Bug Bytes #183 – Learning, reflecting and hacking

BY TRAVISINTIGRITI · NOVEMBER 30, 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 14th until November 27th.

CLICK HERE TO SUBSCRIBE

Intigriti News

- We launch another code challenge...
- ...And give you the solution
- November XSS Challenge
- The Visma #1337up1122 Live Hacking Event has ended! With 784 submissions and over €190,000 paid out!
- We also gave some hackers some new avatars!

From my notebook

This week's top 5 theme is about learning new skills. I think this is something that all hackers will relate to, in this field you are always reading articles, watching videos, etc and looking for new tools, techniques and that's probably why you're reading this blog post. But more important than just consuming new information is to reflect on what you've learned, organise it in your head and turn it into useful information. One of the best ways I've found to do that and actually improve my own learning has been by creating content, so today that's what I'm sharing 5 pieces of content from folks who are learning and sharing.

1. Learning SECURE CODE REVIEW!
2. Most important security lessons of 2022 for me
3. My Top 7 Favorite Websites to (Legally) Improve My Web-Hacking Skills
4. So, you want to get into bug bounties?
5. Blind Students Learn Lockpicking (w/ Deviant Ollam)

Other Amazing Things

Videos

- Web App Wednesday (8/3/22) – Burp Suite Pro
- The Accidental $70k Android Hack
- you should be using PODMAN
- CTF Walkthrough: Hacking An API with Snyk!
- Your choices matter... Responsible Red Teaming w/ HuskyHacks
- Hacker Doxes Himself Accidentally...
- Entry Level Careers & Learning
- Theft of Arbitrary files from LocalStorage | Hacking on Android

Podcasts

- These companies ran an experiment: Pay workers their full salary to work fewer days
- 167 – Bypassing Pixel Lock Screens and Checkmk RCE
- 128: Gollumfun (Part 1)
- 168 – Exploiting Undefined Behavior and a Chrome UAF
- 298: Housing market scams, Twitter 2FA, and the fesshole
- EP98 How to Cloud IR or Why Attackers Become Cloud Native Faster?
- 169 – Racing Grafana, Stealing Mastadon Passwords, and Cross-Site Tracing
- Jailbreaking Tractors [ML BSide]
- 170 – Hacking Pixel Bootloaders and Injecting Bugs
- Internet vs Reality of Working as a Cloud Security Architect!
- 299: EV charging risks, FTX, and an ancient apocalypse

- Corben hacked a phone company this year, here's how he did it
- Yesterday, an old friend sent hipotermia an Instagram DM asking me for help for a contest, here's what they did to hack it
- If you are struggling with persistence while hacking (like renniepak), try taking a different approach.
- Teamviewer fingerprinting using fonts
- What to ignore in a digital world
- Bug Bounty Reports Explains on his year of bug bounties
- Naffy starts a conversation about scope and serious vulnerabilities

- Wanna Bet That CSRF Is Not As Hard as you think?
- A Brief Introduction to SAML Security Vector
- P1 Bug Bounties: What is an IDOR, and how does IDOR == $$$?
- HTTP Header Exploitation
- HOW TO CRAWL LINKS LIKE A PRO!
- Frida & Objection without Jailbreak!
- The Best Ways to Exploit Rate Limit Vulnerabilities
- Dorking: The hidden filters....
- Explaining vulnerabilities : Cross Site Scripting (XSS)
- Email Verification Bypass
- P1 Bug Hunting: A Step by Step Guide to SQL Injection
- Main app methodology : Bug bounties

- Deploying an AWS S3 static site to use Cloudflare WAF
- OAuth and the flaws in its implementation
- How to actually use Amass more effectively – Bug Bounty
- THE ANATOMY OF KERBEROS AUTHENTICATION (AD BASICS 0x1)
- Explaining vulnerabilities : OS command injection {Bug bounties}
- P1 Bug Hunting—Exploiting Common WordPress Vulnerabilities
- Explaining vulnerabilities : File inclusion {Bug bounties}
- Explaining vulnerabilities : Template Injections (Server-Side) {Bug bounties}

- Failed to invalidate session after password change -[Insufficient session Expiration].
- How I bypassed Cloudflare WAF to get my First Bug
- XSS using a username
- Winning QR with DOM-Based XSS | Bug Bounty POC
- Gauing+Nuclei for Instant Bounties
- P1 Bug—Leaked Zendesk Token in GitHub
- Account Takeover worth of $2500
- The Story Of A Strange / Stored IDOR.
- Information Exposure—My Fourth Finding on Hackerone!
- Reflected XSS using Double Encoding
- $250 for Email account enumeration using “NameToMail” tool
- How i found 8 vulnerabilities in 24h?
- How I found CVE-2022–40088
- GAS theft attack in Solv Protocol
- Russian roulette XSS

- How I earned $47000 USD as a high school student
- OTP BYPASS WithOUT RESPONSE MANIPULATION
- SSRF via DNS Rebinding (CVE-2022–4096)
- Interesting Stored XSS via meta data
- Working with a scope using Gowitness
- Fastly Subdomain Takeover $2000 – Bug Bounty Writeup
- Html File Upload Lead to A.T.O in Indonesian Government Site
- Hacking Dutch Government-Broken Authentication To Full Website Takeover (P1)
- [Hacking Bank] The Second Story of Finding Critical Vulnerabilities on Banking Application
- A Confused Deputy Vulnerability in AWS AppSync
- Bug Bounty Tips and Getting Persistence With Electron Applications
- DLL Hijacking Persistence Using Discord
- Remediation Archeology—Finding and Decoding an Ancient XSS
- Header spoofing via a hidden parameter in Facebook Batch GraphQL APIs

- related-domains – Find related domains of a given domain using Whoxy API.
- csprecon – Discover new target domains using Content Security Policy
- google-search – Performs searches on Google and display the resulting URLs, as simple as that!
- Slicer – Tool To Automate The Boring Process Of APK Recon
- nuvola – Tool To Dump And Perform Automatic And Manual Security Analysis On Aws Environments Configurations And Services
- Spoof browser fingerprints in Burp
- Octopii – An AI-powered Personal Identifiable Information (PII) Scanner

- VALID E-mail address payload lists of different bug classes
- The Best Bug Bounty Hunting Tips and Tricks of 2022
- Some “tips” on bug hunting
- Bug Bounty Tips—Part 1
- Master Burp Match and Replace!
- PHP Filters
- AutoSSRF
- Find Bugs
- SQL Injection tip
- WAF filters

- Portswigger’s ongoing Burp Challenge – finished Dec 31st
- YesWeHack Vulnerable Code Snippet solution
- Capture the Talent – Advent Challenge launches 1 Dec!
- HTB University Challenge
- SANS Holiday Hack
- TryHackMe Advent of Cyber

- How was Uber hacked, and what can we learn from the incident?
- Immunefi Launches Timebound Bug Bounty For Proof-of-Capital Vault System
- A Leak Details Apple's Secret Dirt on a Trusted Security Startup