Bug Bytes #184 – Advent of Cyber, NahamCon EU, IWCON2022 and ChatGPT

BY TRAVISINTIGRITI · DECEMBER 7, 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 November 28th until December 4th.

CLICK HERE TO SUBSCRIBE

Intigriti News

- Ali wins 1st place on our November Leaderboard
- Vulnerable code snippet and the solution and finally the code
- Intigriti's head of hackers @securinti will be speaking at #IWCON2022
- The November XSS Challenge has ended! check out the write ups by our community!

From my notebook

It's December, which at least here in the UK means kids (and adults) will be opening up a calendar for each day in the run up to christmas and the new year. As such there's a whole bunch of events running in December, so it's worth shouting them all out.

1. TryHackMe! Advent of Cyber 2022 Kick-Off
2. Who Will You Learn From at IWCON2022? (3 Free Videos to Turbocharge Your Infosec Journey)
3. NahamCon EU Speaker Lineup
4. We recently found a vulnerability affecting Hyundai and Genesis vehicles where we could remotely control the locks, engine, horn, headlights, and trunk of vehicles made after 2012.
5. More car hacking on Honda, Nissan, Infiniti, and Acura vehicles

Other Amazing Things

Videos 

- 2022 Vegas Bug Bash with Bugcrowd
- URL File Attack || Active directory
- catch EVERY reverse shell while hacking! (VILLAIN)
- explore a WordPress PHP BACKDOOR webshell
- Can AI Create a Minecraft Hack?
- Live Recon with Jason Haddix (@jhaddix): AMA!
- Applying Blue Team Defender Theory In Practice (Defend the House)
- Mental Hacking Ep:3 | Staying Motivated in Bug Bounty
- Dockerized Bug Bounty Automation Demo! (Automation Series)
- Bug Bounty Evolution: Not Your Grandson's Bug Bounty
- Supernatural Hacks Live Hacking Workshops

Podcasts

- Episode 351 – Is security or usability a law of the universe?
- EP99 Google Workspace Security: from Threats to Zero Trust
- Norse Corp.: How To NOT build a cybersecurity startup
- 171 – Tailscale RCE, an SQLi in PAM360, and Exploiting Backstage
- Web Application Firewall (noun) [Word Notes]
- SN 899: Freebie Bots & Evil Cameras – iSpoofer no more, Boa server vulnerability, CISA on Mastodon
- 172 – Patch Gaps and Apple Neural Engine Vulns

- A vishing competition and a Black Badge holder.
- Erkang Zheng of JupiterOne

- A JPG file dissection
- Feeling like never finding a bug..
- I'm not writing a report ever again
- How should I remediate the vulnerability in this code?
- I've asked #ChatGPT to make a #bugbounty program policy with bounties aligned to the market average. Here's what it did:
- I've learned 90% of the people who make fun of bug bounty hunters have tried bug bounties and didn't get anywhere, so they put their energy into hating on it instead
- Getting good at hacking takes years...

- Firebase Exploit bug bounty
- Write-up: Basic server-side template injection (code context) @ PortSwigger Academy
- Automate GitHub Actions Security Best Practices
- 5 Different Techniques to Perform Account Takeover
- What is unrestricted file upload vulnerability? And How to exploit it on DVWA!
- Unvalidated Redirects and Forwards
- How To Install Autorize on Burpsuite
- Subdomain Enumeration with DNSSEC
- P1 Bug Hunting—Remote and Local File Inclusion Vulnerabilities
- Subdomain Takeover

- Write-up: Source code disclosure via backup files @ PortSwigger Academy
- SSRF via DNS Rebinding (CVE-2022–4096)
- Banner grabbing leads to RCE
- pentesting.cloud part 2: “Is there an echo in here?” AWS CTF walkthrough
- Sql injection
- Automating Recon: The Tools and Techniques Used by Today’s Hackers

- 2FA Enabled Accounts Can Bypass Authentication & Access Account After Deactivation
- Unique Rate limit bypass worth 1800$
- Access Any Owner Account without Authentication (Auth bypass + 2FA bypass)
- The Untold SendBird Misconfigurations
- How I hacked into a government e-learning website
- A great weekend hack(worth $8k)
- How I DIDN’T get an RCE in a $200 Billion company — Bug Bounty
- Broken access control + misconfiguration = Beautiful privilege escalation
- Improper error handling leads to exposing internal tokens
- Full RCE via File Upload + Reverse shell OpenBugBounty
- Stored XSS at https://www.tiktok.com/
- Unique Rate limit bypass worth 1800$
- My Latest XSS Finding, Explained To Beginners | Bug Bounty
- IDOR Disclose User Pending Trip Information | Part 01
- From Bug Hunter to Threat Researcher!!
- EXPLOTATION / HUNTING OF LOCAL FILE INCLUSION (LFI)
- XSS on account.leagueoflegends.com via easyXDM [2016]

- DoS on a Wifi Router-Wifi Hacking #1 | Harsh Master
- Interesting find on the Invite link
- [WRITE-UP] Irremovable comments on the FB Lite app | A story of a simple FB Lite bug that I found...
- Account Takeover – Inside The Tenant
- A $$$ worth of cookies! | Reflected DOM-Based XSS | Bug Bounty POC
- In and out of Bug bounty in 6 months, Made Over $12K
- URL Validation Bypass Using Browser URI Normalization
- Issue 210: CSRF vulnerability in F5, supply chain attacks, hacking APIs, GCP API security report
- VoIP Spoofing (Intigriti) 1,250€
- Behind the SMS Bombing Application
- Email Graffiti: hacking old email

- How to Install Gf Tool and Patterns on Kali Linux
- The Top 8 Bug Hunting Tools for P1 Bug Bounties
- DomainDouche – OSINT Tool to Abuse SecurityTrails Domain Suggestion API To Find Potentially Related Domains By Keyword And Brute Force
- getallurls (gau) fetches known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, Common Crawl, and URLScan for any given domain. Inspired by Tomnomnom's waybackurls.
- uncover – Quickly discover exposed hosts on the internet using multiple search engines.
- UseReFuzz SQL Injection Tester for HTTP Headers.

- Blockchain Books
- 40 Tips and Tricks to Improve your Bug Bounties as a beginner
- You can clobber classes if a site uses querySelector():
- Local File Inclusion To Access System Files
- Sensitive keyword js
- The new http://cs.github.com search allows for regex, which means brand **new** regex GitHub Dorks are possible!
- Discovered Passwordresx.aspx and paste payload (' waitfor delay'0:0:20'–)

- DOJO CHALLENGE #19 Winners!
- GHW December
- HTBUniversityCTF22
- YesWeHack Vulnerable Code Snippets
- SANS Holiday Hack
- CactusCon CTF

- First Bug Bounty For Homeland Security Uncovers 122 Vulnerabilities
- Zoom's Bug Bounty Programs Have Reached $1.8 Mn
- Building A Virtual Machine inside ChatGPT