Bug Bytes #52 – Account takeover via HTTP Request Smuggling, Lesser-known Tools for Android Application PenTesting and Hunting Credentials and Secrets in iOS Apps

BY INTIGRITI · JANUARY 7, 2020 · LAST UPDATED ON JULY 30, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

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 27 of December to 03 of January.

Our favorite 5 hacking items

1. Video of the week

> "Finding Your First Bug: Goal Setting / Remote Code Execution (RCE)"

This title is voluntarily misleading. The video is not exactly about finding RCEs, rather how to use goal setting and motivation to learn and eventually get your first RCE.
This comes at a perfect time when many hackers (especially bug hunters) are sharing their goals for the new year.
But there is a huge different between a goal expressed as a wish, and measurable and realistic goals accompanied by an actionable plan.
So, this is an absolutely must watch if you want to learn about goal setting (using the S.M.A.R.T. method) applied to bug bounty, how to create an action plan (using the GROW method), non technical skills you need to develop as a hacker, and much more.
If I could like this a hundred times, I would! Thanks @InsiderPhD

2. Writeup of the week

> "Account takeover via HTTP Request Smuggling"

This is an excellent walkthrough of a HTTP Request Smuggling attack. It goes beyond detection and shows how to confirm and exploit the vulnerability for account takeover.
This is interesting because simple detection with Burp's Request Smuggler plugin is not enough, as it is prone to false positives.

3. Tools of the week

> "– Endpointdiff
> – Hakrawler & Introduction"

These are two nice additions to a Web app tester's arsenal.
Endpointdiff can help with JavaScript files monitoring. Its uses LinkFinder to retrieve endpoints from JS files and compares the output with the previous results.
Hakrawler is described as a simple, fast web crawler designed for easy, quick discovery of endpoints and assets. It is similar to Photon but written in Go and made for crawling large lists of domains. It also has an option to export the results for chaining with other tools like Sqlmap.

4. Resource of the week

> "Lesser-known Tools for Android Application PenTesting"

Amazing article by @CaptMeelo for anyone interested in testing the security of Android apps.
It's about some tools he finds helpful for assessments. They are useful for:

- Bypassing protections against screenshots
- Byassing Root detection
- Using ADB over Wifi
- A better method for retrieving logs (simplified and colorful output)
- Removing the terminal size limitation when using ADB shell

– Low-Hanging Apples: Hunting Credentials and Secrets in iOS Apps
– Password Spraying Dell SonicWALL Virtual Office

The first link is a cool tutorial by @spaceraccoonsec on finding credentials and secrets in iOS apps.
Methods explained include both static and dynamic analysis.
These are the basics that can help snag heasy bounties or help with traditional penetration testing. Very helpful indeed!
The second tutorial by @n00py1 goes through a situation where using Burp Macros was necessary. The login functionality he was testing used a CSRF token. So, it was not possible to test it with Intruder without setting up a macro and creating a session handling rule. The article shows exactly how to do that.

Other amazing things we stumbled upon this week

Videos

- How to Build an Active Directory Hacking Lab
- iOS 13 / 12 How To Sign / Install Unc0ver Jailbreak & Other IPAs Without Cydia Impactor & No Revokes

- StrandHogg Bug – Unpatched Android OS Vulnerability

Podcasts

- Security Now 747 – The Year's Best
- Erez Yalon — The OWASP API Security Project
- The Privacy, Security, & OSINT Show 151-Your New Smart TV & CCPA Details
- Paul's Security Weekly #632 – Security History – Lessons from the past
- Paul's Security Weekly #633 – Diplomacy, Norms and Deterrence in Cyberspace – Chris Painter
- Paul's Security Weekly #633 – Security News: January 2, 2020
- Coalcast Episode S1E10 – Hacky Holidays
- 10 Questions – TinkerSec

Webinars & Webcasts

- 20191223 The OSINT Curious Special Facebook Webcast
- What you Need To Know About The Critical Citrix Gateway (Netscaler) Vulnerability CVE-2019-19781

Conferences

- 36C3

Tutorials

Medium to advanced

- I don't need no proxy
- iOS Application Injection
- How to Conduct Jailed Testing with Frida
- Hacking Web using Images (CHIRA Attack Vector) & Demo
- Bypass OkHTTP CertificatePinner on Android (by replacing the certificate hash with Burp's)
- LOLbins not tested against Windows Defender
- Using the InterPlanetary File System For Offensive Operations
- Process Injection – Part V

Beginners corner

- Cross-Origin Resource Sharing (CORS)
- Clickjacking
- Different Types of Root Detection Techniques In Android
- Android Root Detection Bypass Using Objection and Frida Scripts
- Nmap: Perform Information Gathering — Beginners Detailed Explanation
- How Can We Use Messenger Apps in OSINT?
- Hacking a $5 Smartband

Writeups

Challenge writeups

- Clobbering the clobbered vol. 2
- Fake Shell with Python Requests
- PHP Tricks in Web CTF challenges
- CyberTruck Challenge 2019 — Android CTF

Pentest writeups

- Hack Reset Password Code Using Open Redirect
- Hack User Account Via Activation link
- Cocktail of Vulnerabilities

Responsible(ish) disclosure writeups

- Yet Another .NET deserialization #Web #RCE
- Exploiting Wi-Fi Stack on Tesla Model S #Wifi #CarHacking (TIL China has its own CVE like database called China National Vulnerability Database (CNVD))
- D-Link DIR-859 —Unauthenticated RCE (CVE-2019–17621) [EN] #RCE #CodeReview
- Zero day vulnerabilities in Determine Selectica Contract Lifecycle Management (SCLM) v5.4 #Web
- Alert Alarm SMS exploit – English version #IoT

Bug bounty writeups

- Drop the mic?! no! Drop the connection
- Lack or Origin check leads to Cross-Site Websocket Hijacking (CSWSH) on Coda ($800)
- Protected Tweet settings overwritten by other settings on Twitter ($1,540)

- Abusing ImageMagick to obtain RCE ($5,000)
- How did I earn $3133.70 from Google Translator? ($3,133.70)
- Bypass Mobile PIN Verification ($100)
- Bug Hunting Journey of 2019 ($2,500)
- How I made $7500 from My First Bug Bounty Found on Google Cloud Platform ($7,500)
- Exploiting HTML Injection in Email

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Parsuite & Introduction: Simple parser framework
- Random_user-agent.py: Script to make every request through Burp have a random User-Agent. Combined with the Python Scripter Burp Extension & proxycannon-ng, your traffic will be tougher to fingerprint

More tools, if you have time

- Turbolist3r: A fork of the sublist3r subdomain discovery tool. In addition to the original OSINT capabilties of sublist3r, turbolist3r automates some analysis of the results, with a focus on subdomain takeover.
- Bountystrike-sh
- Dirlstr: Finds Directory Listings or open S3 buckets from a list of URLs
- Kostebek: A reconnaissance tool which uses firms' trademark information to discover their domains
- IotShark: Monitoring and Analyzing IoT Traffic
- PENIOT: Penetration Testing Tool for IoT
- PHP Version Audit: Audit your PHP version for known CVEs and patches
- HiddenEye: Modern Phishing Tool With Advanced Functionality And Multiple Tunnelling Services
- TrelloC2: Simple C2 over the Trello API

Misc. pentest & bug bounty resources

- First full version of the Cyber Security Body of Knowledge published
- The Best Write-ups that 2019 Brought Us
- Red Team Notes

- My go-to list as a security professional
- Awesome-mobile-security
- Database Security Cheat Sheet (New OWASP Cheat Sheet)
- Compatible Wireless Penetration Hardware for Kali Rolling
- Active Directory Security Fundamentals

Challenges

- OSINT quiz by @Sector035
- Web Cache Poisoning Lab
- XSS challenge by @PwnFunction & Solution

Articles

- AWS EC2 IMDSv2 versus an esoteric HTTP Method
- Promiscuous Cookies and Their Impending Death via the SameSite Policy
- Revised Homograph Attacks
- Matrix.org hack
- The Paper Password Manager
- Debugging in prod: Maximizing user attack surface
- Why npm lockfiles can be a security blindspot for injecting malicious modules
- From Zero to Lateral Movement in 36 Minutes
- BRONZE PRESIDENT Targets NGOs
- Empirically Assessing Windows Service Hardening
- Looking into Attacks and Techniques Used Against WordPress Sites

News

Bug bounty & Pentest news

- Top 10 web hacking techniques of 2019 – nominations open
- Kali Default Non-Root User
- If you wonder why the recent discussions (articles, etc...) about offensive cybersecurity tools and possibly regulating those... Well, offensive cyber tools are now officially designated as munitions.

- OWASP API Security Top 10 – 2019 edition released
- Sorry to 2019, 2020.. let's improve & hack it
- Apple Is Bullying a Security Company with a Dangerous DMCA Lawsuit: "If Apple Wins, We All Lose"
- Memorable Metasploit Moments of 2019

Vulnerabilities

- First externally discovered flaws in Microsoft Edge (Chromium) uncovered
- FPGA cards can be abused for faster and more reliable Rowhammer attacks
- Patch now: High risk vulnerabilities found in network traffic monitoring tool
- First externally discovered flaws in Microsoft Edge (Chromium) uncovered
- Google kills Xiaomi-Nest integration after user gets images from strangers

Breaches & Attacks

- Chrome extension caught stealing crypto-wallet private keys
- Landry's restaurant chain disclose POS malware incident
- Sextortion Email Scammers Try New Tactics to Bypass Spam Filters
- Cybercriminals Fill Up on Gas Pump Transaction Scams Ahead of Oct. Deadline
- Starbucks Devs Leave API Key in GitHub Public Repo
- Company shuts down because of ransomware, leaves 300 without jobs just before holidays

Malicious apps/sites

Other news

- The year in #StupidSecurity – 2019's biggest security and privacy blunders
- Mean Time to Hardening: The Next-Gen Security Metric
- Brazil surpasses UK in Facebook fine over Cambridge Analytica scandal
- Python is dead. Long live Python!
- Microsoft Products Reaching End of Life in 2020
- California Adopts Strictest Privacy Law in U.S.
- China's TikTok banned by US Army amid security concerns: Report
- U.S. Government Issues Warning About Possible Iranian Cyberattacks
- The FBI Wanted a Back Door to the iPhone. Tim Cook Said No

- BusKill Cable Starts a Self-Destruct Routine on Stolen Laptops
- Oh, Behave! Who Made It to Rapid7 Labs' Naughty List(s) in 2019?
- 2020 Cybersecurity Trends to Watch
- Binary Blogger Tech Predictions for 2020

Non technical

- Hacker impression: my first live hacking event!
- What I've Learned in Over a Decade of "Red Teaming"
- Old Skool Red Team
- Adding to the Dialogue – On the Release of Offensive Security Tools (OST)
- The CEO of $48 billion Shopify says long hours aren't necessary for success: 'I'm home at 5:30pm every evening'
- Maker vs. Manager: How Your Schedule Can Make or Break You

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 12/27/2019 to 01/03/2019.

The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.

Curated by Pentester Land & Sponsored by Intigriti