Bug Bytes #204 – Everything You Missed From NahamCon

BY TRAVISINTIGRITI · JUNE 21, 2023 · LAST UPDATED ON APRIL 1, 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 week from June 12th to June 18th

Click here to subscribe

Intigriti News

- Did you know a new JWT Attack was recently published?!
- What's your favourite Burpsuite plugin?

From my notebook

So this week and weekend saw the return of NahamCon and there were some great talks on the main programme and the villages on Saturday, the talks are still being uploaded so we'll update you when they're all available but here's what's been released so far...

1. #NahamCon2023: Bug Bounty Village | Free Workshops | !discord
2. NahamCon x RTV 1 and NahamCon x RTV 2
3. NahamCon CTF 2023: Web Challenge Walkthroughs
4. Automation tricks for Burp Suite Pro – Agarri_FR
5. Going Beyond Microsoft IIS Short File Name Disclosure – NahamCon 2023 Edition
6. How to Properly Own API's for Your First Valid Submission
7. NAHAMCON 2023
8. Nahamcon [The Power of Shodan Leveraging Shodan for Critical Vulnerabilities]

- How To Extract Plaintext Google Chrome Passwords
- the CHEAPEST path to becoming an ethical hacker
- STEP BY STEP WEBAPP HACKING RESOURCES
- Fireside Chat with John Hammond | Security Researching
- How to do account takeover? Case study of 146 bug bounty reports
- Web App Hacking: File inclusion attacks
- Bypassing Branch Protections with Github Actions (CI/CD)
- Creating VMs with Vagrant
- SQL Injection Beginner Crash Course
- Autorize in 30 Seconds! (shorts)
- Ask a Hacker Anything with Nerdwell
- Building Ippsec's Parrot VM – How to Run the Playbook.
- HackTheBox – Escape
- picoCTF – Rapid Solves! – Live Walkthrough
- Configuring Burpsuite and Firefox via Ansible
- Amazingly simple $100k login bypass on Apple (shorts)
- Genymotion – Proxying Android App Traffic Through Burp Suite | Cameron Cartier

- Episode 379 – Will open source save the world, again?
- NO. 386 — DBIR 2023, Vision, Smol-Developer, and more...
- Talking AI and Content Creation with Daniel Miessler
- Raul Rojas: Navigating the AI-infused Security Landscape
- Right Royal security threats and MOVEit mayhem
- Episode 23: Hacker Loadouts

- Just withdrew my #DEFCON31 talk because the US continues to deny my ESTA application. This looks like another form of occupational hazard for security researchers
- Sometimes you win, Sometimes you lose
- given up on random text files, all my notes are now in burp tab titles
- I still see hackers and bug hunters debating this with triagers or programs so I'm reposting my blog from late last year.
- SAML vulns are always intriguing!
- I continually underestimate how beneficial it is to go for scope that others avoid.

- Beginner
  - NUCLEI101 FOR BUG BOUNTY CHEATSHEET
  - Securing Your Infra: Exploring Nuclei's Defense Arsenal
  - Decoding Log4j : What You Need to Know
  - Exposed Postman Collections
  - Learn How hackers hack Databases (PART 1) & Learn How Hackers hack Databases (PART 2)
- Intermediate
  - Understanding Prototype Pollution and its Exploitation—Part 2
  - Find all Hidden website of Hosted on Server !
  - Process Injection Series Part I: PE Injection
  - Comprehensive Guide to (CSRF) Testing with Python
  - How improper OTP implementation could lead to Account Take Over (Part 3)
  - A guide to DNS takeovers
- Advanced
  - Detecting, Fixing, and Defending Against XXE Attacks in Python and Java

- PowerShell Reverse Shell via Social-Engineering-Toolkit
- Recreating Cordova Mobile Apps to Bypass Security Implementations
- Kubernetes pentest—Bypassing load balancer

- Security Research
  - From Bug Bounty Hunter to Risk Analyst: My Cybersecurity Journey at Deloitte
  - MOVEIt Transfer RCE Part Two (CVE-2023-34362)
  - Speculative Denial-of-Service Attacks in Ethereum
  - Ios App Extraction & Analysis
  - Pentesting Xamarin Android apps: DLLs and root check bypass – hn security
  - can I speak to your manager? hacking root EPP servers to take control of zones
  - How I choose a security research topic
  - Grepping through API payloads with Gron
  - MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise
  - Pre-Authenticated RCE In VMware VRealize Network Insight CVE-2023-20887
- Bugs
  - How I found 5 Sql injection using 3 tools
  - One Bug at a Time: Last 15 days of #30daysofbugbounty
  - Open redirect due to scanning QR code via browser(Brave ,Opera)
  - Best approach to Error-Based SQL injection
  - Unleashing the Power of Recon: How I Earned $2500 in 5 Minutes | CVE-2017–5638 | OGNL injection
  - Admin Panel Bypass without the credentials
  - Unveiling the Secrets: Bypassing Cloudfront XSS WAF
  - PII Data Leakage and US$1500 Bounty
  - SQL Injection in The HTTP Custom Header
  - A critical vulnerability in SajiloCV which allowed me to download 100K + users resume
  - Account Takeover via password reset functionality.

    - Unrestricted file upload
    - IDOR, unpin posts for fun.
    - How I found a Reflected XSS at popular Online Store
    - CVE-2023–25717 RCE Hunt
    - Stored XSS Injection & Permanent Open Redirection
    - A Day of Bounty Bonanza: Discovering Two Bugs Back-to-Back!
    - Critical Finding on TP-Link service or how I got 0$
- CTF challenges
    - HTTP in Detail | TryHackMe
    - HTB: Escape
    - Authentication bypass WH4
    - TryHackMe: Burp Suite—Summary (Part 1)
    - Soccer—HTB Walkthrough

- Unveiling Trickest: My Secret Weapon for Automating the Bug Bounty Hunt
- Capture Login Information from the Captive Portal with SEToolkit
- GitHub – Anof-cyber/MobSecco: Clone Cordova application for bypassing security restrictions
- GitHub – Rudolf-Barbu/Parcel: IMAP brute-force tool
- Firefly – Black Box Fuzzer For Web Applications
- XSS Hunter
- Burpgpt – A Burp Suite Extension That Integrates OpenAI's GPT To Perform An Additional Passive Scan For Discovering Highly Bespoke Vulnerabilities, And Enables Running Traffic-Based Analysis Of Any Type
- Extended XSS Searcher and Finder
- Get a list of associated domains from a list of IPs with hakip2host!

- Find XSS Easily in 3 steps
- 3 months ago, I took the challenge to take over one of the most hardened bug bounty programs ever. 30 days later, ranked top 1 within the rules and exited. Since then, I still have the crown. Sharing a couple mental tips
- Find leaked API Keys and Secrets using a single GitHub search query
- Today's XSS in a Multi-Reflection case
- I've decided to do bug hunt with only dorking for remaining month. Where I'll be creating new dorks to get sensitive information
- This bypass by @Akamai *may* be useful when exploiting Windows-based SSRF vulnerabilities
- trick to find hidden endpoints on web apps, start with Underscore (_)
- API hacking tip: Whenever you see a value called ID in the response, use the search tool to search for mentions of that in other requests

- Time to challenge yourself in the 2023 Google CTF!
- Introducing @github's revamped VIP bug bounty program! Check out the perks of being a Hacktocat and how you can earn an invite: