Bug Bytes #50 – Null Bytes Worth $40K, Getting Your First Bug & Tab Tricks

BY INTIGRITI · DECEMBER 24, 2019 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-50-null-bytes-worth-40k-getting-your-first-bug-tab-tricks

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 13 to 20 of December.

intigriti news

> .@Randstad just launched a responsible disclosure program with an a-ma-zing scope! Check it out https://t.co/Xf0qiCPmVq #HackWithIntigriti pic.twitter.com/jc5cTWgTet
>
> — Intigriti (@intigriti) December 19, 2019

Our favorite 5 hacking items

1. Tutorials of the week

> – From checkra1n to Frida: iOS App Pentesting Quickstart on iOS 13
> – Anyone Can Check for Magecart with Just the Browser
> – Ngrok your DockerSploit

These are excellent tutorials to learn about:

- iOS app pentesting. It's THE tutorial you were waiting for. Everything is explained: Jailbreak with checkra1n, installing Frida and Objection, proxying traffic with Burp, bypassing certificate pinning with SSL Kill Switch 2, bypass Jailbreak detection, etc.
- Detecting Magecart. Useful for penetration testers who want to know which indicators to keep an eye for to detect infected sites.
- The poor man's VPS setup. Useful for tests involving reverse shells and out of band vulnerabilities. No credit card required.

2. Writeup of the week

> Filling in the Blanks: Exploiting Null Byte Buffer Overflow for a $40,000 Bounty ($40,000)

I have a bad memory of buffer overflows from my university days. But this writeup describes a type of overflows that is relatively easy to understand and exploit remotely on Web apps.

@samwcyo was trying to re-register existing usernames. He tried adding special characters (like null byte, CRLF characters, spaces, Unicode…) hoping that they would be removed during the registration process.

The vulnerability is that each null byte inserted was replaced with random data, e.g.:

- Request: *POST /register?username=victim%00@domain.com*
- Response: *username victimIdL@domain.com*

So, injecting multiple null bytes (*victim%00%00%00@domain.com*) made the server return chunks of memory that contained very sensitive data (SSH keys, passwords, usernames, etc).

3. Videos of the week

> Finding Your First Bug: Getting Started on a Target (Part 1) & Part 2

@InsiderPhD continues to delight us with new video tutorials on "Finding your first bug". This series is excellent for anyone starting out in bug bounties or who wants to get into Web app penetration testing. A lot of things are covered from creating your own testing methodology to recon, note taking, what to look for, etc.

4. Tip of the week

> Nine tips for better tab management

This is for firefox users, especially those of us who always have 20+ tabs open. The 9 features mentioned include synchronization between devices, sending tabs to another device, muting tabs, etc.
I find this very helpful for organizing tabs (and reducing anxiety).

5. Tools of the week

> – Silver
> – Flumberbuckets & Introduction

Two cool Python tools to help with recon automation. Silver by @s0md3v is a wrapper around Masscan, Nmap and Vulners. Flumberbuckets by @fellchase is for S3 bucket hunting.

Other amazing things we stumbled upon this week

Videos

- Learning Server Side Request Forgery (SSRF) Basics Using Portswigger's Web Security Academy
- Docker For Pentesting On Windows [Cybersecurity]
- Cybertalk – EP4 – IDA Pro, Malware Analysis & Python Libraries
- 2OC Presents: Brain Damage On The Mic Don't Manage
- How to find vulnerabilities by source code review and how to write scripts to exfiltrate data
- White box pentesting and exploit development part 2

Podcasts

- Security Now 745 – PlunderVolt
- Darknet Diaries EP 55: NoirNet
- Hack Naked News #246
- SwigCast, Episode 4: MAGECART
- Coalcast Episode S1E9 – Brad Woodward
- Paul's Security Weekly #630 – Risks, Ransomware, Data Leaks, Oh My!

Webinars & Webcasts

- Hacking Common AD Misconfigurations (Free registration required)
- Popping Shells Instead of Alert Boxes: Weaponizing XSS for Fun and Profit & Github repo
- Top 5 Mobile Security Stories of 2019 / Article

Conferences

- THREAT CON 2019
- 7 habits of highly effective adversaries (Joe Gray)

Tutorials

Medium to advanced

- Use Telegram bot as a Penetration Testing Framework
- Abusing Electron apps to bypass macOS's security controls
- Persistence – Application Shimming
- Demystifying AWS' AssumeRole and sts:ExternalId
- Streamlining BloodHound Analytics & bloodhound-playbook

Beginners corner

- Security Headers: Whys and Hows
- Root Detection Bypass With Frida
- SSL Pinning Bypass — Android PenTesting
- OAuth 2.0 : Explained
- MITM: Gaining Access to Instagram Photos

- How DNS Cache Poisoning Attacks Work
- Pass the Hash (in French)

Writeups

Challenge writeups

- Taking SQL Injections further (Blind Second Order SQL Injection + TMHC CTF Shitter Writeup)

Responsible(ish) disclosure writeups

- TP-Link Archer Router Vulnerability Voids Admin Password, Can Allow Remote Takeover #Web
- [Exploitation] D-Link DAP-1860 Vulnerability #RCE # Web #CodeReview
- Kids Tracker Watches: CloudPets, exploiting athletes and hijacking reality TV #API #IoT
- eGain Web API Email Header Injection
- CVE-2019–17555: DoS via Retry-After header in Apache Olingo #CodeReview
- From iPhone to NT AUTHORITY\SYSTEM #Windows #PrivilegeEscalation
- From dropbox(updater) to NT AUTHORITY\SYSTEM #Windows #PrivilegeEscalation
- Signal Desktop Windows Elevation of Privilege Vulnerability #Windows #PrivilegeEscalation

Bug bounty writeups

- Abusing feature to steal your tokens
- Hacking GitHub with Unicode's dotless 'i'.
- 4 Google Cloud Shell bugs explained
- [Google VRP] SSRF in Google Cloud Platform StackDriver
- BreakingApp – WhatsApp Crash & Data Loss Bug
- Uncontrolled Resource Consumption in any Markdown field using Mermaid on GitLab ($1,000)
- Git flag injection – local file overwrite to remote code execution ($12,000)
- Group search leaks private MRs, code, commits ($7,000)
- Group search with Elastic search enable leaks unrelated data ($7,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- ReconCobra: Complete Automated pentest framework for Information Gathering

- CustomHeader: Automatic Add New Header To Entire BurpSuite HTTP Requests
- FindScript: Scrape Google and Github to find JS or similar files from a given URL
- Unfurl (online version), Source code & Bookmarklet, Introduction & Difference with @tomnomnom's unfurl

More tools, if you have time

- Online Generate Test Data in CSV or JSON
- SecretX: Extracting APIs and keys from a list of URLs using regex
- Cypher Injection Scanner: Burp Suite Extension that detects Cypher code injection in applications using Neo4j databases
- Dnstwister: Online domain name permutation engine
- Credcheck & Introduction: Credentials Checking Framework
- Scout: URL fuzzer in Go for discovering undisclosed files and directories on a web server
- Koala Toolkit: Bug bounty toolkit for Docker
- alpyntest: A Docker image embedding modern Python3 pentest tools (impacket, pypykatz, lsassy, ntlmrecon, enum4linuxpy, ldapsearch-ad, CrackMapExec...) to avoid dependencies wreckage on your system
- Rubeus2ccache: Generates ccache files directly from Rubeus dump output
- Search-SMB: A wrapper shell script for CrackMapExec that will grab all the SMB shares and search readable ones for your search term

Misc. pentest & bug bounty resources

- Cheatsheet for finding vulnerable PHP code using grep #CodeReview
- KelvinSecurity OSINT & Penetration Testing
- Awesome CTF
- APIsecurity.io Issue 62: Vulnerabilities in Amazon Ring Neighbors and Droom, WebSocket API security
- Bloodhound Custom Queries
- AWS Cyber Range

Challenges

- Lesser Known Web Attack Lab
- A mini challenge, can you read the file at 'data/flag'?
- Mini #CodeReview challenge by @LaNMaSteR53

- New XSS challenge by @rodoassis
- XSS challenge by @Abdulahhusam & hint

Articles

- Weaponizing BURP to work as an evil SSRF Confluence Server.
- GraphQL Batching Attack
- Bots and Crawlers — The automation of information gathering
- Crypto Scam Investigation: Using Spiderfoot HX For OSINT Automation
- Javascript Anti Debugging — Some Next Level Sh*t (Part 1 — Abusing SourceMappingURL)
- Investigating PrivEsc Methods in AWS
- Phishing Concept #1
- Winbox in the Wild
- Undocumented Catalina file access change
- TikTok — Using OSINT to Discover New Leads

News

Bug bounty & Pentest news

- BountyCon 2020
- Trace Labs Global Missing CTF III: An OSINT CTF for Missing Persons
- Apple Security Bounty
- Announcing updates to our Patch Rewards program in 2020
- New Web Security Academy topic: Access control vulnerabilities and privilege escalation
- Bugcrowd Launches CrowdStream and In-Platform Coordinated Disclosure
- How Kali deals with the upcoming Python 2 End-of-Life

Reports

- Cybersecurity: This password-stealing hacking campaign is targeting governments around the world
- New study shows just how bad vehicle hacking has gotten
- Operation Wocao: Shining a light on one of China's hidden hacking groups

Vulnerabilities

- Plundervolt – stealing secrets by starving your computer of voltage
- F-Secure: Wireless presentation system riddled with flaws
- Npm patches two serious bugs
- Alexa, Google Home Eavesdropping Hack Not Yet Fixed
- All it takes to fool facial recognition at airports and border crossings is a printed mask, researchers found
- Hackers Could Use Smart Displays to Spy on Meetings
- One in every 172 active RSA certificates are vulnerable to attack
- Web Cache Deception attacks still impact websites with 'substantial user populations'
- We Tested Ring's Security. It's Awful
- Hackers keep dumping Ring credentials online 'for the giggles'

Breaches & Attacks

- Hiding malware downloads in Taylor Swift pics! New SophosLabs report
- Get in line! 38,000 students and staff forced to queue for new passwords
- A thief stole unencrypted hard drives filled with 29,000 Facebook employees' information
- Ryuk ransomware implicated in City of New Orleans shutdown

Other news

- Doxed credit card data has two hours max before it's nabbed
- Google charts progress in developing Site Isolation browser technology
- A guide to DNS-over-HTTPS – how a new web protocol aims to protect your privacy online
- Edward Snowden's book profits must go to the government, judge rules
- Mozilla mandates 2FA security for Firefox developers
- Decade retrospective: Cybersecurity from 2010 to 2019
- The Verge's gadgets of the decade

Non technical

- Top 10 Best Hacking Films of All Time
- Breaking out of the Shellcode: Jeff Moss on Mr. Robot and hacking movies
- Two-Factor Authentication vs. Multi-Factor Authentication: Differences Explained
- 9 tips for not getting spied on while traveling

- Get Organized Like a Villain
- Bug bounty management, a bad example
- What is CVE? – Common Vulnerabilities and Exposures
- Write Your Passwords in a Notebook and How To Memorialize and Access Deceased Loved Ones' Online Accounts
- Why Constraints Are Good for Innovation
- Open Source Spotlight: DOMPurify with Mario Heiderich
- Twas the Week Before Hackmas
- How to effectively break up your time for maximum productivity

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 12/13/2019 to 12/20/2019.

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