Bug Bytes #121 – Free burp collaborator alternative, hacking chrome extensions & $28k Facebook oauth account takeover

BY ANNA HAMMOND · MAY 5, 2021 · LAST UPDATED ON JULY 17, 2025

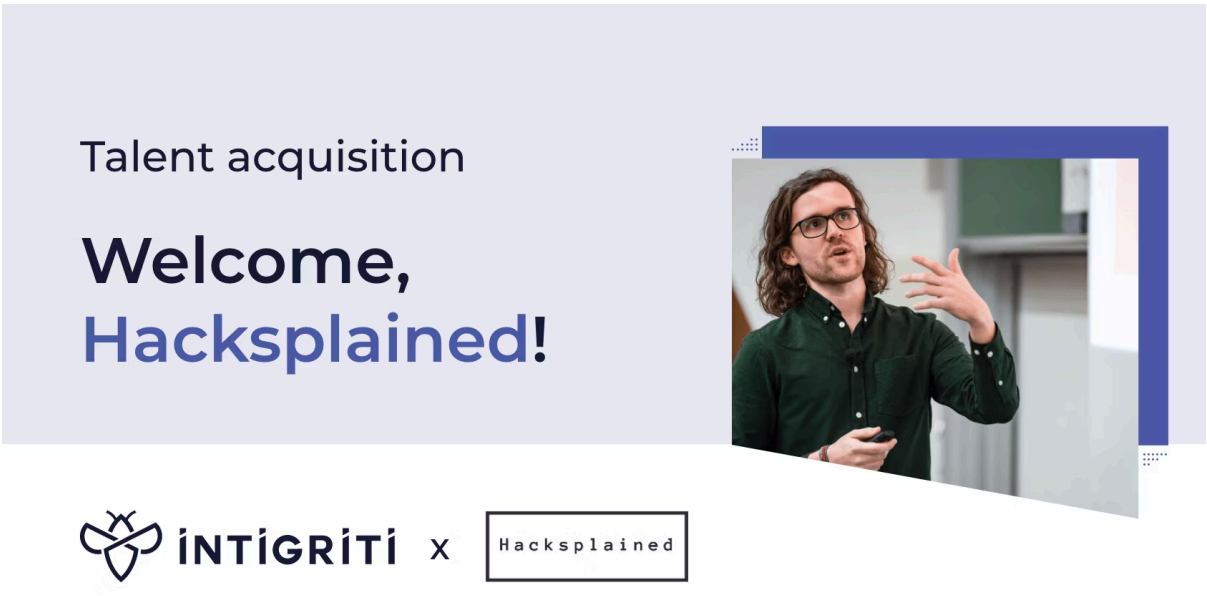
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from April 26 to May 3.

Intigriti News

Congratulations to @p4fg, @0xkasper and @sumgr0 for joining Intigriti's 1337 gang!



Hacksplained joins Intigriti to further enable community of 35.000 ethical hackers

Our favorite 5 hacking items

1. Tool of the week

Interactsh, Intro & Nuclei + Interactsh Integration for Automating OOB Testing

It can be a pain to perform Out-of-Band testing without Burp Collaborator. If you can't or don't want to pay for it, there is now a free open source alternative thanks to @pdiscoveryio.

Interactsh provides a client/server infrastructure, with the possiblity to use a self-hosted server for privacy. It has a beautiful Web interface and can be integrated with Nuclei. Such amazing work by the Project Discovery team!

2. Writeups of the week

DEFCON 29 CTF Qualifier: 3FACTOOORX Write-up
Facebook account takeover due to unsafe redirects after the OAuth flow (Facebook, $28,800)

The first writeup is @bbuerhaus's walthrough of the DEFCON 29 CTF Qualifier 3factooorx challenge. It involves analyzing a Chrome browser extension and navigating through obfuscated JavaScript with Chrome Dev Tools.
If you're learning about this topic, this is a helpful resource especially if combined with the "Tutorial of the week" below.

The second writeup is about open redirect in a Facebook app's OAuth flow that lead to account takeover. A pretty impressive finding and informative writeup by @Samm0uda!

3. Video of the week

Live Recon and Distributed Recon Automation Using Axiom with @pry0cc

Curious to know how Axiom's author uses it to hunt for bugs on real targets? This is the video to watch! In this unique type of hacker interviews by @NahamSec, @pry0cc show how he performs distributed recon with Axiom and tools like meg, nmap, httpx, ffuf, etc.

4. Tutorial of the week

Testing Extensions in Chromium Browsers – Nordpass

This is the ultimate guide to get into testing Chromium browser extensions. @CryptoGangsta shares an incredibly detailed tutorial with the Nordpass Chrome extension as an example.
Topics taught include how to debug extensions, reverse engineer obfuscated JavaScript, perform JavaScript dynamic analysis with Browser DevTools, decrypt AES-GCM encypted messages, and log/instrument extensions.

5. Non technical items of the week

@TinkerSec's alarming burnout story
Redefining What it Means to be a Hacker with Eric Head aka todayisnew

@TinkerSec's burnout story is a cautionary tale for all of us hackers. It's important to read and keep in mind for those times when our bodies are telling us to stop working/hacking and we want to keep pushing.

Another very interesting read is an interview with @codecancare. He is a successful full-time bug hunter who is known for his kindness, for automating everything and advocating for empathy and mindfulness. It's cool to hear from him about these topics, including a very practical mindfulness technique to which he attributes his success.

Other amazing things we stumbled upon this week

Other amazing things we stumbled upon this week

Videos

- iOS Hacking – Application Basics, Filesystem Basics & Inter-App Communication
- Interview With @mr_hacker | Top 20 On Intigriti | Methodology, Tips & Tricks, Etc.
- SecuriTEA & Crumpets – Episode 5 – Parsia Hakimian
- Why Pick sudo as Research Target? & Blog post
- You Do (Not) Understand Kerberos Delegation & Slides
- Katie Paxton-Fear on OWASP DevSlop
- CRLF + XSS + cache poisoning = Access to Github private pages for $35k bounty

Podcasts

- The InfoSec & OSINT Show 54 – Jeff Foley & Asset Discovery with Amass
- DAY[0] Episode 75 – Defcon Quals, Dead μops, BadAllocs, WordPress XXE
- The Ransomware Task Force – Scripps Health, REvil Hacks Quanta Computer, Emotet Botnet, QNAP

Conferences

- Kernelcon 2021 – HACK LIVE
- CANSECWEST 2021: Tbone Drone vs Tesla & Whitepaper
- Hacker Days: Understanding AWS cloud attacks using CloudGoat
- An Azure Sphere Security Breakdown | Lilith Wyatt | Nullcon Conference March 2021

Tutorials

Medium to advanced

- Decrypting Mobile App Traffic using AES Killer and Frida & AES Killer – Usage Guide
- ADExplorer On Engagements
- Utilizing a Common Windows Binary to Escalate to System Privileges

Beginners corner

- Graphql Exploitation – Part 2- Unauthorized Execution Of Queries
- Hacker tools: FFuF (Fuzz Faster u Fool)
- Living off the land

Writeups

Challenge writeups

- Information Leak via Compromised Sandboxed Browser
- HackTheBox – Sharp #video

Responsible(ish) disclosure writeups

- Discovering Null Byte Injection Vulnerability in GoAhead #Web
- Don't Share Your $HOME with Untrusted Guests #VM-Escape
- PHP Supply Chain Attack on Composer #Web

- Wagtail XSS + LocalStorage = Account Hijack #Web
- Bundler is Still Vulnerable to Dependency Confusion Attacks (CVE-2020-36327) #Web
- Dependency Confusion Vulnerabilities in Unity Game Development
- CVE-2021-29921 – Improper Input Validation of octal literals in python 3.8.0 thru v3.10 results in indeterminate SSRF & RFI vulnerabilities #Python #Web

Bug bounty writeups

- WordPress 5.7 XXE Vulnerability (WordPress)
- A tale of Html to Pdf converter ssrf and various bypasses
- Relaying Potatoes: Another Unexpected Privilege Escalation Vulnerability in Windows RPC Protocol (Microsoft)
- Exploiting the Source Engine (Part 2) – Full-Chain Client RCE in Source using Frida & Exploiting the Source Engine (Part 1) (Valve, $7,500)
- PrivateDrop: Breaking and Fixing Apple AirDrop (Apple)
- Exploiting memory corruption vulnerabilities on Android (Paypal, $1,100)
- How did I earn €€€€ by breaking the back-end logic of the server
- How I was able to Retrieve your Personal Documents using the Wayback Machine!

See more writeups on The list of bug bounty writeups.

Tools

- SRePlay (Strict RePlay) & Intro: Burp extension to bypass strict RePlay protection
- PoC of CVE-2021-28482
- Nginxpwner: Python tool to look for common Nginx misconfigurations and vulnerabilities
- gdn / Get Domain Name: A GO module to get domain name from SSL certificates when an IP address is provided
- x8: Hidden parameters discovery suite written in Rust

Tips & Tweets

- Bypass the replace() function in JavaScript for XSS
- Increasing the impact of XSS inside img tags
- SSRF via CSV injection
- @paulmmueller's' IIS/.net hacking checklist

- Running multiple FFUF jobs with RUSH (alternative to Parallel)
- Did you know tar could run lolbins and base64 encode/decode?

Misc. pentest & bug bounty resources

- HTML Sanitizer API
- Resources to learn the basics of Oauth/OpenID/JWT
- Active Directory Security – 101
- Slayer Labs (free for 7 days)
- Rowbot's PenTest Notes

Challenges

- Hacking Json Web Token Signature
- Damn Vulnerable DeFi & Exploiting DOS Vulnerability in Smart Contracts

Articles

- Abusing Replication: Stealing AD FS Secrets Over the Network
- Virtual Namespacing: A Robust Approach to Avoiding Dependency Confusion Attacks
- Detecting and annoying Burp users
- Risks of Microsoft Teams and Microsoft 365 Groups & m365_groups_enum
- Intel CET In Action

Bug bounty & Pentest news

- GitHub: A call for feedback on our policies around exploits and malware
- WPScan: Offensive Security PEN-200 OSCP Course Giveaway
- New pentest exam/certification launched by @thecybermentor: The Certified Practical Ethical Hacker (CPEH)
- BugBountyHunter is launching "FirstBlood" the first Live Hacking Event for practice where you can win real bounties (only open to members)
- Upcoming talks:
  - BSides Vancouver 2021
  - 3kCTF-2021 (May 15-16)
- Tools updates:

- Param Miner now supports path-based cachebusting
- Burp Professional / Community 2021.5: Intruder attacks can now be saved to project files!
- New axiom-build feature allows choosing between three provisioners or using a custom Packer JSON to deploy custom instances

Non technical

- The thin line between the cloud provider and the customer applications
- 2021. The age of the super vulnerability?
- Explaining Threats, Threat Actors, Vulnerabilities, and Risk Using a Real-World Scenario

Community pick of the week

Thank you @Th4nu_0x0 for participating in our “draw our logo” competition! Enjoy your swag!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com