# Bug Bytes #58 – Live with @zseano, Mobile Hacking Cheatsheet & On Full-Time Bug Hunting

BY INTIGRITI · FEBRUARY 18, 2020 · LAST UPDATED ON MARCH 6, 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 07 to 14 of February.

## Our favorite 5 hacking items

### 1. Video of the week

> "@zseano Talks About BugBountyNotes.com, Recon, Reading Javascript, WAF, Wayback Machine, and more!"

Lately, @zseano has been quieter than before. So, it is nice to hear him share insights on his recon process (e.g why he runs subdomain tools last), his hacking methodology, why he closed Bug Bounty Notes, and much more.

### 2. Resource of the week

> "The Mobile Hacking CheatSheet"

No matter how often I use tools like ADB, Keytool or Frida, I always forget the syntax! These two cheatsheets are handy as they sum up commands that are most used used for Android and iOs hacking. Its creators, @RandoriSec, have also been sharing a lot of excellent tips for mobile hacking on Twitter. It's worth checking out.

### 3. Webinar of the week

> "Security Reconnaissance With Codingo: How New Tricks Let Hackers See More & Slides"

Watch this if you want to know the most notable bug bounty trends (tools and techniques) @codingo noticed in 2019. He focuses on recon and some bug classes like XSS, subdomain takeover, finding and testing API keys, etc.
I love that he explains the reasoning behind each idea. For instance, why reporting alert(1) for XSS is never the best idea, or why you should really not use sublist3r on its own for subdomain enumeration.

## 4. Non technical item of the week

> "On Full-Time Bug Bounty Hunting"

Should you give up everything and become a full-time bug bounty hunter? This unbiased feedback by @ajxchapman may help you decide. He tells his story, the pros and cons of bug hunting, and advice that helped him earn his living doing this full-time while living in London (not the cheapest town!).

## 5. Tutorial of the week

> "Proxying and Intercepting CLI Tools"

Have you ever run a command line tool and wondered which requests it was sending to your target? Knowing this can be valuable for pentesters and bug hunters. It helps understanding what the tool does. The solution detailed in this excellent tutorial is to use Burp Suite as a proxy. The process is explained for curl, wget, Java JARs, Python, Node JS and Go binaries.
Another advantage of using Burp is that all requests sent are logged (with request and response times). I can't tell you how many times pentest clients asked for what was being tested at X time and the number of requests, because they noticed network or server issues and wanted to determine if it was caused by the tests.

# Other amazing things we stumbled upon this week

## Videos

- Live Recon and App Profiling: Stream #5 (Tesla)
- Chrome Updates and CSRF Dies?
- PHP PHAR – file_exists can be dangerous
- Tim Medin: Understanding Penetration Testing | DailyCyber 212 ~Watch Now ~

## Podcasts

- The Academy | A Day In The Life Of A Bug Bounty Hunter | A Conversation With Tommy DeVoss And Ben Sadeghipour
- Security Now 753 – Promiscuous Cookies
- Risky Business #572 – Equifax indictments land, some big Huawei news
- Business Security Weekly #162 – Building a Great Culture, Excelling at Failure, and Leadership Book Suggestions
- Security Weekly News #11 – CIA Spying, Equifax Monster, Chinese Military, Election Security
- Security Weekly News #10 – Ashley Madison Sextortion, Iowa, 3D Brains
- [CPRadio] UPSynergy: Chinese-American Spy vs. Spy Story

## Webinars & Webcasts

- API security series
- Why it's easy being a hacker (Free registration required)
- Passwords are a Solvable Problem! (Free registration required)
- Linux Command Line Dojo with Hal Pomeranz
- Webcast: Getting Started in Cyber Deception #BlueTeam

## Conferences

- NSConclave2020
- AppSecCali 2020 Closing Keynote: Browser Manipulation for Bypassing Firewalls – Samy Kamkar
- Recon Montreal 2019, especially:
  - The Path to the Payload: Android Edition by Maddie Stone
  - The Unseen Dangers of Bloatware by Bill Demirkapi

## Slides only

- Pwn me, I m famous (Feat. JS)
- Expose Yourself: Without Insecurity
- Web Platform Security @ CMS Security Summit 2020

## Tutorials

### Medium to advanced

- Blind SSRF exploitation
- How to escalate privileges and steal secrets in Google Cloud Platform
- FIDO2 Deep Dive: Attestations, Trust model and Security
- Bypassing Wireless Captive Portals
- From memory corruption to disable_functions bypass: understanding PHP exploits
- Attacking Azure with Custom Script Extensions
- Network data manipulation on the fly
- Credential Access – Password Filter DLL

### Beginners corner

- #AndroidHackingMonth: Introduction to Android Hacking by @0xteknogeek
- Once upon a time an account enumeration
- How to prevent SQL Injection vulnerabilities: How Prepared Statements Work
- WMI 101 for Pentesters

## Writeups

### Challenge writeups

- SANS Holiday Hack Challenge 2019 Winners and Answers

### Pentest writeups

- From S3 bucket to Laravel unserialize RCE
- Apple iCloud Credential Stealing
- Lateral movement via MSSQL: a tale of CLR and socket reuse & mssqlproxy

### Responsible(ish) disclosure writeups

- ohmyzsh dotenv plugin RCE #RCE
- Checkmarx Research: SoundCloud API Security Advisory #API
- SonicWall SRA and SMA vulnerabilties #Web
- CVE-2020-8498: XSS in GistPress WordPress Plugin #Web
- ModSecurity Denial of Service Details and PoC CVE-2019-19886 #Web
- Interfaces.d to RCE #IoT

### Bug bounty writeups

- Weird Vulnerabilities Happening on Load Balancers, Shallow Copies and Caches ($1,500)
- A step-by-step walk-through of an Invalid Endpoint
- A Simple IDOR to Account Takeover ($4,500)
- How I Made $600 in Bug Bounty in 15 Minutes with Contrast CE – CVE- 2019-8442 ($600)
- Bypass Password Authentication for updating email and phone number – Security Vulnerability ($700)
- URL filter bypass in Enterprise Grid ($100)

## Tools

- Emissary: Send notifications on different channels such as Slack, Telegram, Discord etc.
- SlackSecrets: Scans Slack for API tokens, credentials, passwords, and more using YARA rules
- Pathbrute: Intelligent file/directory bruteforcer in Golang
- Android Application Analyzer: Tool for analyzing the content of android applications in local storage
- Frida iOS App Patching: This technique patches an IPA to perform an action using Frida without requiring to attach a debugger and execute Frida scripts in the background during runtime
- Cookie crimes: Read local Chrome cookies without root or decrypting
- Shosubgo: Go script for grabbing subdomains from Shodan
- DotGit: A browser extension to download site sources (with /.git/)
- FakeLogonScreen & Tutorial: Fake Windows logon screen to steal passwords
- Physmem2profit & Rethinking Credential Theft

## Misc. pentest & bug bounty resources

- Thick Client Penetration Testing Methodology
- SSRF All The Things!! Just a compilation of data from internet for reference
- Keycloak pentest report by Cure53
- Top 8 Exploit Databases for Security Researchers
- Pentesting Playground & Building a Home Lab
- Compiling a DLL using MingGW

## Challenges

- Introducing: Bi-Monthly 0x00sec CTF Exercises!
- DOM XSS challenge by @akhilreni_hs
- IoTGoat: A deliberately insecure firmware based on OpenWrt #IoT
- XSS challenge thread

## Articles

- A Rough Idea of Blind Regular Expression Injection Attack
- CSS data exfiltration in Firefox via a single injection point

- Deep Dive into Real-World Kubernetes Threats
- Subdomain Enumeration Tools Evaluation
- Demystifying Browsers
- Exploiting Netgear's Routerlogin.com
- Taking advantage of game metas and esports betting. Case study: Overwatch League & GOATS
- A Surprisingly Common Mistake Involving Wildcards & The Find Command

## News

### Bug bounty & Pentest news

- Supercharge your command line experience: GitHub CLI is now in beta: May be useful for automation
- #AndroidHackingMonth & Mobile Hacker AMA
- BloodHound 3.0 Release: Article, Webinar & Slides
- Announcing beta sign-up for AttackerKB: a new resource to highlight hacker community knowledge on which vulns matter most—and why.
- ALL NEW OSCP – REVAMPED 2020 (Video)
- SymTCP – a new tool for circumventing deep packet inspections
- Tech Conferences in Asia On Hold Due To Coronavirus Outbreak

### Reports

- Mac malware threats are now outpacing attacks on Windows PCs
- Phishing scams are costing us more than ever. This trick is most likely to catch you out
- FBI: BEC scams accounted for half of the cyber-crime losses in 2019

### Vulnerabilities

- Blind regex injection: Theoretical exploit offers new means of forcing web apps to spill secrets
- Unit 42 CTR: Leaked Code from Docker Registries
- 'Sloppy' Mobile Voting App Used in Four States Has 'Elementary' Security Flaws
- An 'Off-the-Shelf, Skeleton Project': Experts Analyze the App That Broke Iowa
- Unknown number of Bluetooth LE devices impacted by SweynTooth vulnerabilities
- Oh crumbs – Security flaw in WordPress GDPR cookie plugin left 700,000 sites open to abuse

- Dell fixes privilege elevation bug in support software

### Breaches & Attacks

- Netanyahu's party exposes data on over 6.4 million Israelis
- Concern over Coronavirus Leading to Global Spread of Fake Pharmacy Spam
- Apple iPhone Users Targeted with Bogus Dating App for Valentine's Day
- Mobile Phishing Campaign Uses over 200 Pages to Spoof Bank Sites
- 500 Chrome extensions secretly uploaded private data from millions of users
- India data breach: 460,000 credit card details put up for sale on dark web

### Other news

- Corp.com is up for sale – check your Active Directory settings!
- Leaked documents reportedly show the CIA secretly bought an encryption company and used it to spy on clients — while turning a profit
- US charges four Chinese military members with Equifax hack
- Huawei Controversy Highlights 5G Security Implications
- UK police deny responsibility for poster urging parents to report kids for using Kali Linux
- Google to Samsung: Stop messing with Linux kernel code. It's hurting Android security
- Apple joins FIDO Alliance, commits to getting rid of passwords

## Non technical

- My journey reaching #1 on Hack The Box Belgium – 10 tips, tricks and lessons learned.
- Absolute Success is Luck. Relative Success is Hard Work.
- Is it best to quickly test a web app for the most common vulnerabilities and then move on, or get a very deep understanding of one web app and test it for a lot of vulnerabilities?
- Mastering the Skills of Bug Bounty
- These 20 'Hackers' Helped Shape The Cybersecurity Landscape Forever
- An Introduction To Offensive Security
- Social Engineering: Thoughts on Elements of Behavioral Psychology

## 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 02/07/2020 to 02/14/2020.

*Curated by Pentester Land & Sponsored by Intigriti*