Bug Bytes #171 – New Android Web Views attacks, Arbitrary file theft on Android & Scanning for PII in images

BY ANNA HAMMOND · MAY 25, 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 May 16 to 23.

Our favorite 5 hacking items

1. Tool of the week

Octopii & Intro

Octopii is a Personal Identifiable Information (PII) scanner for images. It uses tesseract-ocr and AI to identify images of passports, photos, signatures, etc. This can be useful for automated recon, when you have access to a lot of images (in a local directory, S3 bucket or via directory listing) and cannot go through all of them manually.

2. Writeup of the week

Variant Cloud Analysis

@jespinhara found a Tomcat Manager that used default credentials on a public bug bounty program. The vulnerable host could only be accessed from a *t2.xlarge* AWS instance in the *us-east-1a* region, which probably explains why the bug wasn't discovered before.
So, a valuable lesson for recon automation and vulnerability scanning is to try different cloud providers, regions and instance types.

3. Video of the week

LevelUpX – Series 1: Salesforce Object Recon with B3nac & AuraIntruder

@B3nac shares how to find data leaks by disclosing Salesforce Objects using different techniques, and a Burp extension to automate the process.

4. Tutorials of the week

Ruby Vulnerabilities: Exploiting Dangerous Open, Send and Deserialization Operations
Android security checklist: theft of arbitrary files

@0x00C651E0 three of the most common ways to obtain RCE on Ruby on Rails apps. Although they can be detected with Brakeman, this walkthrough will help go further and construct working exploits.

The second tutorial / cheat sheet by @OversecuredInc is a compilation of multiple techniques to exploit Android apps and access arbitrary files.

5. Articles of the week

The Bridge between Web Applications and Mobile Platforms is Still Broken
Security Code Audit – For Fun and Fails

The first paper presents two new attacks using Android Web Views. One allows leaking user information and the other accessing the user's camera and microphone.

The second paper is an insightful tale of "failed" code review by @frycos. It is very interesting to read about a code auditor's methodology whether there is an RCE at the end or not.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty 101: #18 – Approaching a Public Target (Pinterest) & Interview #4: Question and Answer Session #1
- INDUSTRY Penetration Testing & Training w/ Jean-François Maes
- Stop making excuses
- Hacking networks with Python // Creating malicious packets and breaking TCP/IP rules

Podcasts & Audio

- 401 Access Denied, especially:
  - Creativity, Community, and Bug Bounties with STÖK
  - Hacking the Penetration Test with FC (aka Freaky Clown)
  - Privilege Escalation Using Hack Tricks with Carlos Polop

Webinars

- A Quick Introduction to Manual Source Code Review & Slides

Conferences

- Finding Bugs on NFT Websites for Fun & Profit | IWCON-S22 Talk by Zseano

- Security Automation, (Re) Defined | IWCON-S22 Talk by Dhiyaneshwaran DK
- Nullcon Berlin 2022
- BSides Munich 2022

Tutorials

Medium to advanced

- Azure Virtual Machine Execution Techniques
- Exfiltrating data from a restricted Windows environment using DNS
- Constrained Delegation Considerations for Lateral Movement

Beginners corner

- Abusing S3 Bucket Permissions
- Which Single Sign-On (SSO) is for you? SAML vs OAuth vs OIDC
- XSLT Injections for Dummies

Writeups

Challenge writeups

- CTF Writeup: 2022 HTB Cyber Apolcalypse Web Challenge: Genesis Wallet
- HackTheBox – Pandora & Blog post
- Clean url as a Service

Responsible(ish) disclosure writeups

- Leaking Your GitHub Repositories With Snyk Code #Web
- Yik Yak Vulnerability Exposed Precise GPS Locations: Analysis #iOS
- Mailcow RCE and domain admin privilege escalation (CVE-2022-31245) #Web
- Galleon NTS-6002-GPS Command Injection vulnerability (CVE-2022-27224) #Web
- Printing Fake Fiscal Receipts – An Italian Job p.2 & p.1 #Printers #Android

Known vulnerabilities

- "NginxDay2022": NGINX LDAP reference implementation Zero Day Vulnerability
- How I could exploit the CVE-2022-1388, F5 BIG IP iControl Authentication bypass to RCE

Bug bounty writeups

- Stealing Google Drive OAuth tokens from Dropbox (Dropbox, $1,728)
- Breaking Reverse Proxy Parser Logic
- Finding vulnerabilities in Swiss Post's future e-voting system – Part 2 (Swiss Post)
- Integer overflow vulnerability (Glovo)

See more writeups on The list of bug bounty writeups.

Tools

- h2cSmuggler-proxy: Python script that implements a proxy over h2cSmuggler so you can navigate in your browser making requests to the back-end server
- mx-takeover: Go tool that detects misconfigured MX records using three techniques
- slipit: Utility for creating ZipSlip archives
- righettod/toolbox-pentest-web: Docker toolbox for pentest of web based application

Tips & Tweets

- Accessing an Air Force database via SQL injection
- One of @joernchen's most memorable bugs
- Google dorking for IP addresses
- Combine gron and diff when hacking APIs to see differences in responses
- XSS bypass tip

Misc. pentest & bug bounty resources

- @thedawgyg's Twitch channel
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- Vulnerabilities 1001: C-Family Software Implementation Vulnerabilities
- UNREDACTED Magazine
- Awesome CTF resources

Articles

- A Few Tailscale Tricks For Security Testers
- Dotnet's Default AES Mode Is Vulnerable To Padding Oracle Attacks

- We Love Relaying Credentials: A Technical Guide to Relaying Credentials Everywhere
- No-Fix Local Privilege Escalation Using KrbRelay With Shadow Credentials

Challenges

- Dig Dug (Free TryHackMe challenge room)

Bug bounty & Pentest news

- Bug bounty
  - Pwn2Own Vancouver: 15th annual hacking event pays out $1.2m for high-impact security bugs
  - Eight years of the GitHub Security Bug Bounty program
- Cybersecurity
  - US revises policy regarding Computer Fraud and Abuse Act, will not prosecute good faith research
  - Firefox debuts improved process isolation to reduce browser attack surface
- Upcoming events
  - "Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling" (@albinowax's talk at Black Hat USA 2022)
- Tool updates
  - Kali Linux 2022.2 Release
  - Why Parrot OS 5.0 LTS "Electro Ara" is a milestone
  - Nuclei v2.7.1
  - Hakrawler v2.1
  - Metabigor v1.12
  - Osmedeus v4.1.2