Bug Bytes #54 – Killing Snakes for Fun, Seagate RCE & Finding Bugs in API's

BY INTIGRITI · JANUARY 21, 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 10 to 17 of January.

Our favorite 5 hacking items

1. Webinar of the week

> "SEC642: Killing snakes for fun, Flask SSTIs and RCEs in Python **(Free registration required)**"

This is an excellent course on SSTIs with a focus on Python frameworks.
I love that it does not only explain how SSTIs work and how to escalate them to RCE, but it also mentions a lot of background information to understand the big picture: Why Python frameworks were created, how they work, the history of Python and Flask, etc.

2. Writeup of the week

> "Advisory | Seagate Central Storage Remote Code Execution 0day"

This is a nice example of RCE found using security code review with a bottom-up approach. It also shows how to reverse and analyze the firmware of a NAS.
Both RCE and code review can be intimidating. But the way everything is broken in this writeup makes them seem easy to follow even for beginners.

3. Challenge of the week

> "SKF labs"

There is a plethora of XSS challenges but labs for GraphQL bugs, JWT, SSRF, SSTI, lack of rate limiting, etc, are rarer. So, these labs are perfect if you want to play with these vulnerabilities and many others.
The best part is that detailed walkthroughs are provided for each bug.

4. Video of the week

> "Finding Your First Bug: Finding Bugs Using APIs"

As always, a great tutorial video by @InsiderPhD! I think this is the best introduction to APIs I've ever seen. It covers everything you need to start exploiting them ASAP: What APIs are, how to find and enumerate them, types of APIs (REST, SOAP, GraphQL), what is JSON, what bugs to look for, how to take notes, etc.

5. Tutorial of the week

> "Intruder and CSRF-protected form, without macros"

Did you know that macros are not the only way to deal with CSRF tokens in Burp? @Agarri_FR shows in great detail how to use Intruder Pitchfork to mimick manually replacing the CSRF token with the latest value sent by the server, and the advantages over macros.

Other amazing things we stumbled upon this week

Videos

- What Is The Best Linux Distribution?
- Hacker Millionaire Frans Rosén Interview
- Enumerating, Analyzing, and Exploiting The Citrix ADC RCE – CVE-2019-19781
- A Day In The Life Of A Bug Bounty Hunter (ft. STÖK)
- Detect file path traversal by Burp Suite intruder + regext
- How to handle session expiration in BURP with macros?
- The drawing advice that changed my life
- Introduction to OSINT Video

Podcasts

- Security Now 749 – Windows 7 – R. I. P.
- Risky Business #568 — Let's Decrypt
- [CPRadio] Domestic Kitten: An Iranian Surveillance Operation
- 7MS #396: Tales of Internal Pentest Pwnage – Part 13
- [CPRadio] Hacking Fortnite Accounts
- Application Security News #91
- Paul's Security Weekly #635 – CVE-2020-0601, Netscaler RCE, npm
- Security Weekly News #3
- Podcast: NSA Reports Major Crypto-Spoofing Bug to Microsoft

- Security Weekly News #4 – Win 10 exploit, Tik Tok, Lottery Hacker
- Security In Five Episode 661 – Microsoft Rolls Out New Browser, Whether You Want It Or Not

Webinars & Webcasts

- Webcast: Sacred Cash Cow Tipping 2020
- Webinar: Burp-less Hacking – Learning Web Application Pentesting on a Budget (Free registration required)
- How to Communicate about Security Vulnerabilities (Free registration required)
- Blockchain Basics Part1
- Operations Security (OPSEC) tradecraft tips for online Open Source Intelligence (OSINT) Research (Free registration required)

Conferences

- ZeroNights 2019
- C++ for Hackers
- STÖK Fredrik Closing Note at BSides Ahmedabad
- An introduction to the Router Exploit Kits

Tutorials

Medium to advanced

- Remote Code Execution in Three Acts: Chaining Exposed Actuators and H2 Database Aliases in Spring Boot 2 & Demo app
- Deep dive into the security of Progressive Web Apps
- What Is JavaScript Made Of?
- The noise of brute-force: Hydra and Log Analysis
- Operating system Detection using TTL value Powershell & Ping!
- Managing Active Directory groups from Linux
- Stealing NTLMv2 hash by abusing SQL injection in File download functionality
- What is Azure Active Directory?
- Persistence – Image File Execution Options Injection
- Persistence – Winlogon Helper DLL

- Give Me Back My Privileges! Please?

Beginners corner

- Using Scrcpy to Mirror Android Screens
- Pwning your (web)server and network the easy way – or why exposing ~/.ssh/ is a bad idea
- The Security of DevSecOps – Jenkins
- Xposed Framework Plugins For Android Pentesting
- Excess XSS
- How the BEAST Attack Works
- What I learnt from Sector035's annual quiz
- IoT Security – Part 4 (Bluetooth Low Energy – 101)

Writeups

Challenge writeups

- Nahamsec's 30K CTF by @pirateducky & by @AlMadjus
- 36C3 Senior CTF – SQLi through file metadata to PHP RCE – file magician
- FileMagician 36C3 CTF Web Challenge

Pentest writeups

- Owning a device with a single jump
- Very cool XXE bug in a Web Service

Responsible(ish) disclosure writeups

- Busting Cisco's Beans :: Hardcoding Your Way to Hell & PoCs #RCE #Web #CodeReview
- Breaching the perimeter – PhantomJS Arbitrary file read #Web
- Critical Auth Bypass Vulnerability In InfiniteWP Client And WP Time Capsule #Web
- From an Open Redirect in a Brazilian Bank to Session Token Leak #Web
- Finding someones hotel room number with a phone call.
- Undisclosed CVE-2019–19484,CVE-2019–19486,CVE-2019–19487 #Web #RCE
- Cracking password hashes in Yclas #Web
- Pwning Avast Secure Browser for fun and profit #RCE #BrowserExtensions

Bug bounty writeups

- Arbitrary File Write as SYSTEM from unprivileged user ($1,250)
- How I discovered an interesting account takeover flaw?
- Adding a malicious notebook to be treated like a trusted notebook in Google Colab — 1337$ ($1,337)
- My First RCE (Stressed Employee gets me 2x bounty)
- No Rate Limit – 2K Bounty
- Unrestricted file upload in www.semrush.com > /my_reports/api/v1/upload/image ($500)
- Reflected XSS at https://pay.gold.razer.com escalated to account takeover ($750)

Tools

If you don't have time

- xpasn: Expands an autonomous system (AS) number into prefixes or individual host IP addresses
- Velocity: DNS caching library for Python. Helps speed up network connections (applies to everything from sockets to HTTP requests)
- SWFPFinder: SWF Potential Parameters Finder
- GDA-android-reversing-Tool & Wiki: GDA is a new decompiler written entirely in c++, so it does not rely on the Java platform, which is succinct, portable and fast, and supports APK, DEX, ODEX, oat.

More tools, if you have time

- Burp-IndicatorsOfVulnerability: Burp extension that checks application requests and responses for indicators of vulnerability or targets for attack
- Bug bounty in a box!: A payload callback server & payload generator for bug bounty
- Phoenix CSRF Payload Generator
- Dmap: Advanced Domain Mapper for bug bounty
- Injectus: CRLF and open redirect fuzzer
- Frida API Fuzzer: Experimetal fuzzer for API in-memory fuzzing
- CHAPS – Configuration Hardening Assessment PowerShell Script
- Lil Pwny: Auditing Active Directory passwords using multiprocessing in Python
- AzureADRecon: A tool which gathers information about the Azure Active Directory given valid credentials. Useful for audits & post exploitation
- Gtfo: Search for Unix binaries that can be exploited to bypass system security restrictions

- PoisonHandler: A tool for performing lateral movement. It hides the command you are executing by registering a protocol handler

Misc. pentest & bug bounty resources

- Android Resources
- Information-Security-Tasks
- Shodan official filters list
- Securing The Stack
- Iranian APT Groups & Possible Commands Used By These Groups
- Octopi Hacking Archives
- Wireshark Cheat Sheet
- First Draft's 'Essential Guide to Newsgathering and Monitoring on the Social Web'
- SharpAllTheThings

Challenges

- xss.pwnfunction.com
- InjuredAndroid – CTF
- Announcing the 2020 Metasploit community CTF
- h1-415-ctf

Articles

- What I Learned Watching All 44 AppSec Cali 2019 Talks
- Global developer CAs considered harmful
- An Empirical Study of Wireless Carrier Authentication for SIM Swaps
- Hacking 'Docker', the Shodan way!
- Hack-back: a tale of embarrassing phishing campaign
- Facial recognition for the public: Yandex
- Deceiving blue teams using anti-forensic techniques
- Mapping the Jan 2020 Java Security Patches Back to the Original Source Code Changes

Unusual Patch Tuesday

- Microsoft's January 2020 Patch Tuesday Fixes 49 Vulnerabilities
- Microsoft fix of critical Windows bugs after NSA tip-off prompts questions
- Google Chrome Adds Protection for NSA's Windows CryptoAPI Flaw
- Exploiting CVE-2020-0601
- CVE-2020-0601: the ChainOfFools/CurveBall attack explained with PoC
- PoCs by Kudelski Security & by ollypwn

News

Bug bounty & Pentest news

- Huntr: New bug bounty platform for fixing bugs in open-source code
- MITRE launches ATT&CK for industrial control systems knowledge base
- We have increased our Microsoft Edge bounty awards alongside today's general availability of the new Microsoft Edge
- GitLab Celebrates Awarding $1 Million in Bounties to Hackers on HackerOne
- Burp Suite roadmap for 2020

Reports

- Study says Grindr, OkCupid, and Tinder breach GDPR
- How big is the skills gap, really?
- Cyber-attack fears growing among business leaders and policymakers

Vulnerabilities

- Google hackers successfully use remote exploit to hack iPhone
- Microsoft warns about Internet Explorer zero-day, but no patch yet
- Tails 4.2.2: Emergency release addresses critical Tor Browser vulnerability
- How safe is your phone number? Study highlights mobile carriers' failure to prevent SIM-swap attacks
- Critical Cisco DCNM flaws: Patch right now as PoC exploits are released
- Update now! Popular WordPress plugins have password bypass flaws

Breaches & Attacks

- A hacker is patching Citrix servers to maintain exclusive access
- Hackers Are Breaking Directly Into Telecom Companies to Take Over Customer Phone Numbers
- Threat Spotlight: Conversation Hijacking
- Discord users warned over QR code login scam that can result in pwned accounts
- Lottery hacker gets 9 months for his £5 cut of the loot
- Sodinokibi Ransomware Publishes Stolen Data for the First Time
- Fleeceware is back in Google Play – massive fees for not much at all
- Microsoft spots malicious npm package stealing data from UNIX systems
- FBI: Nation-state actors have breached two US municipalities
- Australia Bushfire Donors Affected by Credit Card Skimming Attack
- Baby's First Data Breach: App Exposes Baby Photos, Videos
- FBI seizes WeLeakInfo, a website that sold access to breached data

Other news

- Behavior Change in Chrome's Download Protection Service Affecting Privacy
- Microsoft's New Edge Browser Released, What You Need to Know
- Mozilla lays off 70 employees as its revenue declines
- US troops deploying to the Middle East told to leave personal devices at home
- Inside Discord's Thriving Black Market for Stolen Credit Cards and Gift Cards
- Only 9.27% of all npm developers use 2FA
- Middle East tech's biggest trends in 2019? Startups, 5G – and internet shutdowns
- Russia responsible for hacking gas firm tied to Trump impeachment: report
- Report: Chinese hacking group APT40 hides behind network of front companies
- Google will now accept your iPhone as an authentication key
- A win for privacy? Google plans to scrap user-agent string in Chrome
- Google to kill third-party Chrome cookies in two years
- Google urged to tame privacy-killing Android bloatware

Non technical

- Interview with Christian Holler

- Security architecture anti-patterns
- The 30 Best Pieces of Advice for Entrepreneurs in 2019
- Do not kill your pentester for little or no value-add
- Burnout linked to potentially deadly irregular heartbeat, study says
- The Guy Who Invented Inbox Zero Says We're All Doing It Wrong
- The Difference Between Business Intelligence, Reporting, Metrics, and Analytics
- CVE In 5 mins – Hands on Guide
- 15 Helpful Tips For Cybersecurity Interviews
- How to Become an Ethical Hacker

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 01/10/2020 to 01/17/2020.

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