Bug Bytes #49 – WHY YOUR HACKING QUESTIONS ARE FRUSTRATING!!! (and more)

BY INTIGRITI · DECEMBER 17, 2019 · 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 06 to 13 of December.

Our favorite 5 hacking items

1. Tutorial of the week

> "Quality of Life Tips and Tricks – Burp Suite"

These tips are very helpful for improving your Burp experience. Some are old news but I'm discovering others for the first time:

- How to reduce the size of Burp projects for long term storage (Burp project hoarders, hello!)
- How to leverage Match and Replace for simplifying the use of complex or long test username/passwords (Simple yet genius! Useful especially with mobile tests)
- How to rearrange Burp Repeater request and response tabs (So useful for taking screenshots for reports!)

2. Tool of the week

> "Bookmarks"

Have you ever used Burp Repeater as a bookmarking feature? I do, and the result is not pretty. Tens of tabs open, which is not practical and slows down Burp.
So, this bookmarking extension can be life-changing. It allows you to save interesting requests/responses, replay requests directly in the extension's tab, sent it to Repeater/Intruder, and highlight the request in Burp Proxy.

3. Video of the week

> "Docker For Pentesting And Bug Bounty Hunting & Bug Bounty Toolkit"

This is an excellent introduction to Docker. If you are not already using it, you can learn in less than 40 minutes why and how to leverage it for pentest and bug bounty.
An example toolkit is also provided. It basically allows you to customize any Linux distribution by adding tools. The list of tools installed can be modified. This would be a good exercise for practicing with Docker.

4. Tip of the week

> "Trying to use Masscan through a VPN client? Use -e to specify the interface. Similarly, Nessus won't scan over a VPN interface unless you set the source_ip setting in the advanced options to your VPN interface's IP."

Tip added to knowledge base! This is good to know and might save me (and you maybe?) time when using a VPN for either pentest or bug bounty.

5. Non technical item of the week

> "Learning How to Learn: Powerful mental tools to help you master tough subjects & @knoxxs's notes"

I know someone who can literally learn anything in a very short period of time. I don't think it is due to an abnormal intelligence or anything, but because of skills like the ability to detect the missing knowledge, where to get it and what to prioritize to get quick results.
These skills can be taught. This free Coursera course is an excellent start. Personally, I've added it to my list of online courses to go through in 2020. It explains both theory and practical techniques to improve learning, tackle procrastination, and understand how memory works.

Other amazing things we stumbled upon this week

Videos

- @spaceraccoonsec talks about Hacker101, bug bounty checklists, collaboration and becoming MVH
- Domain Admin via IPv6 DNS Takeover
- Unbounce Service Takeover with Steps (Poc)
- Mystiko live session 001 #OSCP #SQLi
- HackerOne Hacker Interviews: Cody (@daeken), Eugene (@spaceraccoon), Neiko Rivera (@specters), Collin (@collinmay), Dave (@n0bytes), Naffy (@nnwakelam) & Ron (@ngalongc)
- Hacker culture
- Public Penetration Test Reports – Learning Resource
- How To Learn Hacking With CTFs
- WHY YOUR HACKING QUESTIONS ARE FRUSTRATING!!!

- HACKERSPACES ARE AWESOME!

Podcasts

- Security Now 744 VPN-geddon Denied
- 7MS #390: Tales of Internal Network Pentest Pwnage – Part 11
- Darknet Diaries Ep 53: Shadow Brokers
- Risky Business #566 — Balkanisation, ransomware, comedy bugs close out the decade
- Security In Five Episode 640 – IoT Strikes Again – Jan 14 2020 Doomsday For Health Devices
- Hack Naked News #245
- Paul's Security Weekly #629 – Outlook on Phishing in 2020 – Eric Brown
- Paul's Security Weekly #630 – Risks, Ransomware, Data Leaks, Oh My!
- Iron Sysadmin podcast Episode 71 – Holiday Hack with the Elf Himself!
- The Privacy, Security, & OSINT Show 148 – Camera & Microphone Blocking

Webinars & Webcasts

- A Day in the Life of a Pen Tester – Episode 5
- Passwords: You are the weakest link

Conferences

- KringleCon 2019, especially:
  - How to (Holiday) Hack It: Tips for Crushing CTFs & Pwning Pentests
  - Web Apps: A Trailhead
  - Telling Stories from the North Pole
- Checkmarx API Security Meetup 2
- BlackAlps 2019: Swisscom Bug Bounty: Retour D'Un Chercheur – Daniel Le Gall (in French)
- HD Moore on Modern Network Discovery – Duo Tech Talk & Slides
- Black Hat EU 2019
  - Securing the System: A Deep Dive into Reversing Android Pre-Installed Apps
  - Selling 0-Days to Governments and Offensive Security Companies
  - Finding Our Path: How We're Trying to Improve Active Directory Security
  - Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD)

- Women in Security: Building a Female InfoSec Community in Korea, Japan, and Taiwan

Slides only

- At Home Among Strangers
- An introduction to the Router Exploit Kits
- Securing the DOM from the Bottom Up
- Hacker-Powered Data: Why the Most Common Vulnerabilities Aren't What You Think They Are
- Weaponizing AMSI bypasses with PowerShell

Tutorials

Medium to advanced

- Cross Site Request Forgery: Techniques
- Tunneling traffic through MySQL service (or your mysqld is my new SOCKS5)
- Cracking LUKS/dm-crypt passphrases
- Persistence – Office Application Startup
- macOS Red Team: Calling Apple APIs Without Building Binaries
- WMIC Service Modification for Lateral Movement
- SCshell: Fileless Lateral Movement Using Service Manager

Beginners corner

- Help you understand HTTP Smuggling in one article & HTTP Request Smuggling in one Screenshot
- GraphQL vs REST API model, common security test cases for GraphQL endpoints
  - https://twitter.com/prakashashok4/status/1203226709337591810
- Out-of-Band (OOB) SQL Injection & A Study of Out-of-Band Structured Query Language Injection
- Source Code Analysis XSS
- Root Detection Bypass By Manual Code Manipulation
- Finding Active Directory attack paths using BloodHound

Writeups

Challenge writeups

- EGCERT CTF 2019 – Priv8 Leecher

- CSP Bypass via old jQuery – Thanks parseHTML!

Pentest writeups

- Spilling Local Files via XXE When HTTP OOB Fails
- Deserialized Double Dirty

Responsible(ish) disclosure writeups

- Solismed Version 3.3SP1 # Web
- CVE-2019-19634 – class.upload.php <= 2.0.4 Arbitrary file upload #Web
- ColdFusion Bomb: A Chain Reaction From XSS to RCE #Web #RCE
- Git submodule update command execution #RCE
- CVE-2019-18935: Remote Code Execution via Insecure Deserialization in Telerik UI & PoC #Web #RCE
- Azure Privilege Escalation via Cloud Shell #Cloud
- From iPhone to NT AUTHORITY\SYSTEM #iOS
- IoT Vuln Disclosure: Children's GPS Smart Watches (R7-2019-57) #IoT
- Blink XT2 Camera System Command Injection Flaws #IoT
- Remotely Exploiting IoT Pet Feeders #IoT

Bug bounty writeups

- DoS on HackerOne ($2,500)
- IDOR on GitLab ($5,000)
- CORS with full PoC on LocalTapiola ($1,984)
- Google Chrome portal element fuzzing ($8,000)
- Vimeo upload function SSRF ($5,000)
- SSRF via FFmpeg HLS processing
- Get pwned by scanning QR Code)
- Blind XSS (A mind game to win the battle) ($1,000)
- Authentication bypass on Facebook
- Telegram (v4.9.155353) was rendering file:// links + opening them via NSWorkspace.open -> code execution. ($500)

- Information disclosure on GitLab ($3,000)
- SSRF/ToCToU on GitLab ($5,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Shodan.io-mobile-app: Official repository for the Shodan.io mobile Application
- I Got Urls: WaybackURLS + OtxURLS + CommonCrawl = The Best Results

More tools, if you have time

- Black Hat Europe 2019 Arsenal
- Batea: AI-based tool that automatically filters interesting network assets in large networks using nmap scan reports
- Recsech: Footprinting & recon tool
- Ngrev: Tool for reverse engineering of Angular applications
- Is-website-vulnerable: Finds publicly known security vulnerabilities in a website's frontend JavaScript libraries
- Routine-automation: Automation of commands and tools that @spenkkkkk uses for daily purposes and bug bounty
- PathAuditor, Introduction: Tool for finding file access related vulnerabilities by auditing libc functions & E.g. of bug you can find with it: CVE-2019-3461
- Hashcobra: Generates rainbow tables from wordlists to heavily optimize the cracking process
- grandmaster: A python tool that assists in automating iOS firmware decryption

Misc. pentest & bug bounty resources

- CodePath Web Security Guides
- Bootstrap XSS Collection
- Web Service Hacking
- Awesome Open Source: The Top 132 Osint Open Source Projects
- Bellingcat's Online Investigation Toolkit
- Week in OSINT — #49
- OSINT_TIPS

- ZAP-Mini-Workshop: Easy way to work with and learn ZAP's API and Scripting capabilities
- SFDC Secure Development Cheat Sheet
- Secure IoT: Mapping of IoT Security Recommendations
- Red Teaming Mind Map from The Hacker Playbook 3
- Ethical hacking: Top 10 browser extensions for hacking
- APIsecurity.io Issue 61: Exposed patient records, vulnerabilities at Airtel and Kaspersky

Challenges

- The 2019 SANS Holiday Hack Challenge
- Android CTF — KGB Messenger & Writeup
- Shoping_site: Dummy shopping site for whitebox pentesting
- @shhnjk's XSS challenge
- Red team recruitment challenge
- HTTP-Smuggling-Lab

Articles

- The StrandHogg vulnerability
- Breaking the chains on HTTP Request Smuggler
- Client-side Vulnerabilities in Commercial VPNs
- A technical look at Phone Extraction (PDF) / HTML version
- How I Shut Down a (Test) Factory with a Single Layer 2 Packet
- PHP Autoloading: Local File Inclusion by Design
- Pentest-Report libssh C Library by Cure53 #CodeReview
- Updating adconnectdump – a journey into DPAPI
- Serious Security: Understanding how computers count
- MacOS Filename Homoglyphs Revisited

News

Bug bounty & Pentest news

- Offensive Security Tools (OST) used by the Emotet malware

- AMA about how online volunteers can help find missing people, the open-source intelligence movement (#OSINT) and more
- @SynackRedTeam has a 24 hour "quality" rule with new #bugbounty programs where the @Synack reviewers choose to payout their favorite report if multiple are submitted for the same bug
- PortSwigger is hiring a Web vulnerability researcher
- Amazon Battles Leaky S3 Buckets with a New Security Tool

Reports

- The quiet evolution of phishing
- Download: The 2020 Cybersecurity Salary Survey Results
- 49% of workers, when forced to update their password, reuse the same one with just a minor change

Vulnerabilities

- A technical review of connected toy security
- Networking attack gives hijackers VPN access
- An iOS bug in AirDrop let anyone temporarily lock-up nearby iPhones
- Hackers can jack ShapeShift's crypto wallets in 15 minutes, Kraken warns
- Npm team warns of new 'binary planting' bug
- Critical Remote Code-Execution Bugs Threaten Global Power Plants
- Safer-Eval library branded 'harmful' with no patch planned
- Attackers Terrify Homeowners After Hacking Ring Devices
- Plundervolt attack unpins Intel chip security enclaves
- Atlassian scrambles to fix zero-day security hole accidentally disclosed on Twitter

Breaches & Attacks

- Phishing Attack Hijacks Office 365 Accounts Using OAuth Apps
- TrickBot gang is now a malware supplier for North Korean hackers
- Domain Takeover at Gunpoint Gets Influencer 14 Years in Jail
- Snatch ransomware reboots PCs in Safe Mode to skirt antivirus defenses
- December Patch Tuesday blunts WizardOpium attack chain

Malicious apps/sites

Other news

- $10m GDPR Fine; Why we Need GDPR in Bug Bounties
- Chinese government to replace foreign hardware and software within three years
- Would you rather buy a long range Tesla Model 3? Or... an Apple Computer?
- Generated Passwords, UX and Security Absolutism & @TinkerSec's take on the situation
- Tool Illegally Enables Windows 7 Extended Security Updates
- $5m bounty set on the alleged head of Evil Corp banking Trojan group
- What is DDoS? A complete guide
- Security.txt – IESG issues final call for comment on proposed vulnerability reporting standard
- Chrome 79 released with tab freezing, back-forward caching, and loads of security features
- From DNS hijacking to domain fronting – SANS security pros offer retrospective on 2019 threat predictions

Non technical

- Our Smart TVs Are Watching Us
- How to Become a Web Pentester?
- How smoking led to social engineers gaining physical access to a network
- Young, Successful, and Depressed
- YESWEHACK PROPHILE ON EBODA
- Meet the team: Laura Kankaala – Securing companies by breaking stuff
- CTF Design 101
- The 3 lists you should be making & how to stop letting to-do lists control your life

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 12/06/2019 to 12/13/2019.

Disclaimer:

*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***

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com