Bug Bytes #79 – Burp's story, postMessage XSS on Tumblr & Go tools for faster recon

BY ANNA HAMMOND · JULY 15, 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 03 to 10 of July.

Our favorite 5 hacking items

1. Videos of the week

Ask me anything, with Burp Suite creator Dafydd Stuttard

URL validation bypass | Filedescriptor solves Intigriti's XSS challenge

The first video is a fun one for Burp lovers. @DafyddStuttard answers questions we've all been wondering about: Why "Burp" and "PortSwigger"? Who is "Peter Wiener"? Why Java?...

The second video is a very informative walkthrough of our June XSS challenge. @filedescriptor goes through different solutions including how to bypass a loose regex used for URL validation, with IPv6.

2. Writeup of the week

Art of bug bounty: a way from JS file analysis to XSS (Verizon Media & Tumblr, $1,000)

This is a well-written writeup on XSS via postMessage. @zoczus comments on portions of code to explains what led him to the bug. Highly recommended if you're interested in DOM XSS!

3. Article of the week

Six files that are also a valid PHP

This is a cool resource on creating files that have two formats (e.g. GIF + PHP, or PHP + PDF). It might be helpful for bypassing file upload restrictions.

4. Tools of the week

LORC

ParameterMiner

gofingerprint

@_StaticFlow_ has added 3 new interesting tools to his collection:

ParameterMiner takes a JavaScript file URL as input and returns all variable names found in the JS file.

Gofingerprint helps with Web server fingerprinting. This can be used to quickly identify specific types of servers in your historic data and test them for new vulnerabilities.

LORC (Low Orbit RECON Cannon) is a recon tool that distributes the work using a client/server architecture.

5. Tutorial of the week

An offensive guide to the Authorization Code grant

Yes, another article on OAuth 2.0 attacks! But I really like how this one is organized: For each parameter used in OAuth grant flows (e.g. *state*, *code*, *redirect_uri*...), it tells you what to look for. It's like a high-level organized cheat sheet.

Other amazing things we stumbled upon this week

Videos

- INTERVIEW WITH Chloé Messdaghi || DIVERSITY, WOMEN IN INFOSEC, BUG BOUNTY AND BURNOUT
- Burp for Beginners: How to Use Intruder
- Hakluke Talks About Creating Content, Bug Hunting, Pentest, OSCP and How To Get Started in Hacking!
- My First $15,000 Microsoft Windows Insider Preview Bug Bounty | How to Get Started
- IPv6 Tunneling – Joff Thyer – PSW #657 (starts at 7min 35s)
- Hacking Sunday ep 3 (JWT) & Lab
- $20,000 Hackerone data leakage via GraphQL
- How To Convert Linux Packages With Alien
- Top tier bounty beginner advice from uncle rat
- Why i prefer docker over a VM
- Interview with a hacker: Chris Dale, Principal consultant and founder of river security

Podcasts

- Behind The Bounty
- Huntr EP003 bug huntr – Tips and tricks from a huntr sheriff

- CoalCast #16 – Byt3bl33d3r Returns
- Cybertalk – EP7 – OPSEC & Personal Security Guide
- Darknet Diaries EP 69: Human Hacker
- Million Dollar Fraud
- Shared Security – F5 BIG-IP Exploit, WiFi Router Security Updates, Password Reuse
- Shared Security – TikTok Privacy Concerns, macOS Ransomware, Bad Passwords
- Security Now 774 – 123456
- Risky Business #591 — EncroChat user experience includes getting owned, going to prison

Webinars & Webcasts

- Weaponizing Recon for Fun & Profit by Harsh Bothra
- Hacker Days: iOS Application Vulnerabilities and how to find them
- What about Ransomware? w/ John Strand (1-Hour)
- Extending Your Home Lab to include Cloud
- What Do I Need to Know About CVE-2020-5902; the F5 Networks BigIP RCE Vulnerability

Conferences

- sec4dev 2020
- fwd:cloudsec 2020 & Schedule
- Cyber June'gle Virtual Summit 2020

Slides & Workshop material

- XSS Everywhere! What is it, why should I care, and how can I avoid it? (Next live session in on July 23)

Tutorials

Medium to advanced

- Server Side JavaScript Injection
- Hunting for Endpoints
- Messing up with WebViews on jailbroken iOS
- DLL Search Order Hijacking & DLLHSC

- Payload Delivery for DevOps : Building a Cross-Platform Dropper Using the Genesis Framework, Metasploit and Docker
- Reading Windows Sticky Notes

Beginners corner

- Exploiting Spring Boot Actuators
- Top 16 Active Directory Vulnerabilities
- One custom certificate, Using all tools and your devices (for bug bounty/pentesting)
- Weaponizes nuclei Workflows to Pwn All the Things
- Web application race conditions: It's not just for binaries.
- Evading Firewalls with Tunnels

Writeups

Challenge writeups

- 0CTF/TCTF noeasyphp – Down the FFI Rabbit Hole (Part 1) & From Web to Pwn – FFI Arbitrary read/write without FFI::cdef or FFI::load (Part 2)
- Copy Drag — Paste Drop
- Insecure iOS Storage – DVIAv2 Part 1 & Bypassing JailBreak Detection – DVIAv2 Part 2

Pentest writeups

- FROM ZERO INFO TO ZERO-DAY
- Warcodes: Attacking ICS through industrial barcode scanners

Responsible(ish) disclosure writeups

- Adventures in Citrix security research, Citrix provides context on Security Bulletin CTX276688 & RIFT: Citrix ADC Vulnerabilities CVE-2020-8193, CVE-2020-8195 and CVE-2020-8196 Intelligence #Web
- Remote Code Execution in Citrix ADC #Web #CodeReview
- Bypassing file upload filter by source code review in Bolt CMS #Web #CodeReview #PHP #RCE
- Drupal 8 Remote Code Execution by estimating installation time of site #RCE #Web #CodeReview
- Android MX Player — Path Traversal to Code Execution & PoC #Android #RCE
- CVE-2020-1300: Remote Code Execution Through Microsoft Windows CAB Files #Windows #RCE
- Mutation Cross-Site Scripting (mXSS) Vulnerabilities Discovered in Mozilla-Bleach #Web

- AVideo < 8.9 Privilege Escalation and File Inclusion that led to RCE #Web #CodeReview #PHP
- FDEU-CVE-2019-10222 #Router #RCE
- Dismantling BullGuard Antivirus' online protection #Web

Bug bounty writeups

- Why I paid 3.5K to become a TLD registrar reseller when doing bug bounty ($7,500)
- Case Study I – Browser Anomaly with Facebook Apps -1500$ (Facebook, $1,500)
- Issue 1040755: Security: Another "universal" XSS via copy&paste (Google/Chromium, $2,000)
- Blast from the past: Cross Site Scripting on the AWS Console (Amazon)
- XSS in Zoom.us Signup Flow (Zoom)
- Global grant uri in Android 8.0-9.0 (2018 year) (Google)
- My First Bug: Blind SSRF Through Profile Picture Upload
- Stealing Zomato X-Access-Token: in Bulk using HTTP Request Smuggling on api.zomato.com (Zomato, $5,000)
- Blind SSRF on https://labs.data.gov/dashboard/Campaign/json_status/ Endpoint (TTS Bug Bounty, $300)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- IOXY (IoT + Proxy) & Intro: An MQTT intercepting proxy written in Golang. It supports MQTT, MQTTS and MQTT over WebSockets and has both a CLI and a GUI
- JSMon & Intro: A javascript change monitoring tool for bug bounties
- Introducing Chaos Bug bounty recon data API
- PAN-OS GlobalProtect Portal Scanner: Determine the Palo Alto PAN-OS software version of a remote GlobalProtect portal or management interface
- Foam: A personal knowledge management and sharing system inspired by Roam Research, built on Visual Studio Code and GitHub
- Urlgrab: A golang utility to spider through a website searching for additional links

More tools, if you have time

- Pipx: Install and Run Python Applications in Isolated Environments & How id differs from pyenv/pipenv

- Fermion: An electron wrapper for Frida & Monaco
- aaaguirrep/pentest & Video tutorial: Docker image for pentest/bug bounty
- Slicer: A tool to automate the boring process of APK recon
- CodeArgos: Detect and watch for changes to Javascript files and scriptblocks of a target web app
- graftcp: A flexible tool for redirecting a given program's TCP traffic to SOCKS5 or HTTP proxy
- Webgrep: Python tool for grepping Web pages
- DomainExtractor: Extract domains/subdomains/FQDNs from files and URLs, with a log of new domains found
- favihash: Subdomains enumeration via favicon.ico hashing
- SMBGhost (CVE-2020-0796) and SMBleed (CVE-2020-1206) Scanner:
- GoGhost: High Performance, lightweight, portable Open Source tool for mass SMBGhost Scan
- Cloudtopolis: A tool that facilitates the installation and provisioning of Hashtopolis on the Google Cloud Shell platform, quickly and completely unattended
- LeakDB: Python tool that let's Red Teams build their own plaintext version of "Have I Been Pwned"

Misc. pentest & bug bounty resources

- Project straylight
- Tiny-XSS-Payloads: @terjanq's collection of short XSS payloads that can be used in different contexts
- Metasploit exploit for Directory Traversal in Spring Cloud Config Server (CVE-2020-5410)
- Uphack: Learn application security, for free.
- How does Single Sign-On work?
- Pentest Lab: Local penetration testing lab using docker-compose
- BinaryEdge Cheatsheet
- Google Advanced Search Operators
- thelikes/fuzzmost: Wordlists for asset discovery, fuzzing & password spraying
- letmeoutofyour.net & Let Me Out of Your Net – Egress Testing: Server that listens on all ports for HTTP, HTTPS & SSH. And script to find out open ports/protocols on your network (useful for egress filtering/data exfiltration)
- How to Set Up Your Hardware Lab

Challenges

- "Cracking JWT keys" challenge by @digininja
- @SecurityMB's XSS challenge #3

Articles

- Understanding the root cause of F5 Networks K52145254: TMUI RCE vulnerability CVE-2020-5902
- Bean Stalking: Growing Java beans into RCE
- Reverse Engineering Nike Run Club Android App Using Frida
- A Second Look at CVE-2019-19781 (Citrix NetScaler / ADC)
- Patchless AMSI bypass using SharpBlock
- Restricting SMB-based lateral movement in a Windows environment
- MS08_068 + MS10_046 = FUN UNTIL 2018
- WastedLocker Goes "Big-Game Hunting" in 2020

News

Bug bounty & Pentest news

- Facebook offers $40k for JavaScript vulnerabilities in bug bounty program
- Defcon AppSec Village CTF Task Fight: Deadline is July 24
- Open source community toasts efforts of EU-FOSSA 2 bug bounty program

Reports

- Home router security report 2020
- Number of stolen credentials on cybercrime marketplaces quadruples in just two years

Vulnerabilities

- Firefox spoofing bug row rumbles on two years after first report
- Citrix, Juniper and VMware patch array of vulnerabilities
- Citrix tells everyone not to worry too much about its latest security patches. NSA's former top hacker disagrees & FYI: Someone's scanning gateways, looking for those security holes Citrix told you not to worry too much about
- Palo Alto Networks fixes another severe flaw in PAN-OS devices (CVE-2020-2034)
- Sony awards $10,000 bug bounty for PlayStation 4 kernel exploit

- Hacking smart devices to convince dementia sufferers to overdose
- Researchers create magstripe versions from EMV and contactless cards
- Popular TP-Link Family of Kasa Security Cams Vulnerable to Attack
- Zoom working on patching zero-day disclosed in Windows client

Breaches & Attacks

- 240 top Microsoft Azure-hosted subdomains hacked to spread malware
- Sixteen Facebook apps caught secretly sharing data with third-parties
- WordPress security: RCE flaw in Adning Advertising plugin exploited in the wild & Technical writeup
- Phishing attacks: This sophisticated new group has been operating undiscovered for at least a year
- Over 1,300 phishing kits for sale on hacker forum
- Joker Android malware keeps evading Google Play Store defenses
- Cerberus banking Trojan infiltrates Google Play
- More pre-installed malware has been found in budget US smartphones
- Keeper Threat Group Rakes in $7M from Hundreds of Compromised E-Commerce Sites
- Windows POS malware uses DNS to smuggle stolen credit cards

Other news

- Apple: Closing MacBooks with camera covers leads to display damage
- Risky blogspot.in domain for sale after Google fails to renew it
- Firefox Send suspended amid concern over malware abuse
- Malwarebytes AdwCleaner now removes malware from the command line
- Microsoft's new KDP tech blocks malware by making parts of the Windows kernel read-only
- Microsoft touts free malware-busting virtual machine forensics service (Project Freta)
- Google Chrome 84 released next week with revived SameSite cookie changes

Non technical

- DNS Cache that almost ruined my PoC for a private bug bounty program, and a few tips on avoiding the same
- Bug Business #5 – Get to know Intigriti's Q1 Top 3 Hackers: bitmap

- Hacker Spotlight: Interview with meals
- Researcher Spotlight: RQU
- Is Zoom's $500,000 RCE really not worth it?
- Sustaining Performance Under Extreme Stress
- Bug bounty writeups using nothing but emojis
- Troubleshooting Burp with iOS 13 or higher

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 07/03/2020 to 07/10/2020.