Bug Bytes #187 – NahamCon, IWCon, Hacking Misconceptions, Scaling Recon and Jason's Pentest

BY TRAVISINTIGRITI · DECEMBER 28, 2022 · 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 December 12th until December 25th.

Click here to subscribe

Intigriti News

- Happy holidays from the Intigriti team!
- Spot the vulnerability from our code snippet and the solution
- Mini-CTF
- Cryptocat will be joining Intigriti!

From my notebook

1. NahamCon EU 2022: A Free Virtual Offensive Security Conference – NahamCon's first regional conference, focusing on the EU/India timezones and hosted by InsiderPhD and Farah Hawa. Tons of great talks but here are the 3 available at the moment!
    - #NahamCon2022EU: Command-Line Data-Wrangling by Tomnomnom
    - #NahamCon2022EU: RTFR (Read The Bleeping RFC)" by securinti
    - #NahamCon2022EU: Story of an RCE on Apple Through Hot Jar Swapping by Frans Rosen
2. IWCon 2022 – IWCon was just the week after and again a fantastic conference, no videos yet but some speakers have shared their slides!
    - Recon Skills and Tips by God Father Orwa
    - Pwning Admin Panels Methodology by Ahsan Khan
    - Starting into Smart Contract Security by CredSheilds
    - Hacking Cloud: For Fun and Profit by Hacking Cloud: For Fun and Profit by Dhiyaneshwaran
3. I Hope This Sticks: Analyzing ClipboardEvent Listeners for Stored XSS. When is copy-paste payloads not self-XSS? – Technically this was a talk at NahamCon so this is kinda a 2-for-1 but this

write up by SpaceRacoon looks at event listeners and stored XSS

4. CVE-2022-42710: A journey through XXE to Stored-XSS – Follow Omar as they find CVE-2022-42710
5. Hacker Gift Giving ideas by insiderPhD – I put together some threads if anyone is looking for last minute gifts for their hacker friends, I've summarised it in 3 categories, IRL stuff you can wrap, virtual gifts and books
    - Stuff
    - Virtual
    - Books

Other Amazing Things

- Ethical Hacking in 15 Hours – 2023 Edition – Learn to Hack! (Part 2)
- Which XSS payloads get the biggest bounties? – Case study
- What is a Protocol? (Deepdive)
- 2022 Vegas Bug Bash with Bugcrowd
- Web Sec Academy – What should we do?
- Web OSINT
- I Was Scammed With 800 MicroSD cards
- HackTheBox Certified Penetration Testing Specialist (CPTS) – Review.
- Revisiting 2b2t Tamed Animal Coordinate Exploit
- How I connect my automation to a database! (Automation Series)
- How I scale my containerized bug bounty automation! (Automation Series)
- Bug Bounty – Hackerone Hacktivity / Bug Bounty Platforms / How to find more Bug Bounty Programs

- 130: Jason's Pen Test
- Domain Naming System (DNS) (noun) [Word Notes]
- 175 – Pwn2Own Bugs and WAF Bypasses
- 176 – JS Type Confusions and Bringing Back Stack Attacks
- AWS REINVENT 2022 RECAP FOR CLOUD SECURITY PROFESSIONALS
- 302: Lensa AI, and a dog called Bob
- NO. 362 | Dependency Scanner, Citrix Attacks, AI Analysis
- SN 902: A Generic WAF Bypass – Pwn2Own Toronto, URSNIF malware, Vivaldi Mastodon support, Bye Bye SHA-1

- Hacking misconceptions: Hacking is way easier and harder than you think.
- My information caption system
- JavaScript for hackers
- Trigger your friends in one sentence
- AI art discussion
- Favourite Cybersecurity YouTubers

- AWS security services—Start with IAM
- Using an Android emulator for API hacking

- Write-up: SQL injection with filter bypass via XML encoding @ PortSwigger Academy
- Portswigger Lab: JWT authentication bypass via algorithm confusion with no exposed key
- CVE-2019–6238: Apple XAR directory traversal vulnerability
- SUBDOMAIN ENUMERATION
- Hacking server using SSTI
- XML External Entity (XXE) Injection Payload List
- Directory Payload List via PayloadBox
- Getting Started With 5 Bugs part(1)
- Explaining Vulnerabilities : Broken Access Control
- How To Exploit File Inclusion Vulnerabilities: A Beginner's Introduction.—StackZero
- How to Informe an Organization about a Security Vulnerability
- How to create nuclei templates?
- Param Hunting to Injections
- Getting Started with Reverse Engineering
- Burp Suite Extension Development
- Everything about Cookie and Its Security
- How Capabilities actually Work ? | Exploitation | Privilege Escalation
- Our Top 5 favorites Mobile Hacking Tools
- Katana Framework: How To Use It To Scan And Mass Collect Website Data
- Everything about Docker Security
- Bypass Apple's redirection process with the dot (".") character
- Race conditions : bug bounties

- Payment Gateway Bypass on Government Domain.

- PII data exfiltration within minutes
- IDOR allows updating user profiles, leading to full account takeover. | Part 02
- Doing it the researcher's way: How I Managed to Get SSTI (Server Side Template Injection)
- Lack of Rate Limiting
- Privilege escalation leads to deleting other user's account and company Workspace [Access Control]
- No Rate Limit on Forget Password CodingStudio.id
- Introspection GraphQL on Sayurbox.com
- XSS Reflected on Bukalapak.com
- Sensitive Information Disclosure on bukalapak.com
- XSS Stored on JD.id
- Bypass Admin Panel Using Google & fetch all Users Data [Data Breach]
- Simple CORS misconfig leads to disclose the sensitive token worth of $$$
- Amazon vulnerability that can flood user's mailbox.
- How I was able to steal users credentials via Swagger UI DOM-XSS
- [GraphQL IDOR]Leaking credit card information of 1000s of users
- Destroying the Scammers Portal—SBI Scam
- Directory Traversal Vulnerability in Huawei HG255s Products
- How I found my first RCE? A simple one...
- In this article, I'll tell you how I got a 4 digits( ) bounty from an Indian company.
- 0 click Account Takeover and Two-Factor Authentication Bypass
- RCE on admin panel of web3 website
- Zero Click To Account Takeover (IDOR + XSS)
- My First Bug in Bugcrowd
- Hack Analysis: Omni Protocol, July 2022
- blockchain | Immunefi | smart contract auditing | C4
- How these IDOR vulnerability earned 5000$ | Hackerone Reddit Bug Bounty
- $350 XSS in 15 minutes
- CRLF Injection—xxx$—How was it possible for me to earn a bounty with the Cloudflare WAF?

- Offsec.tools
- S3Crets_Scanner – Hunting For Secrets Uploaded To Public S3 Buckets
- Octosuite – Advanced Github OSINT Framework
- HTTPLoot – An Automated Tool Which Can Simultaneously Crawl, Fill Forms, Trigger Error/Debug Pages And "Loot" Secrets Out Of The Client-Facing Code Of Sites
- 10 Practical Recon & vulnerability Scanners for bug hunters (part two)

- A javascript bookmarklet that will extract all endpoints (starting with /) from your current DOM and from all the all the external script sources embedded on the page.
- The reality is that if you aren't where you want to be financially or professionally and you get caught up wasting your time playing video games, or any other time sink instead of putting the hours in you have nobody to blame but yourself.
- Shodan for educational use
- Portswigger XSS Cheatsheet!
- TakSec's favorite Google dork flow and part 2
- TakSec's favorite recon tools
- Open redirect to account takeover
- XSS via URL encoded ASCII tab characters

Challenges

- Advent of Cyber 2022: Day 15 Santa is looking for a Sidekick
- Advent of Cyber 2022: Day 16 SQLi's the king, the carolers sing
- Advent of Cyber 2022: Day 17 Filtering for Order Amidst Chaos
- Hardware Hacking! Day 19 – TryHackMe Advent of Cyber
- Do You Need Attack Surface Reduction? (Advent of Cyber Day 22 2022)
- Capture The Flag! NahamCon EU CTF "MMORPG"
- Start Hacking with the HEARTBLEED vulnerability: NahamCon CTF
- Filter Evasion in a REVERSE SHELL (no spaces!!)
- HackTheBox UniCTF 2022 Talk – Variable is what you make of It

Bug bounty/Pentest news

- ONLYOFFICE on HackerOne: 2022 overview