Bug Bytes #192 – Post-recon blues, a lesson in Rust and fuzzing open source

BY TRAVISINTIGRITI · FEBRUARY 15, 2023 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The second series is curated by InsiderPhD. Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the weeks from February 6th to February 12th

CLICK HERE TO SUBSCRIBE

Intigriti News

- Weekly code snippet challenge! and then the solution
- Ubisoft join us with their VDP why not take a look and skill up your game hacking?
- New scope and double bounties, what else do you want? itsmeDigitalID has a had a major app update and is inviting all BE/NL citizens to report vulnerabilities. Promotion runs until Feb 19th, so be quick!
- Our heart goes out to everyone impacted by the Turkey-Syria earthquake. You can now donate your bounties to the 1212 relief fund by changing your default invoice details to DONATE-1212.

From my notebook

Hi everyone! I'm back! I took 2 weeks off while I adjusted to the new semester here. inthe UK, but we're back so let's check out this week's top 5...

1. CyberSecurity Journey With @HarshBothra | Hacker2Hacker | SSRF
2. PHP Filter Injection: LFI2RCE Explained
3. A deep dive into certificates
4. Solving a VM-based CTF challenge without solving it properly
5. What Should You Do After Recon?!

Other Amazing Things

Videos

- How to Bug Bounty in 2023
- Web Application Hacking – File Upload Attacks Explained
- BeVigil || OSINT and Bugbounty
- Why Police Hacked this Messaging App
- ChatGPT Built Me a Hacking Tool...
- How Hackers Run For The Money!
- Malicious LNK File Analysis
- Cracking JSON Web Tokens
- $1mln – Generating ETH from thin air – Aurora rainbow bridge
- Computer Hacking – Gartner Peer Insights DOM XSS
- Why you should try bug bounty hunting with application analysis!
- @PatrickAlphaC Web3 Education, Auditing and Advice for New Engineers in Web3

Podcasts

- Episode 362 – A lesson in Rust from Carol Nichols
- 186 – An XNU Exploit and a Chrome Heap Overflow
- 185 – Facebook Account Takeovers and a vBulletin RCE
- EP 107 How Google Secures It's Google Cloud Usage at Massive Scale
- Episode 361 – GitHub got pwnt, but it wasn't very exciting

- Sounds like someone is looking at your data closely... Protip: Host your own instance of xsshunter-express or ezxss to avoid leaking potentially sensitive data to this company. – MrTuxRacer
- Announcing Nuclei Cloud – SaaS platform built on the top of Nuclei – @emgeekboy
- Hey fam, What are some of the best shodan resources you all have seen? – @Jhaddix
- If you were restricted to only using one tool to perform subdomain discovery, which of these would you choose? @gregxsunday
- Hackvertor autocompletion in action – @garethheyes

- OWASP Top 10: A Guide for Pen-Testers & Bug Bounty Hunters
- Understanding SSL—Secure Socket Layer | 2023
- ARE SMART CONTRACTS REALLY SMART?
- BROKEN FUNCTION LEVEL AUTHORIZATION [API SECURITY—0x2]
- WHEN CLUSTERING MEETS CYBER-SECURITY
- ASSOCIATION RULE MINING
- How to test Exposed API Keys using Nuclei
- Securing Azure: Hunting with AzureHound
- SameSite Lax Bypass through Method Override | 2023
- Broken Access Control: Understanding and Finding Issue
- Hacking XML—XML Injection
- Cryptography for Blockchain Security
- The Role of Hash Functions in Cryptography
- SSRF—Server Side Request Forgery

- Creating and Winning a Capture the Flag Challenge
- Basic server-side template injection (code context) | 2023
- Creating your own tools to hunt bugs, a power often neglected
- NULL Pointer Dereference [CWE-476]
- Attacking and securing Docker containers

- Logic Error Bug Fix Review
- Bypassing SameSite=lax cookie restrictions to preform CSRF resulting to a horizontal privilege
- Blind Time-based SQL injection vulnerability in an Indian government website
- SSRF That Allowed Us to Access Whole Infra Web Services and Many More
- IDOR Leads to MASS Account Takeover
- HubSpot Full Account Takeover in Bug Bounty
- [BUG BOUNTY] SUBDOMAIN TAKEOVER IN TARGET CNAME GHOST.IO
- We Hacked GitHub for a Month
- How I Was Able to Takeover User Accounts via CSRF on an E-Commerce Website
- Disabling js for the win
- Making $500 by flipping a 0 to 1
- The truth behind the 3rd argument for exploiting the Webexservice
- Information disclosure or GDPR breach? A Google tale...
- How I got a $2000 bounty with RXSS
- Bug Bounty Hunting 101, Js files Diving.
- Finding Treasures in Github and Exploiting AWS for Fun and Profit— Part 1
- Fuzz Open Source, Get Paid by Google
- Reflected XSS on Target with tough WAF (WAF Bypass)

- Chaining Bugs to get my First Bug Bounty
- Debugging a Windows Service in User-Mode
- BlueKeep in details
- Does it really helps? Partially redacting account numbers contained in the credit report.
- SSRF in redacted.com: How I Found and Reported a Vulnerability
- Bypassing API Restrictions for Fun and Profit
- Deserialization of untrusted data—[502]
- ROP chains on ARM64
- OTP Bypass By Response Manipulation
- Easy Account Takeover on dell subdomain
- WHy are you getting Indexed by Web Crawlers on the Intranet

- Firefly: a smart black-box fuzzer for web applications testing
- DNSrecon-gui – DNSrecon Tool With GUI For Kali Linux
- S3BucketList – Firefox plugin that lists Amazon S3 Buckets found in requests.
- InQL – Burp Extension for GraphQL Security Testing.

- XSS WAF bypasses
- XNL's toolkit
- Double encode LFI payloads

- Googledorking for pastebin