the week

param-miner-doc

Param Miner's Attack Config options are not officially documented. So, to understand what they mean, @_nikitastupin looked at the tool's source code and compiled their descriptions in a repo.

4. Tool of the week

Padding Oracle Hunter

@spaceraccoonsec's colleague released this new tool to detect and exploit padding oracle vulnerabilities. It is a Burp extension that supports the PKCS#7 and PKCS#1 v1.5 padding schemes.
If you're not sure where to use this tool, here is a tip on identifying potential entry points.

5. Video of the week

Finding 0day in Apache APISIX During CTF (CVE-2022-24112)

@LiveOverflow published a new video walkthrough of a Real World CTF challenge. This one is about a 0-day RCE in the default configuration of Apache APISIX. Discovering it involved code review, reading documentation, spoofing the "real" client IP, and much more. As usual, it is incredibly informative.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- BOUNTY THURSDAYS – LIVE #2 (NEWS/TOOLS and Community Questions with Jason Haddix)
- Bug Bounty | $1870 for blind command injection & Lab
- Chilling – let's find a program to look at
- Bug Bounty 2022 Guide: Where to focus // Money // Get started
- TheXSSRat Talks About Hacking, Creating Content, Security Certificates and API Hacking

- admin:admin password allowed stealing Teslas around the world & Original report
- Ghidra – Pwn Zero To Hero 0x02

Webinars

- ZAP Automation in CICD

Conferences

- NSEC2021 – Philippe Arteau – Request Smuggling 101
- Evelyn Lam – Authentication challenges in SaaS integration and Cloud transformation

Tutorials

- Weakly Typed SQL Injection
- Gitlab Reconnaissance Introduction
- Bash Tricks for File Exfiltration over HTTP/S using Flask
- Manipulating User Passwords Without Mimikatz
- Give Me Some (macOS) Context...

Writeups

Challenge writeups

- HackTheBox – Hancliffe & EXE Analysis with Ghidra]
- Hackerone Android Challenges Writeups
- Time-Based Blind SQL Injection!

Pentest writeups

- Authentication bypass due to weak verification of SAML Token

Responsible(ish) disclosure writeups

- CVE-2022-24948: Apache JSPWiki preauth Stored XSS to ATO
- CVE-2022-24990: TerraMaster TOS unauthenticated remote command execution via PHP Object Instantiation #CodeReview

Bug bounty writeups

- More secure Facebook Canvas Part 2: More Account Takeovers (Meta / Facebook, $98,250)

- CVE-2022-22947: SpEL Casting And Evil Beans
- Piercing the Cloud Armor – The 8KB bypass in Google Cloud Platform WAF (Google)
- Moodle 2nd Order SQLi (Moodle)
- Password Reset to Admin Access

See more writeups on The list of bug bounty writeups.

Tools

- Uncover: Quickly discover exposed hosts on the internet using multiple search engines
- dontgo403
- HaxUnit: Python wrapper around Project Discovery tools (combining subdomain enumeration, port scanning and vulnerability discovery tools)
- Vajra: GUI tool with multiple techniques for attacking and enumerating in the target's Azure environment
- sdlookup: IP Lookups for Open Ports and Vulnerabilities from internetdb.shodan.io

Tips & Tweets

- Burp Collaborator riddle
- Forcing an app to use XHR instead of WebSockets
- SSRF via WEBSERVICE function in spreadsheets
- Using x55.is to load any JS file inside a domain for XSS
- @d0nutptr on reading the tech blogs of major companies
- Bash tricks for hackers
- RCE via a malicious README

Misc. pentest & bug bounty resources

- Inventory
- Repository of CVEs found by Orange Cyberdefense people
- How do I get Started in Cyber Security? — My Perspective & Learning Path!
- Angular + React: Vulnerability Cheatsheet

Articles

- Finding an Authorization Bypass on my Own Website
- Rust FFI – Fuzzing Like a (much faster) Caveman & Repo
- TCP Middlebox Reflection: Coming to a DDoS Near You
- Escaping privileged containers for fun

Challenges

- 1337UP LIVE CTF (March 11)

Bug bounty & Pentest news

- Bug bounty
  - Cloudflare's Always Online and the Internet Archive Team Up to Fight Origin Errors
- Cybersecurity
  - We're 'firefighters' for victims of armed conflict – Hackers Without Borders co-founder on NGO's timely arrival
  - Cybercriminals who breached Nvidia issue one of the most unusual demands ever
- Tool updates
  - Feroxbuster 2.6.0
  - Go 1.17.8 and 1.16.15 are released (fixed CVE-2022-24921)
  - CrackMapExec now supports RDP protocol

Non technical

- The State of Secrets Sprawl 2022
- 3 female hackers inspiring the next generation of infosec talent