Bug Bytes #87 – Google Android Local Arbitrary Code Execution, ADB over WIFI & A bunch of New Relic bug reports

BY ANNA HAMMOND · SEPTEMBER 9, 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 28 of August to 04 of September.

Our favorite 5 hacking items

1. Tutorial of the week

Supercharge Android dev with Scrcpy and ADB WIFI

This will be helpful if you have a physical Android device and want to use it wirelessly from your laptop for tests.

Using Genymotion's scrcpy, you can cast the device's screen on your laptop, use ADB over WIFI, record PoCs or demos from your laptop, etc.

2. Writeups of the week

Oversecured automatically discovers persistent code execution in the Google Play Core Library (Google)
~30 reports by Jon Bottarini (New Relic)

The first writeup is about a local arbitrary code execution vulnerability in Google Play's Core Library. It was possible to target any application (including Google Chrome) by crafting a malicious APK. If a victim installed it, it would perform directory traversal, execute code as the target app and access its data.

The second link is what it looks like when @jon_bottarini plays swith a Web app to get familiar with it. It's about 30 reports of IDOR, Privilege Escalation, Stored XSS and Logic bugs found on New Relic, without recon, on a span of two years. So interesting, and a perfect response for anyone who says there aren't any bugs left to find!

3. Video of the week

How to use ffuf – Hacker Toolbox & ffuf translator

This is an excellent introduction to ffuf. @InsiderPhD explains everything you need to start using this powerful tool now: Options for subdomain bruteforcing, fuzzing parameters and headers, cutting down false positives, handling the output, oneliners for common uses, etc.

4. Resource of the week

Weak JWT secrets dictionary & Intro

This is a list of public JWT secrets found with Google dorking and Google BigQuery. It can be used as a wordlist for bruteforcing JWT signatures. The idea is that sometimes developers only sign JSON Web Tokens without encryption, and copy/paste secrets (like the ones compiled) from tutorials.

5. Tools of the week

Masscan Parser
jf

Two Go tools that help with recon automation: Masscan Parser parses Masscan's output, as the name suggests, and returns IP:port combinations. This is useful for extracting open ports and feeding the list into another tool.
jf is a wrapper around gf which makes it easier to grep for common patterns in text files. jf provides the same functionality but for JSON files.

Other amazing things we stumbled upon this week

Videos

- Bruteforce Attacks and Bypassing Rate Limits with Fireprox
- Hacking 1Password | Episode 2 – Decrypting the Protocol
- Interview with a hacker: Inti from Intigriti (Community manager)
- BugBountys: Writing your own SSRF tool in golang & SSRF-Detector
- $6,5k + $5k HTTP Request Smuggling mass account takeover – Slack + Zomato
- Is Success Luck or Hard Work?
- Why Hackers Love the Number 1,094,795,585
- JavaScript Enumeration in practice with a live example
- Full bug bounty methodology to get you started V 2.0 (Say cheese)

Podcasts

- Security Now: I Know What You Did Last Summer – Russian Tries to Hack Tesla, Web Browser History Research
- Risky Business #597 — Alex Stamos talks news, Pompeo's "clean networks" initiative
- Darknet Diaries EP 73: WANNACRY

- The InfoSec & OSINT Show 23 – Samy Kamkar & Reverse Engineering
- SWN #61 – Slack RCE, Charming Kitten, & KryptoCibule Malware
- SWN #62 – 'Sepulcher' Malware, Tesla Dodges Attack, & Snowden Vindicated? – Wrap Up

Webinars & Webcasts

- Go-ing for an evening stroll: Golang beasts & where to find them & Slides
- Analyzing the OWASP API Security Top 10 for Pen Testers
- Hunting Logic Attacks – A Peak at SEC552: Bug Bounties & Responsible Disclosure
- Webcast: How to Present: Secrets of a Retired SANS Instructor

Conferences

- The Diana Initiative

Tutorials

Medium to advanced

- Diving into unserialize()
- Bypass AMSI by manual modification
- Extracting and Diffing Windows Patches in 2020
- The Hash Monster: ESP32 Tamagotchi For WiFi Cracking
- IoT Security – Part 12 (MQTT Broker Security – 101)

Beginners corner

- Javascript for bug bounty hunters — part 3
- Quick Guide to Using ffuf with Burp Suite
- Getting access to internal source code of multiple organizations
- cors/sop/origin
- Backdooring Android Apps for Dummies
- So, You Got Access To a *NIX System... Now What?
- Abusing COM & DCOM objects
- On secure-shell security: SSH hardening guide

Writeups

Challenge writeups

- Google CTF – Authentication Bypass (video)

Pentest writeups

- How a badly configured DB allowed us to own an entire cloud of over 25K hosts (part 1/2) & Part 2/2

Responsible(ish) disclosure writeups

- Smuggling SIP headers past Session Border Controllers FTW! #SIP
- Inconsistent Behavior of Go's CGI and FastCGI Transport May Lead to Cross-Site Scripting #Web #CodeReview #Go
- Grafana 6.4.3 Arbitrary File Read #Web
- Cloud firewall management API SNAFU put 500k SonicWall customers at risk #Web
- Watchcom Security Group Uncovers Cisco Jabber Vulnerabilities #RCE #XMPP
- Maltego CVE-2020-24656 Analysis #Web #XXE
- Lock screen/Bitlocker bypass/elevation of privilege in Bitlocker #Bitlocker #Windows

Bug bounty writeups

- Exploiting Jira for Host Discovery (Atlassian)
- XSS via unicode characters in upload filename (WordPress, $600)
- Takeover an account that doesn't have a Shopify ID and more (Shopify, $22,500)
- DOM XSS triggered in secure support desk (QIWI, $500)
- Stealing data from customers.gitlab.com without user interaction (GitLab, $3,500)

See more writeups on The list of bug bounty writeups.

Tools

- oobfuzz: Conduct OOB Fuzzing of targets with custom payloads towards callback server
- Fuxi: Penetration Testing Platform
- iblessing: iOS security exploiting toolkit that includes application information collection, static analysis & dynamic analysis
- wadl-dumper: Dump all available paths and/ endpoints on WADL file

- jwt-hack: Go tool for JWT hacking
- mainRecon: Automated reconnaissance docked image
- SNIcat & Intro: Proof of concept tool that performs data exfiltration, utilizing a covert channel method via Server Name Indication, a TLS Client Hello Extension
- Tunshell: Remote shell into ephemeral environments
- Red Commander & Intro: Red Team C2 Infrastructure built in AWS using Ansible!
- MoveScheduler: .NET 4.0 Scheduled Job Lateral Movement q

Misc. pentest & bug bounty resources

- hsts-preload-recon: One-liner bash script for gathering domains from hsts preload list
- imran-parray/Mind-Maps
- IDOR: Attack vectors, exploitation, bypasses and chains
- sh377c0d3/web-payloads
- @bogdantcaciuc7 AMA
- VPS Cheatsheet for bug hunting
- Combinations of default usernames and passwords for the Medusa password cracker
- PhishingKitTracker
- judyrecords: 379 million+ United States court records #OSINT s

Challenges

- trailofbits/not-going-anywhere: A Set of Vulnerable Golang programs
- lucasmartinelle/AnotherVulnerableWebApp
- Vulnerable-AD

Articles

- Privilege Escalation in AWS Elastic Kubernetes Service (EKS) by compromising the instance role of worker nodes
- How To Call Windows APIs in Golang
- How I Hacked Your Vending Machine
- How secure is the PDF file?
- Stopping phishing campaigns with bash – how to poison phishing sites with fake data

News

Bug bounty & Pentest news

- Introducing the GraphQL Add-on for ZAP & ZAP JWT Support Add-on
- Professional / Community 2020.9
- New Web Security Academy topic: Business logic vulnerabilities
- August 2020 Monthly Vulnerability Roundup
- Surprise! Voting app maker roasted by computer boffins for poor security now begs US courts to limit flaw finding
- Facebook's Vulnerability Disclosure Policy
- Facebook to list all WhatsApp security issues on a new dedicated website
- Google Announcing new reward amounts for abuse risk researchers

Reports

- Vulcan Cyber study finds serious problems with vulnerability management
- Average BEC attempts are now $80k, but one group is aiming for $1.27m per attack

Vulnerabilities

- Hackers actively exploiting severe bug in over 300K WordPress sites
- Security in PRIME networks – Current status
- Cisco fixes critical code execution bug in Jabber for Windows
- The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy
- Apps built using Go could be vulnerable to XSS exploits
- Squid proxy addresses web cache poisoning vulnerability with latest release
- Microsoft Defender can ironically be used to download malware

Breaches & Attacks

- Flaw allowed adware slingers to slip past Apple's approval protocol
- TikTok Ad Scams: Insufficient Moderation Leaves 'For You' Page Filled with Dubious Apps, Products and Services
- Cisco warns of actively exploited IOS XR zero-days
- Iranian hackers are selling access to compromised companies on an underground forum

- Attackers abuse Google DNS over HTTPS to download malware
- Low hanging 'Forbidden' fruits: Post-compromise tool targets unguarded Magento flank

Other news

- US federal agencies required to launch security vulnerability disclosure policies
- US court deems NSA bulk phone-call snooping illegal, possibly unconstitutional, and probably pointless anyway
- Microsoft confirms why Windows Defender can't be disabled via registry
- Google Has a Plan to Disrupt the College Degree
- TLS certificate lifespan cut short: A win for security, or cause for chaos?
- Mozilla research: Browsing histories are unique enough to reliably identify users
- AWS introduces Bottlerocket: A Rust language-oriented Linux for containers

Non technical

- Hacker Spotlight: Interview With Mayonaise
- We Didn't Encrypt Your Password, We Hashed It. Here's What That Means:
- Signs You're Following A Fake Twitter Account...
- Build tools around workflows, not workflows around tools
- 8 Steps To Getting The Perfect Mentor For You
- Top 15 XKCD comics for Linux and Unix fans

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 08/28/2020 to 09/04/2020.