Bug Bytes #90 – The impossible XSS, Burp Pro tips & A millionaire on bug bounty and meditation

BY ANNA HAMMOND · SEPTEMBER 30, 2020 · LAST UPDATED ON MARCH 6, 2025

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 18 to 25 of September.

Our favorite 5 hacking items

1. Article of the week

Redefining Impossible: XSS without arbitrary JavaScript

This is a guest article by Luan Herrera (@lbherrera_) who solved one of PortSwigger's impossible XSS labs. He used several techniques including an obscure method to prevent a page from loading and a side-channel attack. A pretty advanced and informative XSS attack!

2. Writeups of the week

Universal XSS in Android WebView (CVE-2020-6506) (Google, Microsoft, Twitter..., $15,560+)
Chains on Chains: Chaining multiple low-level vulns into a Critical.
Exploiting Tiny Tiny RSS

I couldn't choose only one writeup this week, as these are all excellent and focus on different topics.

The universal XSS is a great read if you want to learn about XSS in Android.

The second writeup is a beautiful chain of low/medium impact bugs that ended up becoming a "critical". It involves blind XSS, CSP bypass, an exposed JWT generation page, lack of rate-limiting and sensitive information disclosure.

The Tiny Tiny RSS writeup is also a mix of vulnerabilities (XSS, SSRF & LFI) that led to RCE. It is really well written with everything explained, from source code review to mass exploitation.

3. Videos of the week

Web Cache Deception For Beginners!

Todayisnew Talks About Bug Bounty, Meditation, Automation, Tooling and Making $1M in Bounties!

This is a great introduction to Web Cache Deception if you want to learn about it and find the topic too complex. Farah Hawa (@farah_hawa01) explains the gist of it in a very approachable way, with resources to go further.

Also, finally an interview with todayisnew (@codecancare)! He is known as a bug bounty millionaire, and for his kindness. It's fantastic to see what he has to say about bug hunting, recon, tooling, meditation, burnout, etc.

4. Resources of the week

@MasteringBurp

HunterSuite Assets & Vulndb

Because of the coronapocalypse, Nicolas Grégoire (@Agarri_FR) moved his Burp Pro training online. He also started this new Twitter account, @MasteringBurp, to share all kinds of Burp tips.

For example, did you know that if the left part of a Collaborator hostname is "spoofed", it is resolved to 127.0.0.1?

HunterSuite Assets was just publicly launched. It's a free online database of subdomains of programs from all major bug bounty platforms. A fantastic resource but I wouldn't use it as an only source of subdomain enumeration, rather as a comparison tool to find out where I stand in terms of recon results.

5. Tool of the week

burp-headup

Burp head-up is an extension to toggle Burp proxy and get its status with a global keyboard shortcut. It was created for i3 but could be adapted to other windows manager.

This is so handy! Could someone port it to Mac OS, pretty please ?

Other amazing things we stumbled upon this week

Videos

- $XX,000 eight XSS with 4 bypasses on Airbnb
- Better Bug Bounty Reporting with BBR
- Browser hacking: Simple cross-frame scripting
- Hacking The U.S. Air Force and Verizon Media to Make $500,000 in Bounties!
- Secondary Context Path Traversal
- Forever Free Push Notifications are Here | App – Notify-Me | Push Notifications For your Recon & Notify-Me app source code

- What after Recon? – Sup Subdomains?!

Podcasts

- The InfoSec & OSINT Show 26 – James Kettle and Becoming a Security Researcher
- A Byte-ful With Tomnomnom
- Hacking into Security #26 – Poker player, Developer, Penetration Tester, top 20 bug hunter and Global Head of Security Operations and Researcher Enablement at Bugcrowd, with Michael Skelton (@Codingo)
- Security Now – Formal Verification – iOS 14 & Android 11 Security Features, DuckDuckGo Gets Big

Webinars & Webcasts

- Webinar : Exploiting iOS & Android apps through FirebaseDB & Fireprint

Conferences

- BSides Singapore 2020 & Beware of the Shadowbunny – Using virtual machines to persist and evade detections
- Australian OSINT Symposium
- Packet Analysis Using Wireshark

Tutorials

Medium to advanced

- How to enhance BurpSuite (or any other Java app) font rendering
- How SSRF (and XXE) Vary in Severity (Part 1) & Part 2
- h1Beacon Object File ADVENTURES: Some Zerologon, SMBGhost, and Situational Awareness
- I Like to Move It: Windows Lateral Movement Part 1 – WMI Event Subscription & Part 2 – DCOM
- MacOS Injection via Third Party Frameworks
- Building a custom Mimikatz binary

Beginners corner

- ZeroLogon(CVE-2020-1472) – Attacking & Defending
- XSS: Beyond the pop-ups
- A Pentester's Guide to SQL Injection (SQLi), Demo part 1 & Part 2

- How I got 1200+ Open S3 buckets...!
- Create your own OSINT database (with bookmarks)
- Understanding Binary and Data Representation with CyberChef
- vickieli.dev
- Getting started with iOS testing

Writeups

Challenge writeups

- Beat The Clock: The CSIT InfoSecurity Challenge
- TokyoWesterns CTF 2020 | writeups by @terjanq

Pentest writeups

- Pentest discoveries on EyesOfNetwork
- Azure Account Hijacking Using Mimikatz's Lsadump::setntlm

Responsible(ish) disclosure writeups

- Pandora FMS 742: Critical Code Vulnerabilities Explained #Web #CodeReview
- Abusing Group Policy Caching #Windows #PrivEsc
- cPanel UI & Permission bug leads to source code dump of millions of sites #Web
- Security: Bitwarden Desktop app grants RCE to Bitwarden developers #Desktop #RCE
- Backdoors and other vulnerabilities in HiSilicon based hardware video encoders #RCE #IoT
- No buffers harmed: Rooting Sierra Wireless AirLink devices through logic bugs #RCE #LUA
- Escaping the Dark Forest #SmartContract
- The Return of Raining SYSTEM Shells with Citrix Workspace app #PrivEsc

Bug bounty writeups

- CVE-2020-9964 – An iOS infoleak (Apple)
- Taking down the SSO, Account Takeover in the Websites of Kolesa due to Insecure JSONP Call
- Dangling DNS: AWS EC2 ($2,900)
- Hacking the Medium partner program (Medium)
- suPHP – The vulnerable ghost in your shell

- Reflected XSS on www.hackerone.com via Wistia embed code (HackerOne, $500)
- [steam client] Opening a specific steam:// url overwrites files at an arbitrary location (Valve, $750)
- CVE-2020-3187 – Unauthenticated Arbitrary File Deletion (U.S. Dept Of Defense)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- NoSQLi & Intro: NoSql Injection Go tool
- Hetty: HTTP toolkit for security research. It aims to become an open source alternative to commercial software like Burp Suite Pro, with powerful features tailored to the needs of the infosec and bug bounty community
- Duplicut: C tool that remove duplicates from MASSIVE wordlist (e.g. a billion entries and 10GB), without sorting it (for dictionnary-based password cracking)
- PostMessage POC Builder: @honoki's tool to build POCs for cross-domain postMessage vulnerabilities
- Offensive Terraform Modules: Automated multi step offensive attack modules with Infrastructure as Code(IAC)

More tools, if you have time

- gitjacker: Go tool for extracting content from sites that have an exposed .git directory
- Cloudleaks & Intro: Search engine that indexes S3 buckets and their content
- Whalescan: Vulnerability scanner for Windows containers, which performs several benchmark checks & checks for CVEs/vulnerable packages on the container
- Offensive Docker VPS & Offensive Docker
- ReconNote: Python automated recon framework with a GUI
- go-stare: A fast & light web screenshot without headless browser but Chrome DevTools Protocol!
- httpimg: Headless screenshot tool for web servers (uses wkhtmltoimage)
- AutoDirbuster & Intro: Automatically Run and Save DirBuster Scans for Multiple IPs
- Wappy: A CLI tool to discover technologies in web applications. It uses the wap library, that is a python implementation of the Wappalyzer browser extension
- Wafalyzer: Web Application Firewall (WAF) Detector

Misc. pentest & bug bounty resources

- HowToHunt
- Awesome Stars
- TJnull's guide to building a Home Lab
- File Upload Bypass
- BugBountyTips-AMA
- @RenwaX23's ES6 Unicode Encoder/Decoder

Challenges

- Hands On Hacking practice labs
- Practice CTF List / Permanent CTF List

Articles

- Critical Information Disclosure on WP Courses plugin exposes private course videos and materials
- NTHashes and Encodings
- Are You Docking Kidding Me?
- A different way of abusing Zerologon (CVE-2020-1472)
- Securing Windows networks against WSUS attacks
- Macos Injection Via Third-party Frameworks
- New Snort, ClamAV coverage strikes back against Cobalt Strike
- Categorizing human phishing difficulty: a Phish Scale

News

Bug bounty & Pentest news

- GitLab's top tips for better bug bounty reports, plus a hacker contest!
- Introducing The 4th Annual Hacker-powered Security Report
- Code for free Spyse trial (valid until October 10)
- ZAP Sites Tree Modifiers

Reports

- Gamers fragged by surge in credential stuffing attacks during lockdown

- Microsoft report shows increasing sophistication of cyber threats
- Youth unemployment risks fueling Indian cybercrime boom

Vulnerabilities

- Action View: XSS bug discovered in popular Ruby Gem
- FortiGate VPN Default Config Allows MitM Attacks
- Twitter is warning devs that API keys and tokens may have leaked
- Take your pick: 'Hack-proof' blockchain-powered padlock defeated by Bluetooth replay attack or 1kg lump hammer
- Node.js applications open to prototype pollution attacks via legacy function in popular encryption library

Breaches & Attacks

- Microsoft Security—detecting empires in the cloud
- 'OldGremlin' in the system: Russian-speaking ransomware group defies 'unspoken rule' against attacks on home soil
- CISA alert: Federal Agency Compromised by Malicious Cyber Actor
- Microsoft leaks 6.5TB in Bing search data via unsecured Elastic server. *Insert 'Wow... that much?' joke here*
- Windows XP source code leaked online, on 4chan, out of all places
- Microsoft says it detected active attacks leveraging Zerologon vulnerability &As you're scrambling to patch the scary ZeroLogon hole in Windows Server, don't forget Samba – it's also affected
- Airbnb may be exposing private host inbox messages, bookings and earnings data

Other news

- This Hacker Creates Fake Cheats That Make Cheaters Jump Off Buildings In-Game
- Pastebin adds 'Burn After Read' and 'Password Protected Pastes' to the dismay of the infosec community
- Students Are Pushing Back Against Proctoring Surveillance Apps
- Nist Overhauls "security And Privacy Controls" Publication – Here's What You Need To Know
- Tribune Publishing apologizes for fake bonus offer in phishing-simulation email
- Spain's highway agency is monitoring speeding hotspots using bulk phone location data

Non technical

- Proposal of a Novel Bug Bounty Implementation Using Gamification
- No, Moving Your SSH Port Isn't Security by Obscurity
- 'I thought it was a complete fluke' – Katie Paxton-Fear on her bug bounty baptism and why AI will never fully replace security researchers
- 'I'm not a fan of critical bugs' – Santiago Lopez on his route to becoming the world's first bug bounty millionaire
- Hacker Spotlight: Interview With Bitk
- A guide to Twitter for bug hunters
- On Pen Testing Rabbit Holes, and How to Avoid Them
- No Trespassing In The Cloud

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 09/18/2020 to 09/25/2020.