Bug Bytes #85 – Google Firebase keys worth $30K, How to find a mentor & Abusing Content-Type for WAF bypass & other shenanigans

BY ANNA HAMMOND · AUGUST 26, 2020 · 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.

This issue covers the week from 14 to 21 of August.

Our favorite 5 hacking items

1. Tutorials of the week

Multiple Android User Profiles

Hakluke's Guide to Amass — How to Use Amass More Effectively for Bug Bounties

Did you know you could use multiple user profiles in Android, each with a different set of installed apps? It's not something new but I'm just discovering this and see at least two applications for Android app testing.
As detailed in the tutorial, it helps with authorization tests since you can authenticate to the app you're testing with different credentials. It also helps separate your normal phone apps for everyday usage from your testing environment.

The second tutorial goes over some undervalued Amass options. An interesting because bug hunting is not just about the tools you use, but mostly how you use them.

2. Writeups of the week

Firebase Cloud Messaging Service Takeover: A small research that led to 30k$+ in bounties

How to contact Google SRE: Dropping a shell in cloud SQL

These are fantastic findings and really well-written writeups.

@absshax found many hardcoded Firebase keys in multiple Android apps including ones from Google. He went on an investigation to figure out which keys would give him access to sensitive information or actions. One of them could be exploited to send push notifications to a billion users, facilitating phishing campaigns.
The whole writeup is worth reading with great attention if you want to do research and learn how to go from "Hey, I found a hardcoded key but I'm not sure what it does", to real compromise with a $30K bounty.

The second writeup is a cool RCE on Google Cloud SQL. @wtm_offensi and @epereiralopez were able to abuse it and escalate their limited MySQL privileges to a root shell. It is interesting to see what a complex bug chain leading to RCE on Google looks like!

3. Resource of the week

Content-Type Research

@Black2Fan shared some tricks found by researching the Content-Type header. Browsers process it differently and mistakes in parsing can be used for CSRF and XSS. WAFs and Content-Type checks can be bypassed by specifying multiple types (e.g. “Content-Type: text/plain; application/json”).

4. Conference of the week

LevelUp0x07 – Hack Another Day

I don’t know about you, but I haven’t finished watching hacker Summer Camp conferences, and here’s another one!
LevelUp 0x07 brings us new interesting talks like @InsiderPhd’s intro to AI for bug hunters or @hakluke’s talk on crushing bounties in your first 12 months. Other topics include reverse engineering obfuscated Android apps, recon, reviewing Chrome extensions, etc.

5. Non technical item of the week

How to Initiate Contact With a Mentor

If you’re wondering where to find a mentor, this blog post is just for you. @DanielMiessler gives clear actionable advice on what you need to do to ask for help or get mentorship.
The examples will also give you an idea of the fine line between positive messages for potential mentors and the ones that’d probably be ignored.

Other amazing things we stumbled upon this week

Videos

- SCANNING AT SCALE (masscan, nmap, axiom, recon.dev)
- Interview with a hacker: Stök
- DEFCON Safemode – What I Watched at DEFCON
- Hacking 1Password | Episode 1
- Burp Suite Essentials
- Cobalt Strike BOF Making
- The Stuxnet Story: What really happened at Natanz

- Collecting IPs ft. massdns | shuffledns & Recon – Open Ports | Comparison – Masscan | RustScan | Naabu
- Exploit Subdomain Takeover Vulnerability
- SQL Tutorial For Beginners – SQL Database Design

Podcasts

- Security Now: Microsoft's 0-Day Folly – Microsoft Acts Badly, Canon Ransomware, Mozilla Tries to Pivot
- Risky Business #595 — NSA and FBI document GRU's Linux malware for them
- Darknet Diaries EP 72: Bangladesh Bank Heist
- The InfoSec & OSINT Show 21 – HD Moore & Advanced Asset Inventory Techniques
- PSW #663 – Voice Phishers, 'SpiKey' Lock Picking, & Coffee Cup Hackers

Webinars & Webcasts

- Webcast: What to Expect When You're Expecting a Penetration Test
- Discord Hangouts: Dave Kennedy's Birthday Bash
- Hacker Days: Kubernetes Security: From Control Plane to Layer 7

Conferences

- USENIX Security '20 Technical Sessions

Slides & Workshop material

- KubeCon + CloudNativeCon

Tutorials

Medium to advanced

- Race Conditions Can Exist in Go
- Modern PHP Security Part 2: Breaching and hardening the PHP engine
- Lateral Movement in Azure App Services
- Performing Kerberoasting without SPNs
- Azure AD Pass The Certificate
- Improving Packet Capture Performance – 1 of 3 & 2 of 3

- Template Injection in Documents

Beginners corner

- grep: command-line tools #1
- Javascript for bug bounty hunters — part 1 & part 2
- 5 ways to download a Twitter video
- Alternate Data Streams (ADS)
- Abusing Splunk Forwarders For Shells and Persistence
- Bypass Certificate Pinning in modern Android application via custom Root CA
- SMB: Enumeration & Exploitation & Hardening
- CrackMapExec Basics
- Hunting for low-hanging fruits in SAP Applications

Writeups

Challenge writeups

- @terjanq's XSS Challenges Solutions
- Leveraging JSONP to SOME via HTTP Parameter Pollution
- BugCrowd LevelUp0x07 CTF Writeup
- Solving BugPoC XSS Challenge

Pentest writeups

- From SSRF to Compromise: Case Study
- Why you should always scan UDP ports (part 1/2) & part 2/2
- A Country Hijacking

Responsible(ish) disclosure writeups

- X-Cart 5 <= 5.4.0.12/5.4.1.7 Unauthenticated RCE via File Write #Web #CodeReview 1PHP
- A SmorgasHORDE of Vulnerabilities :: A Comparative Analysis of Discovery #Web #CodeReview #PHP
- Rocket.Chat Cross-Site Scripting leading to Remote Code Execution CVE-2020-15926 #Web
- How To Exfiltrate Internal Information Using Web Proxies. #Web #AV
- GlueBall: The story of CVE-2020–1464 #Windows

- CSRF Protection Bypass in Play Framework #Web
- Openvas Credentials Hunt — Part II #Web
- SSTI in Apache Camel modules #Web #CodeQL
- Vulnerabilities in ATM Milano's mobile app
- Chasing doorbells: Finding IoT vulnerabilities in embedded devices #IoT

Bug bounty writeups

- Stealing your data using XSS
- A perfect duplicate or how to send an email with a spoofed invoice's content
- How I was able to send Authentic Emails as others — Google VRP [Resolved] (Google)
- The Short tale of two bugs on Google Cloud Product— Google VRP [Resolved] (Google)
- Insufficient validation on Digits bridge (Twitter, $5,040)
- pre-auth Stored XSS in comments via javascript: url when administrator edits user supplied comment & Stored XSS in Post Preview as Contributor (WordPress, $650 * 2)
- Denial-of- service By Cache Poisoning The Cross-Origin Resource Sharing Misconfiguration Allow Origin Header (Automattic, $200)
- Get analytics token using only apps permission (Shopify, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Parth: Heuristic Vulnerable Parameter Scanner
- Hackium, shift-refactor & shift-interpreter: A CLI tool, a browser, and a framework for analyzing and manipulating web sites. And a suite of utilities to query and modify JavaScript source
- graphql-path-enum & GraphQL path enumeration for better permission testing: Tool that lists the different ways of reaching a given type in a GraphQL schema.

More tools, if you have time

- gwen001/ejs.sh: Onliner to extract endpoints from JS files of a given host
- crystal-subs & Writing a Subdomain Discovery Tool in Crystal: Simple subdomain discovery tool that uses the Shodan API to grab domain information
- hunterio.sh: Script to gather emails from Hunter.io API

- SuperSu Patcher & Creating a Custom Root by Patching SuperSU: A utility that patches the SuperSu binaries to evade common root detection techniques
- CRLFuzz: A fast tool to scan CRLF vulnerability written in Go
- Grex: A command-line tool and library for generating regular expressions from user-provided test cases
- Digit: Extract endpoints from specific Git repository for fuzzing
- Leecher: Python script that takes a list of URLs and builds a wordlist for content discovery based on the paths extracted
- PaGoDo (Passive Google Dork): Automate Google Hacking Database scraping and searching
- cisagov/crossfeed: External monitoring for organization assets
- Checkov: Static code analysis tool for infrastructure-as-code
- SharpEDRChecker: Checks running processes, process metadata, Dlls loaded into your current process and the each DLLs metadata, common install directories, installed services and each service binaries metadata, installed drivers and each drivers metadata, all for the presence of known defensive products such as AV's, EDR's and logging tools
- Powershell Webserver: A Powershell script that starts a webserver (without IIS). Powershell command execution, script execution, upload, download and other functions are implemented

Misc. pentest & bug bounty resources

- AMA with @securinti
- Smallest possible syntactically valid files of different types
- ffw-content-discovery
- FoxyProxy for Pentesters — Regex Cheat Sheet
- United Bug Bounty program's thank you thread
- The Go Language Guide Web Application Secure Coding Practices & A Quick Intro to Go Language Security Topics
- Script to enable tab completion on all of @pdiscoveryio's tools
- Linux Privilege Escalation: Quick and Dirty

Challenges

- How to play GitLab's Capture the Flag at home

Articles

- PostgreSQL Code Execution: UDF Revisited
- Dynamic analysis of apps inside Android Cloning apps – Part 1 & Repo
- Death from Above: Lateral Movement from Azure to On-Prem AD
- How to Sell Counterfeit Cash on Instagram in 7 Easy Steps
- How SPF, DKIM, and DMARC Authentication Works to Increase Inbox Penetration (Testing) Rates
- Facebook: Classic vs New – Which is Better for OSINT?
- FireWalker: A New Approach to Generically Bypass User-Space EDR Hooking
- Think Private Facebook Profiles Pages Are A Dead End? Think Again! #OSINT

News

Bug bounty & Pentest news

- AWS launches open source tool to protect against HTTP request smuggling attacks
- 2020 CWE Top 25 Most Dangerous Software Weaknesses
- Professional / Community 2020.8.1
- Kali Linux 2020.3 Release (ZSH, Win-Kex, HiDPI & Bluetooth Arsenal) & Kali Linux gets a GUI desktop in Windows Subsystem for Linux
- Mozilla Bug Bounty Program Updates: Adding (another) New Class of Bounties
- Great, now we've got 'legit' companies doing borderline illegal/gray-hat hacking for marketing purposes?

Reports

- 2020 State of the Software Supply Chain
- Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme
- The state of vulnerability management in the cloud and on-premises

Vulnerabilities

- Pretty wild that a malicious mailto: link might attach your secret keys and files from your PC to an outgoing message
- Google fixes major Gmail bug seven hours after exploit details go public
- Google Firebase messaging vulnerability allowed attackers to send push notifications to app users
- Picking Locks with Audio Technology

- Memory leak in IBM DB2 gives access to sensitive data, causes DoS
- New Vulnerability Could Put IoT Devices at Risk
- Virtual shoplifting: Critical flaw found in WooCommerce extension NAB Transact
- A simple telephony honeypot received 1.5 million robocalls across 11 months

Breaches & Attacks

- The Secret SIMs Used By Criminals to Spoof Any Number
- FritzFrog: A New Generation Of Peer-to-peer Botnets
- Experian South Africa data breach may impact millions of residents
- Fearing coronavirus, a Michigan college is tracking its students with a flawed ap
- Security Advisory: Mitiga Recommends All AWS Customers Running Community AMIs to Verify Them for Malicious Code
- Researchers Warn of Active Malware Campaign Using HTML Smuggling
- Team Tnt – The First Crypto-mining Worm To Steal Aws Credentials

Other news

- Former Chief Security Officer For Uber Charged With Obstruction Of Justice
- Browser fingerprinting 'more prevalent on the web now than ever before' – research
- US government built secret iPod with Apple's help, former engineer says
- Artificial intelligence can stop IoT-based DDoS attacks in their tracks – research
- Chromium DNS hijacking detection accused of being around half of all root queries
- Cat and mouse: Privacy advocates fight back after China tightens surveillance controls

Non technical

- Bug Business #9 – Get to know pudsec, Intigriti's Top Hacker in Q1 & Q2
- Hacker Spotlight: Interview With Dawgyg
- Ask a Pen Tester, Part 1: A Q&A With Rapid7 Pen Testers Gisela Hinojosa and Carlota Bindner
- What They Don't Tell You About Being a Bounty Hunter or Security Content Creator
- The Ultimate OSCP Preparation Guide, 2020
- Expiring vs. Permanent Skills
- My first 6 months experience as a Bug Bounty Hunter

- The OPSEC of Protesting
- A Discussion On Serverless Application Vulnerabilities

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 08/14/2020 to 08/21/2020.