Bug Bytes #197 – In the Clouds

BY TRAVISINTIGRITI · APRIL 26, 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 April 17th to April 23rd

CLICK HERE TO SUBSCRIBE

Intigriti News

- Our April Challenge ends on May 2nd!
- Check out our discord
- We also want to know your favourite creators

From my notebook

This week I've put together some cloud security resources, starting with some "new to me" resources and some recent write ups, if you're looking for somewhere to start check out NahamSec's series!

1. Hacking Kubernetes: Vulnerable Apps to Cluster Admin
2. Cloud Hacking: Hacking Amazon AWS
3. Cloud Red Teaming: AWS Initial Access & Privilege Escalation
4. Hundreds of companies' internal data exposed: The Confluence Cloud misconfiguration
5. Identifying vulnerabilities in GitHub Actions & AWS OIDC Configurations

Other Amazing Things

- Learn WebApp Pentesting: 2023 edition
- Here's how to ACTUALLY start bug bounties (shorts)

- Which tool should you use to find critical vulnerabilities frequently? (shorts)
- Learn to Hack Web Apps – Live | #APIs #BOPLA #CTF
- Wi-Fi Exploitation Framework(Automated)
- 5 Books to get into bug bounty and web hacking (shorts)
- ZIION – Set up your web3 testing env with a few clicks
- "Easiest" Beginner Bugs? Access Control and IDORs
- Web Challenges [Space Heroes CTF 2023]
- TryHackMe – Git Happens (Easy) – Live Walkthrough
- CVE-2022-23935 Analysis: Command Injection in Exiftool
- TryHackMe – TakeOver (Easy) – Live Walkthrough
- Snapchat paid a hacker $15,000 (shorts)
- Amazon Code Whisperer VS Github Copilot
- Hacker Interviews: @ArchAngelDDay

- Episode 16: The Hacker's Toolkit
- Reversing the AMD Secure Processor (PSP) – Part 2: Cryptographic Co-Processor (CCP)
- Tesla workers spy on drivers, and Operation Fox Hunt scams

- I'm doing a talk about hacking EPP servers and the EPP protocol with @samwcyo for #nahamcon later this year. We will talk about how we hacked 15+ ccTLDs and could control the DNS record delegation for all of them.
- Jason Haddix shares some of his favourite newsletters and his own
- Dependency confusion – mismanaged by @Google security VRT

- This is an absolutely dope mindmap for attacking AD.
- My thoughts on recon today

- Prompt Injection Attacks and Mitigations
- The Top 5 Obstacles Newcomers Face in Infosec (And How to Overcome Them)
- SSRF methodology by Aakash Rathee
- JAVASCRIPT DEOBFUSCATION FOR PENTESTER
- What is Prototype Pollution Vulnerability
- Struggling to prepare for a Smart Contract audit? Check how I prepared for Gravita protocol audit
- Understanding Unrestricted Resource Consumption: A Comprehensive Guide | 2023
- HTB: Investigation
- 10 Common XSS Payloads and How to Use Them for Bug Bounty Hunting
- Mass Assignment in vAPI
- SDLC (Software Development Lifecycle) | Tryhackme Writeup/Walkthropugh By | Md Amiruddin
- Cookie Hack: Protecting Your Online Snacks?
- Understanding Broken Authentication in OWASP API2
- Why Next.js is the Future of Web Development: A Comprehensive Guide for Developers
- Path Traversal vs File Inclusion Vulnerability! How to Tell the Difference?
- Docker Hardening Best Practices
- Buffer Overflow Basics
- Securing AWS Step Functions
- My Journey and Lessons from the #30dayofweb3 Challenge
- Hack a Smart Contract: Time Manipulation Attack.
- A Comprehensive Guide to Protecting Your Applications from XXE Vulnerabilities
- Tricks and Tips to Bypass reCAPTCHA

- Protecting Against Sensitive Data Exposure in Express.js: Best Practices and Example
- The Ultimate SQLmap Tutorial: Master SQL Injection and Vulnerability Assessment!

- Exploiting and Securing Jenkins Instances at Scale with GroovyWaiter
- Stealing GitHub staff's access token via GitHub Actions
- Hijacking Arch Linux Packages by Repo Jacking GitHub Repositories
- Zero Trust Access to Private Webapps on AWS ECS with Cloudflare Tunnel
- Container security fundamentals part 3: Capabilities
- Two Ways to Access EKS: Kubernetes RBAC and AWS IAM
- Data Exfiltration from Air-Gapped Systems: Exploring Covert Channels
- Entity authentication with a KEM
- Abusing Javascript:history.back() as an open redirect
- XS-Leak: Deanonymize Microsoft Skype Users by any 3rd-party website
- Playing Hide and Seek with PDF Files
- Turning Vulnerability into Bounty: How CVE-2020–17453 XSS Earned Me a $500 Bounty
- How I detected Open Redirect on a WhatsApp Message
- Uncovering a Critical Vulnerability: My Journey of Discovering CVE-2021–31589
- Privilege Escalation via Broken Authentication: A Story of $$$
- Critical IDOR At Big company $600
- IDOR a Highest Bounty
- $??? USD for Blind OS Command Injection via Account Activation Request
- How careless default credentials impact to massive account takeover
- A successful prototype pollution chained to a DOM XSS
- My Report on How I got $$$ on 30 minutes {Information Disclosure }.

- Broken Object Property Level Authorization in API Security
- Bypassing 403s like a PRO! ($2,100): Broken Access control
- Telegram bug bounties: RCE, privacy issues, and more
- Grafana RCE via SMTP server parameter injection (Worth $5000)
- Insecure Docker Registry API Leads To Pull All Private Docker Images
- How I Leveraged Open Redirect to Account Takeover
- Bypassing Link Sharing Protection in Messenger Kids Parent's Control Feature | Meta Bug Bounty
- Found +6 DomXSS at different programs (Hacking Swagger-UI)
- No Rate Limiting on Forget Password Page Leads to OTP Bypass and Account Takeover.
- [BAC/IDOR] How my father credit card help me to find this access control issue
- Uncovering an IDOR Vulnerability in a Major Online Store
- From payload to 300$ bounty: A story of CRLF injection and responsible disclosure on HackerOne
- Sensitive Data Disclosure (Unauthenticated Calls on Endpoints)
- How Deep Recon help me to get critical Bug in Xiaomi
- My First Case of SSRF Using Dirsearch
- Crazy stored XSS on a router!

- Making TruffleHog faster with Aho Corasick
- Introducing the Columbus Project
- Katana – A Next-Generation Crawling And Spidering Framework
- Nuclearpond – A Utility Leveraging Nuclei To Perform Internet Wide Scans For The Cost Of A Cup Of Coffee
- KubeStalk – Discovers Kubernetes And Related Infrastructure Based Attack Surface From A Black-Box Perspective
- XSpear Powerful XSS Scanning and Parameter analysis tool&gem.

- LAZYPARIAH Generate reverse shell payloads on the fly.
- tlsx Fast and configurable TLS grabber focused on TLS based data collection.

- SSRF via proxying and why it works
- How to stop finding duplicates
- HackSpaceCon Slides
- Adobe AEM Dispatcher filter bypass technique
- Pwned 2 admin panels
- Find valid endpoints redirecting to login page.
- Bug bounty, recon methodologies, tips and trick
- Unauthorized access to open dashboards
- IDOR tip, of multiple parameters
- Burp Suite Extensions you should check out!