Bug Bytes #57 – Th3G3nt3lman's Secret Recon Methods, Checkmarx VS API's & Vulns in React Native Apps

BY INTIGRITI · FEBRUARY 11, 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 31 of January to 07 of February.

Our favorite 5 hacking items

1. Tools of the week

> "– Quiver & Introduction
> – PlaystoreDownloader"

The first tool tries to solve the inconvenience all bug hunters and pentesters face: Having to use so many different tools, to remember their command line options, to juggle between terminals and note-taking apps, copy-pasting commands...
Quiver allows you to run recon scripts or single commands organized into categories with auto-completion, and to access markdown notes from the terminal. This last feature is really interesting. It makes it possible to manage a markdown knowledge base that can be accessed from both GUI (with an app like Joplin) and CLI.
The second tool is handy for Android application tests. It helps download APKs directly from the Google Play Store using the command line. Practical if you want to automate APK downloads.

2. Video of the week

> "@Th3G3nt3lman Shares His Recon Methodology and How He Consistently Collects $15,000 Bounties! & Summary notes"

This is a must watch if you want to up your recon game. @Th3G3nt3lman shares so many good gems, especially on how he differentiates himself, and finds assets/bugs that everyone has missed.
He has a full-time job and hunts for only 4/5 hours a week. Using strategies like quick/smart assets enumeration (e.g. building custom short lists) helps him make the most of his time. This clearly shows that time is no excuse!

3. Tutorial of the week

> "Expanding the Attack Surface: React Native Android Applications"

Assetnote's specialty is reconnaissance. So it is worth listening when they're talking about expanding attack surface.
This tutorial shows how to extract JavaScript from React Native Android apps (without decompiling with dex2jar). Then how to analyze it and find juicy information (think endpoints, API keys, Firebase credentials, etc).

4. Conference of the week

> "Meetups at Checkmarx: API Security Concerns (Part II)"

This is an excellent talk about API security testing. @InonShkedy covers multiple vulnerability types including mass assignments, CSRF (and how to combine them), BOLA, 2 complex account takeovers he found, etc.
The company he works for, @traceableai, also shared 31 tips on API security & pentesting.
These are both awesome resources for anyone who wants to dive into API security.

5. Tip of the week

> "When testing for SSRF, change the HTTP version from 1.1 to HTTP/0.9 and remove the host header completely. This has worked to bypass several SSRF fixes in the past"

Cool SSRF technique shared by @thedawgyg. Switching to HTTP/0.9 allows you to remove the Host header (because it is not required in this version as opposed to HTTP/1.1). This can help bypass fixes.

Other amazing things we stumbled upon this week

Videos

- Debrief on the Arrest of Coalfire Pen Testers in Iowa with Brian Krebs
- Bug In Focus: Remote Code Execution (RCE)
- 10 Minute Tip: Viewing LinkedIn Profiles Anonymously
- Cyber Security Salaries, Skills and Stress (ft. Exabeam)
- How to use Portspoof (Cyber Deception) – John Strand

Podcasts

- Darknet Diaries EP 58: OxyMonster
- Security Now 752 – The Little Red Wagon
- Risky Business #571 — Is Joshua Schulte The Shadow Brokers?
- Security Weekly News #9 – Iranian Campaign, Twitter Conspiracy, Bangladesh Hacked
- Application Security Weekly #94 – Xbox Bounty Program, Magento Patch, RCE in OpenSMTPD

Webinars & Webcasts

- Employee, Contractor, Consultant: Which Work Model is Best For You?

Slides only

- Frans Rosén Keynote at BSides Ahmedabad
- Modern Web Security: The Art of Creating and Breaking Assertions
- Don't Cross Me! Same Origin Policy and all the "cross" vulns: XSS, CSRF, and CORS
- Revisiting ReDoS: A Rough Idea of Data Exfiltration by ReDoS and Side-channel Techniques
- Democratizing Electron.js Security

Tutorials

Medium to advanced

- Extending BloodHound Part 1 – GPOs and User Right Assignment
- Taking over Windows Workstations thanks to LAPS and PXE
- Persistence – WaitFor
- Red Teamer's Cookbook: BYOI (Bring Your Own Interpreter)
- Defense and Detection for Attacks Within Azure
- Adding a Backdoor to AD in 400 Milliseconds

Beginners corner

- Simple Remote Code Execution Vulnerability Examples for Beginners
- Content Security Policy (CSP) Bypasses
- It's Okay, We're All On the SameSite
- Introduction to mobile network intrusions from a mobile phone
- Android: How to Bypass Root Check and Certificate Pinning
- A Gray Hacker's Intro to Wireshark
- Forwarding Reverse Shells Through A Jump Box Using SSH
- Reverse engineering my router's firmware with binwalk
- Hacking with WSL2

Writeups

Challenge writeups

- Forwarding Shells Through A Jump Box Using SSH
- Facebook's BountyCon 2020 CTF Writeup
- All h1-415-ctf writeups and the winners' writeups: p4fg & manoelt

Pentest writeups

- CVE-2019-12180 – ReadyAPI & SoapUI command execution via malicous project file
- Straight Outta Script Kiddie Zone : Deep dive on how to get a SYSTEM shell on Windows
- A bug and a misconfigured file share: a tale in two parts
- Exploiting LDAP Server NULL Bind
- Forging SWIFT MT Payment Messages for fun and pr... research!

Responsible(ish) disclosure writeups

- From CSRF to RCE and WordPress-site takeover: CVE-2020-8417 #Web
- SpringBoot 'DevTools' Insecure Deserialization — Analysis & Exploit #Web

Bug bounty writeups

- Critical Security Flaw Found in WhatsApp Desktop Platform Allowing Cybercriminals Read From The File System Access (Facebook, $12,500)
- Responsible Disclosure: Breaking out of a Sandboxed Editor to perform RCE (HackerEarth)
- Exploiting Insecure Firebase Database! & Insecure-Firebase-Exploit script
- An Unexpected Bounty — Email Bounce Issues
- Site wide CSRF on a popular program
- H1514 Remote Code Execution on kitcrm using bulk customer update of Priority Products (Shopify, $15,000)
- Gitlab (CodeQL) writeups: Netty HTTP Response Splitting ($1,500), CSRF in Spring apps ($1,800), LDAP injectionin Java ($3,000), Use of insecure protocol in Java (Maven) ($2,300)
- Disclose Any Store products, Files, Purchase Orders Via Email through Shopify Stocky APP (Shopify, $2,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- OWASP D4N155: Intelligent and dynamic wordlist using OSINT
- Scripts and snippets for ffuf payloads & TL;DR
- Fuzz-lightyear & Automated IDOR Discovery through Stateful Swagger Fuzzing

More tools, if you have time

- SEcraper: Search engine scraper tool in Bash. Uses Ask, Bing & Yahoo search engines
- Wildcheck: A Go script for detecting wildcard domains based on Amass's wildcards detector
- Gwdomains: Subdomain wildcard filtering tool
- Dufflebag: Search exposed EBS volumes for secrets
- Codeza: Python script that scans URLs listed in a file and returns Content-Length, Status-Code, Title, Forms & those potentially vulnerable to DOM XSS
- Codict & Introduction: A framework to learn and assess source code
- Eslinter: A Burp Suite extension that extracts JavaScript and lints them with ESLint
- FockCache: Minimalized Test Cache Poisoning
- Injectus: CRLF and open redirect fuzzer
- Berserko: Burp Suite extension to perform Kerberos authentication
- PrivescCheck: Privilege Escalation Enumeration Script for Windows
- OverwriteStrings & Introduction: Overwrite Strings in an executable to avoid detection

Misc. pentest & bug bounty resources

- Actual XSS in 2020
- PolyShell: a Bash/Batch/PowerShell polyglot
- HACK THEM ALL
- List of Attack Vectors
- Application-Security-Engineer-Interview-Questions

Challenges

- Can you spot the vulnerability? #CodeReview

Articles

- DOM Clobbering strikes back
- Obfuscated javascript, scam emails, and American Express
- Wacom drawing tablets track the name of every application that you open
- Inside a malicious Chrome Extension
- Ghost in the shell: Investigating web shell attacks
- Symantec Endpoint Protection Bypass + Meterpreter Pivoting
- AD Privilege Escalation Exploit: The Overlooked ACL & Who Can See LAPS Passwords?
- Challenges in IoT security
- Warzone: Behind the enemy lines
- The return of the spoof part 1: Parent process ID spoofing & Part 2: Command line spoofing

News

Bug bounty & Pentest news

- Google Chrome to Block Mixed Content Downloads, Prevents MiTM Attacks
- Chrome 80 released with silent notification popups, support for same-site cookies
- TLS 1.0/1.1 end-of-life countdown heads into the danger zone
- Leap Day Twitch Stream: Free online conference on 29 Feb 2020
- University Students: Join Us at BountyCon: Apply before February 29 2020
- Bug hunter finds cryptocurrency-mining botnet on DOD network
- Safe Harbor, or Thrown to the Sharks by Voatz?
- Recognizing Security Researchers in 2020
- Announcing Bugcrowd's 2020 Incentive Programs!
- 2019 in review by Dropbox, Shopify & Facebook

Reports

- Unit 42 CTR: Sensitive Data Exposed in GitHub
- Combatting Stress and Burnout in Cyber Security – From Surviving to Thriving

Vulnerabilities

- Nasty Linux, macOS sudo bug found and fixed
- Academics steal data from air-gapped systems using screen brightness variations
- TeamViewer stored user passwords encrypted, not hashed, and the key is now public & DecryptTeamViewer
- Tesla and other autopilot-driven cars tricked with 2D projections
- Spotlight shone on Microsoft Azure vulnerability
- Critical Cisco 'CDPwn' Protocol Flaws Explained: Podcast

Breaches & Attacks

- Emotet can spread to poorly secured Wi-Fi networks and computers on them
- Ransomware installs Gigabyte driver to kill antivirus products
- New ransomware doesn't just encrypt data. It also meddles with critical infrastructure
- Malware stew cooked up on Bitbucket, deployed in attacks worldwide
- Twitter says an attacker used its API to match usernames to phone numbers
- Hackers deface Facebook's official Twitter and Instagram accounts

Other news

- Android Flash Tool Lets You Install Android Using a Browser
- Police Warning: Cyber Criminals Are Using Cleaners to Hack Your Business
- Google says it accidentally sent some users' private videos to strangers
- How to create fake traffic jams in Google Maps with bucket full of smartphones
- Government spyware company spied on hundreds of innocent people
- What is WireGuard? Why Linux Users Going Crazy Over it?

Non technical

- Staying Motivated with a –^ uı q sp q
- [EN] – Starting BugBounty : From noob to beginner
- A Graduate's Thoughts: How to Get Started in Information Security and Cyber Security
- Mobile Security 101: Common Threats and How to Protect Yourself Against Them
- Pen Testing Ships. A year in review
- How To Become More Successful and Achieve your Dreams ?

- Hacking Tool Developers

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 01/31/2020 to 02/07/2020.

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