Bug Bytes #73 – Hacking JWTs for $100k on Apple, @JobertAbma's founder stories & Chaining bugs for fun and profit

BY ANNA HAMMOND · JUNE 3, 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 22 to 29 of May.

Our favorite 5 hacking items

1. Video of the week

@JobertAbma Talks about HackerOne, Entrepreneurship, Hacking, Bug Bounties and his recon approach!

@JobertAbma's story is fascinating. As a hacker and entrepreneur myself, I hung on his every word during this deliciously long interview. He tells the backstory of HackerOne, how he started this successful business with @michielprins while being a student and still finding the time to hack, his hacking process, and much much more!

2. Writeups of the week

– Zero-day in Sign in with Apple (Apple, $100,000)

– My Expense Report resulted in a Server-Side Request Forgery (SSRF) on Lyft (Lyft)

Read the first writeup if you want to see what a $100,000 bug looks like. It's surprisingly easier (to understand at least) than one might think: "Sign in with Apple" had a flaw that allowed for generating valid JWTs for any Email ID. This resulted in account takeover on any apps using Apple's sign-in functionality.

The second writeup's video is nice to watch if you need inspiration for hacking. The bug is an SSRF affecting the WeasyPrint PDF generator. @NahamSec talked about it before, but it's lots of fun to watch hackers hacking Lyft while taking Lyft rides!

3. Resource of the week

RandoriSec Mobile Hacking Workshop – iOS & Android

@RandoriSec have a track record of sharing awesome mobile hacking resources. This time, they released slides and material used for BSides Budapest 2020 workshops. This includes intentionally vulnerable apps for practicing, and slides providing theory and steps to solve the challenges.

An excellent opportunity to get into mobile hacking!

4. Slides of the week

Android app vulnerability classes

This is a valuable resource for anyone interested in Android app hacking or in the Google bug bounty program. The document provides an overview of the program's 19 most commonly reported vulnerabilities, with auditing and remediation tips.

Because this is about bug bounty, the bugs described are the type that will earn you bounties, not just good security practices or low-impact bugs. So, definitely worth a read!

5. Non technical item of the week

My self-help guide to making sense of a confusing world

How can one avoid being deceived by fake news and disinformation campaigns? This is a question @halvarflake asked himself. His answer comes in the form of a long article detailing 7 habits he came up with to regularly examine his own beliefs.

This piece might seem too theoretical but actually provides an excellent framework for critical thinking and practicing self-critique, which is essential in these turbulent times.

Other amazing things we stumbled upon this week

Videos

- Katie Explains: My Methodology
- BOUNTY THURSDAYS – Reconless, Axiom, DNSObserver, GF-Patterns, Pimp my terminal
- Bug bounty 101: writing a good report with Intigriti tips from community and triage team
- Live RECON ft. Neoshaman & neoshaman1105/bug-hunting-toolkit
- Bug Bounty Methodology: Recon in action
- Bug Bounty Bits: Importing H1 scope into burp (HackerOne)
- Bug Bounty Bytes: Lets tackle DOM XSS
- My own basic bounty methodology: Bug Bounty Bytes
- What is the dark web? Your questions answered, in plain English

Podcasts

- A Day in the Life of an Ethical Hacker: Büşra Turak

- Security Now 768 – Contact Tracing Apps R.I.P.
- Risky Business #585 — UK mulls Huawei ban, NGOs urge COVID-19 hack de-escalation
- Darknet Diaries EP 66: Freakyclown
- Layer 8 Podcast Episode 27: TrustedSec Social Engineers Ask Me Anything
- The Many Hats Club Ep. 85, Time has no meaning anymore (with Stu and a lot of guests)
- Naked Security Podcast S2 Ep 41: Super-sized ransomware, FBI v Apple and AirPods hot or not
- SWN #37 – Rogue Drones, Sarwent Malware, Microsoft MFA Attack
- Ragnar Locker, Windows Hello, & OpenSSH – Wrap Up – SWN #38
- PSW #653 – 2020 MITRE ATT&CK Malware Trends – Greg Foss
- PSW #653 – Ed Skoudis & Security News

Webinars & Webcasts

- How to Hunt for Jobs like a Hacker
- Webcast: Kerberos & Attacks 101 & Slides
- Securing Office 365 and Azure AD Defend Your Tenant
- Securing Active Directory: Resolving Common Issues
- Who's Your Hacker – Episode 8 Breaking Into Your Building: A Hackers Guide to Unauthorized Access
- SANS webinars
  - Mobile Application Dynamic Analysis
  - Post Modern Web Attacks: Cloud Edition
  - SANS @MIC Talk – Tricking modern endpoint security products

Conferences

- Detect complex code patterns using semantic grep
- vOPCDE #5 | Mobile Tracking, Xiaomi, Aarogya Setu, and Chrome Sandbox escape.
- Null Ahmedabad May 2020 meetup & Slides
- Kubernetes from a Attacker's Perspective & Slides

Tutorials

Medium to advanced

- SQL Injection – MySQL comment: the double dash mystery
- How to Hide Secrets in Strings— Modern Text hiding in JavaScript
- Automating a RedELK Deployment Using Ansible
- Introducing Proxy Helper – A New WiFi Pineapple Module & Proxy Helper
- Bypass Defender and other thoughts on Unicode RTLO attacks
- Automate Octopus C2 RedTeam Infrastructure Deployment
- Hijacking Library Functions and Injecting Code Using the Dynamic Linker
- AppDomainManager Injection and Detection

Beginners corner

- BEGINEER'S CRASH COURSE FOR FINDING ACCESS CONTROL VULNERABILITIES IN THE WEB APPS:PART 1
- OSCP: Understanding SSH Tunnels
- Pentesting 101: Working With Exploits
- RCE on Windows from Linux Part 4: Keimpx
- Leveraging Street Art in OSINT Investigations
- The Bash Scripting Tutorial, Part 4
- Investigate TikTok Like A Pro!
- SecretsDump Demystified
- Kerberos: Achieving Command Execution using Silver Tickets

Writeups

Challenge writeups

- Attacking CloudGoat 2
- The Tangled Browsers: Beyond XSS (Part 1)

Pentest writeups

- Tampering Encrypted Parameter to Account Takeover
- Extracting credentials from a remote Windows system – Living off the Land

Responsible(ish) disclosure writeups

- StrandHogg 2.0 – The 'evil twin' #Android

- Exploring macOS Calendar Alerts: Part 2 – Exfiltrating data (CVE-2020-3882) #MacOS
- Moodle DOM Stored XSS to RCE #Web #RCE
- Android App Hacking: Hardcoded Credentials #Android
- Abusing PackageKit on Fedora/CentOS for fun & profit (from wheel to root). #Linux
- Security Flaws in Adobe Acrobat Reader Allow Malicious Program to Gain Root on macOS Silently #MacOS #PrivEsc

Bug bounty writeups

- How dangerous is Request Splitting, a vulnerability in Golang or how we found the RCE in Portainer and hacked Uber (Uber)
- IDOR in session cookie leading to Mass Account Takeover ($2,000)
- Attacker with an Old account might still be able to DoS ctf.hacker101.com by sending a Crafted request (HackerOne, $500)
- [Critical] Insufficient Access Control On Registration Page of Webapps Website Allows Privilege Escalation to Administrator (U.S. Dept Of Defense)
- Pixel flood attack cause the javascript heap out of memory (Node.js third-party modules)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- BurpIntruderDownloader/extract.py & Extracting files from Burp Intruder Output
- DNSObserver & Intro: A handy DNS service written in Go to aid in the detection of several types of blind vulnerabilities. It monitors a pentester's server for out-of-band DNS interactions and sends lookup notifications via Slack
- httpx: A fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library, it is designed to maintain the result reliability with increased threads

More tools, if you have time

- Elevate: Vertical Domain Discovery
- Needle: Instant access to you bug bounty submission dashboard on various platforms + publicly disclosed reports + #bugbountytip
- Ligolo: Reverse Tunneling made easy for pentesters, by pentesters
- EXCELntDonut: XLM (Excel 4.0) Macro Generator for Phishing Campaigns

- Cillian-Collins/subscraper: Recon tool which scans JavaScript files for subdomains & then iterates over all JS files hosted on subsequent subdomains to enumerate a list of subdomains for a given URL
- ParamCleaner: Removes duplicate entries from a file, resulting in only unique parameter combinations. Useful for parsing waybackurls and making recon more effective
- CorsMe: Cross Origin Resource Sharing MisConfiguration Scanner
- Kalu: Keeping ArchLinux Up-to-date
- RepoPeek: Python script to get details about a repository without cloning it
- Kubetap: Kubectl plugin to interactively proxy Kubernetes Services with ease
- Waybackcollector & How it differs from existing tools like Waybackurls & GAU: Fetch wayback machine historical content for a given url
- imran-parray/paramReplacer.py: ython script which replaces the parameter values in target URL's with your desired input, for fuzzing & mass testing
- S3BucketList: Firefox plugin that lists Amazon S3 Buckets found in requests
- go-windapsearch: Utility to enumerate users, groups and computers from a Windows domain through LDAP queries
- apkLeaks: Scanning APK file for URIs, endpoints & secrets

Misc. pentest & bug bounty resources

- Q&A session with InsiderPhD
- Practical Python Programming
- Identify SalesForce custom domains against bug bounty programs
- 100 Hacking Tools and Resources
- Ffufalias
- MobexlerLite
- A Red Team Maturity Model
- Top 30+ Most Popular Red Team Tools
- The Art Of Command Line
- Amazon Web Services described each in 1 sentence

Challenges

- h1-ctf

- @gynvael's Node.js / Express Web Security Challenge Level 6
- Bust-a-Kube: An intentionally-vulnerable Kubernetes cluster
- Kubernetes Easter CTF
- DefCon CTF Quals – uploooadit challenge, Walkthrough video & Written walkthrough
- S3 game – Amazon S3 challenge
- New Web Security Academy topic & labs: Authentication

Articles

- I am a security researcher who has found hundreds of bugs and vulnerabilities. Ask me anything about the best methods for finding bugs and spotting emerging vulnerabilities
- Safely and Quickly Brute-Force Java RMI Interfaces for Code Execution & RMIScout
- These Aren't the Phish You're Looking For
- Promiscuous Wireless Packet Sniffer Project
- Bringing VandaTheGod down to Earth: Exposing the person behind a 7-year hacktivism campaign #OSINT
- Being Stubborn Pays Off pt. 1 – CVE-2018-19204 & pt. 2 – Tale of two 0days on PRTG Network Monitor
- DNS Rebinding: Stealing WiFi credentials through your solar panel inverter

News

Bug bounty & Pentest news

- Google launches CTF-style bug bounty challenge for Kubernetes
- Bug Bounty 101: How to Choose Your First Bug Bounty Target and Stay Motivated: June 15
- A one million milestone for the Web Security Academy
- The Journey in Data: HackerOne Hits 100 Million Dollars in Bounties
- HackFest & Ranges Summit – Live Online

Reports

- Python and Go Top the Chart of 2019's Most Popular Hacking Tools
- Analysing over 1M leaked passwords from the UK's biggest companies
- Summary of Tradecraft Trends for 2019-20: Tactics, Techniques and Procedures Used to Target Australian Networks

- Google TAG's updates about government-backed hacking and disinformation
- Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cybercriminal Forums

Vulnerabilities

- Android 'StrandHogg 2.0' flaw lets malware assume identity of any app
- LadderLeak: Side-channel security flaws exploited to break ECDSA cryptography
- RangeAmp attacks can take down websites and CDN servers

Breaches & Attacks

- How iPhone Hackers Got Their Hands on the New iOS Months Before Its Release
- GitHub warns Java developers of new malware poisoning NetBeans projects
- Discord client turned into a password stealer by updated malware
- Steganography in targeted attacks on industrial enterprises
- Thousands of enterprise systems infected by new Blue Mockingbird malware gang
- Valak 2.0: The malware loader turned information stealer
- Russian cyberspies use Gmail to control updated ComRAT malware
- Qihoo & Baidu disrupt malware botnet with hundreds of thousands of victims
- RATicate drops info stealing malware and RATs on industrial targets
- Voter info for millions of Indonesians shared on hacker forum
- Cisco hacked by exploiting vulnerable SaltStack servers

Other news

- Android security: Regional differences make mobiles devices in some countries more hackable than others
- List of well-known web sites that port scan their visitors
- Shodan founder John Matherly on IoT security, dual-purpose hacking tools, and information overload
- India said its coronavirus contact-tracing app is perfect... adds bug bounty and open-sources it anyway
- Microsoft blocks Trend Micro code at center of driver 'cheatware' storm from Windows 10, rootkit detector product pulled from site
- New fuzzing tool finds 26 USB bugs in Linux, Windows, macOS, and FreeBSD

- Twitter places public interest notice on President Trump's tweet
- Vigilante hackers target 'scammers' with ransomware, DDoS attacks
- Contact-tracing app may become a permanent fixture in major Chinese city

Non technical

- Discover Unlisted Bug Bounty Programs with Google Dorks
- Phone Number Privacy? We don't do that here: Google Hangout Call!
- Coping up with Bug Bounty Failures
- Security Lessons From Hacker-Themed Board Games
- Series by 4 social engineers on their first on-site social engineering engagement: 1, 2, 3 & 4
- Why OPSEC Is For Everyone, Not Just For People With Something To Hide – Part III

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 05/22/2020 to 05/29/2020.