Bug Bytes #175 – 60 RCEs in 60min, Free Google Play Store ebooks & How to easily parse Burp Project files

BY ANNA HAMMOND · JUNE 22, 2022 · LAST UPDATED ON MARCH 6, 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 weeks from June 13 to 20.

Special announcement

After this issue, **Bug Bytes will be on pause**.

After almost three and a half years of working with Intigriti, I (@PentesterLand) have nothing but respect, admiration and love for this company, its people and culture.

So, it is with great sadness that I am announcing that I have to stop this beautiful collaboration with Intigriti for personal reasons.

I'm beyond grateful to Stijn and Inti for giving me (and so many other content creators!) support and a platform to share knowledge and this passion for hacking.

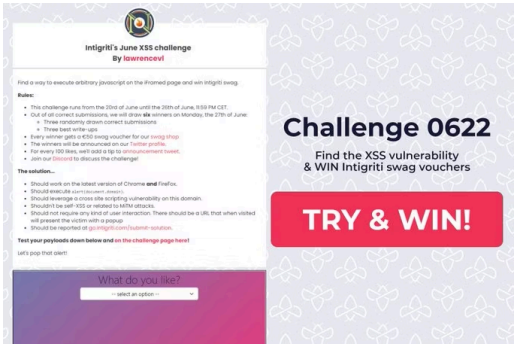
To all of Bug Bytes's faithful readers, thank you for your ongoing support and love.

Hopefully, this won't be the end of Bug Bytes. Until another content creator picks up the torch, I invite you to follow Intigriti's Twitter account, Youtube channel and Intigriti Hackademy to stay informed of any new resources and news.

I also invite you to keep an eye on my list of bug bounty writeups which I continue to update regularly.

Last but not least, Intigriti is **looking for new content creator(s)** to join their community team. If you'd like to work on the next iteration of Bug Bytes, I strongly encourage you to apply at **community@intigriti.com**.

Intigriti news



Intigriti's June XSS challenge By lawrencevl

Our favorite 5 hacking items

1. Conference of the week

60 Remote Code Execution in 60 minutes – Laluka & Slides

If you like RCEs (and who doesn't?!), you will love this talk. @TheLaluka presents 60 ways he obtained unauthenticated RCE, with the full chains and links to learn more about all the vulnerabilities.
Note that the talk is in French, but slides are in English and are full of details, links and good memes.

2. Writeup of the week

How to download eBooks from Google Play Store without paying for them (Google)

This is about an interesting logic flaw that @Yess_2021xD found in Google. It looks simple once explained. However it probably took a lot of persistence and attention to detail to notice the series of behaviors that led to leaking a small part of an ebook, then come up with automation to access the whole ebook.
A very clever and creative finding with great impact.

3. Tutorials of the week

Building on an AppSec Pipeline with Burp Suite data – Part 1 & Part 2
Hack with 'goodfaith' – A tool to automate and scale good faith hacking

If you often find yourself looking for information across multiple Burp project files, @0xRST's burpsuite-project-file-parser is a must. It is two years old but these new tutorials do an amazing job of explaining what the tool does exactly, and how to leverage it for bug hunting with eight concrete examples.

@ryanelkins's goodfaith is another really useful tool for bug hunters and pentesters. It solves the issue of ensuring that you stay within scope when doing recon and large-scale scanning.

4. Tools of the week

xnLinkFinder
PentagridScanController & Related talk

I noticed xnLinkFinder a while ago but didn't have time to play with it and compare it to other endpoint discovery tools like LinkFinder. According to @nullenc0de, it found him more endpoints. So, it'd be interesting to test and look at its code to understand what it does differently.

Another interesting tool is PentagridScanController. It is a Burp extension by @floyd_ch that improves Burp's active scanning by excluding irrelevant requests (e.g. non-repeatable requests). Its behavior is detailed and can be customized.

5. Video of the week

How to get started with and how to improve on secure code review

The best way to learn security code review is by doing it, but it is easier said than done when you are starting out. If this speaks to you, this video might help. @wireghoul reviews some code and shares practical tips and techniques to find 0-days in code.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- I Know Where You Live Thanks to Your Cooking Tutorial
- Bug Bounty Redacted #4: Writing to S3 buckets & Insecure JWT Implementation
- Active Directory
- Configuring SSH Tunnels and VPNs | Ralph May
- Get the Best Python Books for Free
- Fundamental Cryptography in Theory and Python

Podcasts & Audio

- Hacker Valley Red – From Black Hat to Bug Bounties [Pt. 1] with Tommy DeVoss
- Cloud Security Podcast EP71 Attacking Google to Defend Google: How Google Does Red Team

Webinars

- LevelUpX – Series 3: How I hacked 55 Banks & Cryptocurrency Exchanges with Alissa Knight
- Phishing with Microsoft 365 and Microsoft Device Codes | Steve Borosh

- Open House: Real Property OSINT and Researching Public Records

Conferences

- Area41 2022
- Badkeys: Finding Weak Cryptographic Keys At Scale
- DevSecCon24 – 2022
- Comment construire des reverse shells – Rémi Gascou (@Podalirius_)

Tutorials

Medium to advanced

- How to: Look for TLS private keys on Docker Hub
- The State of CSRF Vulnerability in 2022
- Extracting Dynamic Values from Multiple Requests in a Nuclei Template
- Why Are My Junctions Not Followed? Exploring Windows Redirection Trust Mitigation
- Guide to Reversing and Exploiting iOS binaries Part 2: ARM64 ROP Chains
- NTLM Authentication with Firefox & FoxyProxy

Beginners corner

- Virtual Hosting – A Well Forgotten Enumeration Technique
- How to orchestrate Bug Bounty tools with Python and Slack
- How to see the impact installing BApps might have on Burp Suite
- AWS Lambda Command Injection
- Azure Attack Paths: Common Findings and Fixes (Part 1)
- Writing Burp Suite Extension in Python – Part 1, Part 2, Part 3 & Part 4

Writeups

Challenge writeups

- HackTheBox – Paper & Blog post
- Stealing cookies through XSS — VoN — Query Service BCACTF 2022
- Command Injection – Lab #2 Blind OS command injection with time delays
- AWS Misconfigurations (CloudGoat walkthrough)

Pentest writeups

- The Importance of White-Box Testing: A Dive into CVE-2022-21662
- Frontend Security Audit Report – Tornado Cash

Responsible(ish) disclosure writeups

- SmarterStats – Yet Another RPC Framework #Web #gRPC
- How I found 5 CVEs #Web #CodeReview #Automation
- Hacking into the worldwide Jacuzzi SmartTub networkhttps://eaton-works.com/2022/06/20/hacking-into-the-worldwide-jacuzzi-smarttub-network/ #IoT #Web #SPA
- An Autopsy on a Zombie In-the-Wild 0-day #MemoryCorruption

Bug bounty writeups

- Personal Access Token Disclosure in Asana Desktop Application (Asana, $6,100)
- CSRF leads to account takeover in Yahoo! (Yahoo, $3,000)
- Amazon Linux "log4j hotpatch" <1.3-5 local privilege escalation to root (race condition) (Amazon)
- That Pipe is Still Leaking: Revisiting the RDP Named Pipe Vulnerability (Microsoft)
- The Android kernel mitigations obstacle race (Qualcomm)
- Cryptographic Side-Channels (Timing Leaks) in JSBN (Xfinity Opensource)

See more writeups on The list of bug bounty writeups.

Tools

- sfleet: Go utility to manage multiple ssh
- Ermir: An Evil Java RMI Registry
- DFSCoerce: PoC for MS-DFSNM coerce authentication using NetrDfsRemoveStdRoot method
- Aced: DACL parser for Active Directory

Tips & Tweets

- Reverse dynamic ssh tunnels
- @alexjplaskett's thoughts on learning how to find high impact issues in hard targets
- Bypass rate limiting on Ruby on Rails apps
- @garethheyes's new XSS vector which exploits the new Chrome Navigation API

- Resources to learn how to learn

See more tips on this week's Twitter collection.

Misc. pentest & bug bounty resources

- The Open Cloud Vulnerability & Security Issue Database
- elttam's semgrep-rules
- MrTuxracer/advisories
- Awesome iOS Security
- OSINT Attack Surface Diagrams & Video intro
- webs3c.com

Articles

- Exception Handling and Data Integrity in Salesforce
- Embedding Payloads and Bypassing Controls in Microsoft InfoPath
- Evolutionary Multi-Task Injection Testing on Web Application Firewalls & DaNuoYi
- The Security Lottery: Measuring Client-Side Web Security Inconsistencies & TL;DR
- Pulling MikroTik into the Limelight, Slides & Universal "unpatchable" jailbreak for all MikroTik RouterOS versions
- Attacking With WebView2 Applications

Challenges

- The 2022 Google CTF (July 3)
- Intigriti's June XSS challenge By lawrencevl
- BSidesSF CTF 2022 & @itsC0rg1's walkthroughs

Bug bounty & Pentest news

- Cybersecurity
  - Siemens, Motorola, Honeywell and more affected by 56 'ICEFALL' vulnerabilities
  - New Hertzbleed side-channel attack affects Intel, AMD CPUs
  - Debate rages over Microsoft vulnerability practices after Follina, Azure issues
- Upcoming events

    - 2022 Source Zero Con (June 22 – 24)
    - AMA Webinar On Your Kali Linux Experience (June 28)
- Tool updates
    - Help Needed: Fund ZAP Development
    - Support curl to have new cool features added like WebSockets support
    - Burp Professional / Community 2022.6 & Finding client-side prototype pollution with DOM Invader
    - OneListForAll v2.4
    - Introducing Ghostwriter v3.0 (new GraphQL API and CLI)

Non technical

- A hackers guide to FINDING cybersecurity jobs
- The ugly side of collaboration in bug bounties
- Hang Fire: Challenging our Mental Model of Initial Access
- From Physics Student To Red Team Consultant: Josiah Beverton's Story