Bug Bytes #190 – BBTips, Attacking Wide Scopes, AWS and Containers

BY TRAVISINTIGRITI · JANUARY 18, 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 January 9th to January 15th

CLICK HERE TO SUBSCRIBE

Intigriti News

- We posted a big list of SQL injection resources
- EAR tip
- Code review challenge and the solution

From my notebook

The rough theme for this week is cloud security, honestly this is a must learn skill for bug bounty hunters in 2023, at least the basics of how to deploy to AWS. I've walked right past a valid AWS key without realising it, thankfully now I use TruffleHog if I'm looking at open source but it's definitely a skill worth picking up even with tools.

1. Beginners Guide to Container Security
2. AWS Autoscaling Privilege Escalation | by notdodo
3. HACKERS ARE HIJACKING WEBSITES!
4. #NahamCon2022EU: Attacking Wide Scopes by @Hussein98d
5. Critical Thinking – A Bug Bounty Podcast – Introductions, Bug Bounty Reports, and BB Tips

Other Amazing Things

© Intigriti

- $1 mln bounty in Aurora blockchain for no input sanitisation bug
- Spying with Google Home
- An Adversaries Approach to Smart Contracts (with @hackermate_)
- What you're getting wrong with AppSec
- Being Content, Insecurity, Confidence
- NoSQL Injection Analysis [Shoppy – HackTheBox]
- HackTheBox – Shoppy
- Live Recon Sundays – Interview a Hacker: @gf_256 – Smart Contract

- 177 – Web Hackers vs. Cars and a Facebook Account Takeover
- SN 905: 1 – LastPass Aftermath, LastPass vault de-obfuscator, LastPass iteration count folly
- The age old battle between social engineering and banking.
- HACKING THE AWS CLOUD & AWS ECR (THERE'S MORE!)

- Besides curl and sed/awk/grep, what are some of your most frequently used linux commands that you think will help with hacking?
- If you're looking for a job, try to blog regularly about CVEs (one you didn't find)
- Thread of high profile breaches of 2022
- Portswigger upcoming conference talks
- Some days you don't report any vulnerabilities, but that does not mean you didn't accomplish anything.
- S3 Bucket configuration
- Harsh Bothra is teaching his wife about AppSec

© Intigriti

- Learn iOS penetration testing

- How To Attack Admin Panels Successfully Part 2
- Open redirects : bug bounties
- Seven Common Ways To Bypass Login Page
- Unlock the boundless possibilities of ChatGPT: Hunt down pesky bugs and enjoy seamless automation!
- Broken Access Control: What I have learned
- Bug Hunting 101: Parameter Injection Vulnerabilities
- JWT Security 101: How to defend against common attacks on JSON Web Tokens
- Brute-force attacks Cheat Sheet (FTP, POP3, SNMP, SSH, VNC, ...)
- Clear communication is crucial: why writing effective vulnerability reports matters
- All about: Business Logic Bugs
- Easy XSSHunter Express Setup Script
- Bug Hunting 101: Directory Enumeration & Authentication Bypass
- Kerberos Authentication (again... but better)
- Bypass mysql_real_escape_string and addslashes from Injection Attacks
- Domain Name System 0x1 | DNS 101
- OWASP TOP 10
- The toddler's introduction to Dynamic Memory Allocation
- [2023] Guide to Web3 Data Tools (H/T HiveFive)
- Optimise Wordlists with Masks (H/T FiveFive)
- How I Found AWS API Keys using "Trufflehog" and Validated them using "enumerate-iam" tool

© Intigriti

Write ups

- “2022: A Year of Fascinating Discoveries”
- Uploading the Webshell using filename of Content-Disposition Header Story!
- Bug hunting: Open access to S3 bucket
- bypass two-factor authentication in Android apps and web 1000$ TikTok
- How I Earned $1000 From Business Logic Vulnerability (account takeover)
- Hack Analysis: Nomad Bridge, August 2022
- SMB “Access is denied” caused by anti-NTLM relay protection
- A Newbie’s Guide to Bug Bounty Hunting: Navigating the World of Subdomain Enumeration
- JNDI Injection Series: RMI Vector—The Final Piece of The Puzzle
- Which bug did you find that you are most proud of?
- Strange 2FA Misconfiguration
- How a Ukrainian developer quaked the French government.
- How Browser’s Save As Feature might lead to Code Execution (CVE-2022–45415)
- How I was able to hack anonymous texting services?
- India’s Aadhar card source code disclosure via exposed .svn/wc.db
- API based IDOR to leaking Private IP address of 6000 businesses
- Exploiting API with AuthToken
- CSRF leads to account takeover in Yahoo!
- Finding CVE-2022–3786 (openssl) with Mayhem
- Control Web Panel RCE Vulnerability
- Identifying Coin Scammers with Wallet-Tracker
- Free Cloud (Browser-based) Labs of DVWA and bWAPP
- Full Account Take Over by very simple trick.

© Intigriti

- Awesome Hacker Search Engines – A curated list of awesome search engines useful during Penetration testing, Vulnerability assessments, Red/Blue Team operations, Bug Bounty and more
- Burp Extensions API – Montoya Burp API
- LinWinPwn – Active Directory Vulnerability Scanner (H/T 0dayCTF)

- A few dorks to find common bugs while testing
- OWA tip
- Top 10 web hacking techniques of 2022 voting
- TodayIsNew Interview with his tips
- Recon management tips by Jason Haddix
- PHP info page pays out $5k
- Custom wordlists tip
- SQL injection payloads

- Full Team Takeover
- Illumination—HackTheBox Forensics Writeup | 2023
- TryHackMe writeup: Dunkle Materie

© Intigriti

- Soccer—Hack The Box | Writeup with Flag | 2023
- Lost Modulus—HackTheBox Crypto Challenge(RSA) Simple Writeup | 2023
- Juicy Details—TryHackMe Writeup
- QuillAudit CTF challenges—Writeups

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com

© Intigriti