Bug Bytes #189 – Top YouTube Channels of 2022, Web Hackers vs Ferrari, Cognito Security Misconfiguration

BY TRAVISINTIGRITI · JANUARY 10, 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 2nd to January 8th

CLICK HERE TO SUBSCRIBE

Intigriti News

- We share our top YouTube channels of 2022
- Cryptocat joins Intigriti, check out this interview we did with him!
- Cristi shares some swag from our event with The Paranoids!
- Another code review challenge! and the solution
- December monthly leaderboard
- Our XSS challenge results

From my notebook

It's been a quiet week in the offensive security community, this week I've put together a must read list on more advanced resources shared this week. From a look into the world of automotive security and household names, to the nitty gritty of Java Deserialisation, scaling up a neat website idea into a search engine and proxying encrypted traffic.

1. Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More
2. Exploring the World of ESI Injection
3. Image Stacks and iPhone Racks – Building an Internet Scale Meme Search Engine
4. Fetch Diversion
5. Manipulating AES Traffic using a Chain of Proxies and Hardcoded Keys

Other Amazing Things

Videos 

- Holehe OSINT
- #NahamCon2022EU: I Hope This Sticks: Analyzing ClipboardEvent Listeners
- Playing with a (CTF) Smart Contract [Hackvent 2022 – Day 6]
- Reflective XSS via Link Click / SSRF [Hackvent 2022 – Day 14]
- #NahamCon2022EU: Hunting for Amazon Cognito Security Misconfigurations
- The Flipper Zero Scam
- Would you prefer a password-less login? #cybersecurity #shorts
- LevelUpX – Series 13: SPI Flash for Bug Bounty Hunters with Nerdwell
- Bugcrowd Security Flash – The Kaseya REvil Attack Explained
- Hacking KringleCon [Sans Holiday Hack 2022]

Podcasts 

- Episode 357 – Is open source being overexploited?
- 287-Listener Questions, UNREDACTED 5, & OSINT 10

Tweets 

- I hacked a large company (70k+ employees) through social engineering. Legally of course.
- My first bug of 2023

- If you could only listen to one song while hacking for the rest of your life, which one would you pick?
- Hacking is a mentality that can be applied to much more than computers.
- While working in tech, having a strong technical base is key, But don't underestimate the power of good social communication skills
- Is a open redirection a real bug?
- Javascript for Hackers paperback version

- The three main types of XSS
- Automated and Continuous Recon/Attack Surface Management—Amass Track and DB
- An amazing way to turn a xss into an ATO
- A Deep Dive Into DNS Hijacking
- simple Python script that can scan a URL for a Remote Code Execution (RCE) vulnerability.
- Python script that will get a search term from the user and search for related articles on Medium...
- Golang Programming and Security Vulnerabilities
- P1 Bug Bounties: Subdomain Takeover Bug Hunting
- Race Condition Vulnerabilities
- Scheduling Recon Scripts with Docker
- 5 Google Dorks Every Hacker Needs to Know
- Cross-Site Scripting—XSS [CWE-79]
- Everything about Cookie and Its Security
- The Dangers of Remote Code Execution (RCE)
- How to perform dynamic analysis of a smart contract with Myth
- How to automate your initial recon and extend ASM using Sub-Scout
- How To Attack Admin Panels Successfully Part 2

- CVE-2022-38627: A journey through SQLite Injection to compromise the whole enterprise building
- ChatGPT—Bug Bounty Recon Automation
- India's Aadhar card source code disclosure via exposed .svn/wc.db
- Web-Cache Poisoning $$$? Worth it?
- IDOR and API-keysToken Hardcode Exposed
- Vue JS Reflected XSS
- FTP Access-with-anonymous-login-credentials-enabled.
- Access to page with default credentials that require authenticate $$$.
- Bypass Premium Account Payment (GetPocket)
- XSS: What I have learned
- I Reverse engineered an Amazon Prime Error
- Blind XSS in Email Field; 1000$ bounty
- Logic Bug Can Create Multiple User Accounts with 1 Phone Number (Reward $150)
- Got Takeover Account From Multiple Bugs
- How I Found My First Vulnerbility/Bug Bounty at Hackerone.
- IDOR and API-keys Token Hardcode Exposed
- JNDI Injection Series: RMI Vector – Insecure Deserialization
- My First Bug Bounty Reward : $100 in 5 min

- JsonCrack – Json visualised into trees
- Gitscraper – Scrapes public PHP repositories to create dictionaries
- googd0rk – Fire off google dorks against a target domain, it is purely for OSINT against a specific target domain.

- What I Learned Exploiting an SSRF bug, by Raymond Lind
- Email Subdomain Takeovers
- Googledorking for Adobe Experiment Manager
- Fileupload to RCE
- phpmyadmin and Shodan
- Top recon processes
- Bug Bounty Automation tips
- Nuclei to find secrets in javascript
- Nmap cheatsheet

- Hackvent 2022 – Easy, Hackvent 2022 – Hard
- 2022 SANS Holiday Hack Challenge, featuring KringleCon V: Golden Rings
  - Holiday Hack 2022: KringleCon Orientation
  - Holiday Hack 2022: Web Ring
  - Holiday Hack 2022: Cloud Ring
  - Holiday Hack 2022: Burning Ring of Fire
- HTB: Health

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com