Bug Bytes #182 – Infosec twitter migrates to Mastodon, Google Pixel Lock Screen Bypass and Next-Gen Spidering with Katana

BY TRAVISINTIGRITI · NOVEMBER 16, 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.

We're running a survey about Bug Bytes: What do you think of Bug Bytes? Let us know!

This issue covers the weeks from November 7th until November 13th.

CLICK HERE TO SUBSCRIBE

Intigriti News

- We published a blog on how to set up your own XSSHunter with a Video tutorial
- This week hackers descend on Copenhagen for 1337UP1122 with Visma
- SSTI in 100 seconds
- We're on Mastodon Intigriti@infosec.exchange
- We gave some hackers some profile pictures

From my notebook

There has been some great blog posts this week but I think the whole community was wowed by the lock screen bypass on the Google Pixel and the new tool from project discovery Katana, promising a next-gen spidering tool. I've also included Awesome API security which has a ton of API resources, with bugs, how tos, tools and CTFs you can practice on.

1. Accidental $70k Google Pixel Lock Screen Bypass
2. SMS Multifactor Authentication in Antarctica
3. Chaining Path Traversal with SSRF to disclose internal git repo data in a Bank Asset
4. Katana – A next-generation crawling and spidering framework
5. Awesome API security

Other Amazing Things

Videos 

- Dehashed || A Data Breah Search engine
- Cybercrime & Dark Web Conversations (w/ Shmuel!)
- How to get greater bounties for MEDIUM and LOW risk reports?
- What is a Server? (Deepdive)
- Stop Hackers With This!
- Hospitality To Cyber Secrets Revealed (You Can Do It Too!)
- The challenge that shall not be named [Flare-On 2022]
- Hacking on Android With Gaurang Bhatnagar | Creator #InsecureShop
- Bug Hunting Experience on Code4rena
- Israel (Cyber) Defense Forces, Blockchain, DeFi and Life as a Web3 Digital Nomad @Johnny Time
- [0x0a] Reversing Shorts :: Apple's Cross-Process Communication (XPC)

Podcasts

- EP95 Cloud Security Talks Panel: Cloud Threats and Incidents
- What can chess grandmasters teach us about Cyber? [ML BSide]
- 165 – Apache Batik, Static Site Generators, and an Android App Vuln
- SN 896: Something for Everyone – Dropbox breach, cyber bank heists, Russia goes Linux, OpenSSL flaw update
- 297: Mastodon 101, and the Hushpuppi saga
- 166 – OpenSSL Off-by-One, Java XML Bugs, and an In-the-Wild Samsung Chain

- OSINT Search Engine List
- Between July 7th to July 17th, 2022, we formed a small team of hackers and collectively hunted for vulnerabilities on John Deere's security program
- Dwagyg is looking for a mental health / addiction charity
- Pwn College
- Open Source Hacking
- Book of Tips by Aditya Shende
- Do we really need to try harder?

- Hacking Tools & Resources for Bug Bounties, Red Teaming, And More!
- Some Tips to Finding IDORs more easily and Fixing them
- How to mimic Kerberos protocol transition using reflective RBCD
- Let's Cheat by changing FALSE to TRUE!
- SMTP Misconfiguration
- Automate and finds the IP address of a website behind Cloudflare
- Cool Recon techniques every hacker misses! Episode 3
- Fuzzing Web Applications using FFuf
- Searching for Subdomain Vulnerabilities using Censys
- My Recon Tools and Methodology.
- 10 Minute Bug Bounties: OSINT With Google Dorking, Censys, and Shodan
- A Beginner's Guide to Nmap
- Cross-origin resource sharing (CORS) Explanation & Exploitation

- content discovery usage and tools with real example for bug bounty(part 1)
- Intercept Mobil Application Pentest Flutter traffic on iOS and Android (HTTP/HTTPS/ Ssl Pinning)
- Understanding Privilege Escalation by Abusing Linux Access Control
- Hacking a JWT – JSON Web Token (part 1)
- Hacking JWT – JSON Web Token (part 2)

- Story of a $1k bounty—SSRF to leaking access token and other sensitive information
- New Writeup:- $6000 with Microsoft Hall of Fame | Microsoft Firewall Bypass | CRLF to XSS | Microsoft Bug Bounty
- How we 'hacked' Telenet's cybersecurity quiz
- Comodo: From .Git to Takeover
- MY FIRST ACCOUNT TAKEOVER
- Interesting Account Takeover Bugs
- Sleep SQL injection on Name Parameter While Updating Profile
- Google VRP (Acquisitions)—[Insecure Direct Object Reference] 2nd
- Router NR1800X—Command injection via setUssd
- CORS via XSS leaks User details including Credit Card details.
- Bypass Duplicate Tweet Protection using negative tweet id
- From Shodan Dork to Grafana Local File Inclusion
- How to find ("Business_logics") AND ("Broken Access Control") Bugs !
- Finding Reflected XSS In A Strange Way
- S3 misconfiguration
- Analysis of a Smishing Text
- How i get $100 in just 10 minutes !

- My First Bounty Story
- How we handled a recent phishing incident that targeted Dropbox
- Issue 208: Urlscan.io leaks sensitive data, Dropbox phishing attack, contract test for microservices

- Scripting My Custom Script Automation Tool For Web Application Hacking & Reconnaissance
- Making API Bug Bounties A Breeze!
- autoSSRF – Smart Context-Based SSRF Vulnerability Scanner
- Unblob – Extract Files From Any Kind Of Container Formats
- Tool Release – Web3 Decoder Burp Suite Extension
- HTTP Request Smuggler probes for desync flaws

- Removing a trailing slash to leak a user list by Nahamsec
- Finding a Zip file in .DS_Store by Hussein
- Easy P1 by GodFather Orwa
- ffuf over multiple hosts by H4x0r.DZ
- OOB MSSQL Injection by TESS
- RCE on file upload by Rez0

Challenges

- The Burp challenge – Complete the four challenges by 31 December 2022 for chances to prove your skills, win swag, and a Burp Suite Certified Practitioner exam credit.

Bug bounty/Pentest news

- SynFutures Launches V2 Mainnet Bug Bounty

Non-technical

- 5 mistakes to avoid on the bug bounty program
- UK Gov scans UK IP address space for bugs
- A Russian Missile Crew Was Geolocated From Just This Photo