Bug Bytes #76 – How to learn anything, Fantastic writeups & A tool to play with Burp's REST API

BY ANNA HAMMOND · JUNE 24, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-76-how-to-learn-anything-fantastic-writeups-a-tool-to-play-with-burps-rest-api

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 12 to 19 of June.

Our favorite 5 hacking items

1. Tool of the week

Seltzer & Intro

Seltzer is a Bash script and Burp extensions by Coalfire, that make it really easy to user Burp 2.0's REST API. With a simple command, you can start Burp in headless mode, scan a target, monitor the progress, export results and save the Burp project file.

This may be the fastest way to start playing with Burp's REST API!

2. Writeups of the week

The Curious Case of Copy & Paste – on risks of pasting arbitrary content in browsers (Google & Mozilla, $30,000)

How I made more than $30K with Jolokia CVEs ($33,500)

Hacking Starbucks and Accessing Nearly 100 Million Customer Records (Starbucks, $4,000)

One Token to leak them all : The story of a $8000 NPM_TOKEN & Video (Google, $8,000)

SMTP Injection in Gsuite (Google, $3,133.7)

I know... How can there be 5 writeups of the week, right? Actually, these are all incredible findings worth reading about. In a nutshell:

@securitymb presents new research on copy-pasting issues in browsers, WYSIWYG editors & websites. In total, 9 bugs including universal XSS, mutation XSS & CSS data exfiltration.

@itsecurityguard shares how he leveraged existing Jolokia CVEs to make it rain bounties. The writeup is particularly interesting if you want to learn about setting up a test environment and applying exting research to bug bounty.

@samwcyo tells in great details how he accidentally found a path traversal bug on Starbucks. Not only does he share the final payload, but the whole thought process: How he identified a suspicious request, questions he asked himself at each step, indicators of vulnerability, payloads tested...

@AseemShrey writes about a well-hidden NPM token found by analyzing JavaScript code. An excellent read if you want to learn about JS analysis.

Zohar Shachar explains how he found an SMTP injection in Google and could spoof any email address! Impressive, the bounty seems suprisingly low considering the impact and the target.

3. Video of the week

Interview with @Th3G3nt3lman || Recon, Methodology, Learning etc.

@farah_hawa01 looks like a rising bug hunter and Youtuber. I love her style: concise, straight to the point and professional. This video in particular features @Th3G3nt3lman. Watch it if you want to hear about his no BS approach to recon and efficient bug hunting.

4. Tip of the week

> **"I'm claiming if they had just started immediately, with anything, even the first shittiest tutorial that shows up as the first result on Youtube, they would now be closer to their goal than after they made that plan"**
>
> From How To Learn Something New? – Game Devlog #1

I was about to dismiss this video, thinking it was about game development... But watched it anyway because @LiveOverflow has a knack for making any topic interesting.

I'm glad I did! Around the 15 min mark, he mentions his secret for learning anything: Just pick up any resource ("even the shittiest") and start there. Don't overthink it, don't make sophisticated plans. Then, follow it up with another resource by reserching words you didn't understand.

It might not work for everyone, but this is definitely something I needed to hear. I generally tend to spend too much time planning, then lacking the time to actually execute the plan! This learning approach works better when time is lacking.

5. Tutorial of the week

Building a Discord Bot for ChatOps, Pentesting or Server Automation, Part 2 & Part 3

This is an interesting idea: A Discord bot that allows you to run any command on a remote server. Writing `!exec ls` in Discord would execute `ls` on the server, and display the results in Discord.

Between this and the ability to run tools that send Discord notifications when new results are found, everything can be done from a phone... Recon on the move, movie-style!

Other amazing things we stumbled upon this week

Videos

- Katie Explains: Top 10 API Bugs (and Where to Find Them)
- Q&A: Bug Bounty with Katie (InsiderPhD)

- BOUNTY THURSDAYS – All about them writeups and content creators.
- INTERVIEW WITH @Th3G3nt3lman | | RECON, METHODOLOGY, LEARNING ETC.
- Web, Android and API hacking...all in ONE place! #bugbounty #hacking #pentest
- Job Application Tips
- Raspberry Pi Project: Kali Linux Tablet (Kali-Pad) The Ultimate Pentesting Device

Podcasts

- Security Now 771 – Lamphone
- Risky Business #588 — Catastrophic bugs to plague ICS for years
- Layer 8 Podcast Episode 29: Social Engineers from Rapid7
- Huntr Podcast: How a 16 year old made it into top 100 on HackerOne
- CallStranger, SMBleedingGhost, & Misconfigured Kubeflow – ASW #111
- Ripple 20, Akamai DDoS, & CallStranger – Wrap Up – SWN #44
- T-Mobile Outage, DARPA Bug Bounties, & Bob Erdman – SWN #43

Webinars & Webcasts

- SANS@MIC -Arcane web and mobile application vulnerabilities
- frida-boot – a binary instrumentation workshop, using Frida, for beginners & Workshop material
- Introduction to Callidus (Red Team assessments Tool)
- Bad As You Want To Be – Adversary Emulation Basics (Free registration required)
- Webinar: Password Recovery 101 – Cracking More of Your List
- Webcast: Securing Active Directory: Performing Your Own AD Security Review
- SANS@MIC – Maldocs: a bit of blue, a bit of red
- You Can Write an Infosec Book!

Conferences

- BSidesATL 2020

Slides & Workshop material

- [mDevCamp 2020] Reversing Android Apps
- [mDevCamp 2020] iOS Security: Deep Dive I & Deep Dive II

Tutorials

Medium to advanced

- Introducing Axiom – The Dynamic Pwnstation Orchestrator for Red Team & Bug Bounty
- Understanding Web Security Checks in Firefox (Part 1)
- How to exploit the DotNetNuke Cookie Deserialization
- Proxyjump, the SSH option you probably never heard of
- Introduction to GKE Kubelet TLS Bootstrap Privilege Escalation
- Building a Discord Bot for ChatOps, Pentesting or Server Automation, Part 2 & Part 3
- Abusing access to mount namespaces through /proc/pid/root
- Understanding and Bypassing AMSI
- Autocrack – A Responder to Hashcat Queue with Notifications
- PE Parsing and Defeating AV/EDR API Hooks in C++
- Making AMSI Jump

Beginners corner

- Just another Recon Guide for Pentesters and Bug Bounty Hunters
- PostMessage Vulnerabilities. Part I
- How to pentest: proprietary protocols
- Bypassing Android's RootBeer Library (Part 2)
- Python For Pentesters: Beyond the basics. Part1
- Horizontal domain correlation
- How to Deal with FlutterApp Penetration Testing (Another Way to Bypass SSL Pinning)
- Using GPU Accelerated Hashcat on Google Colaboratory FREE!
- Bettercap Usage Examples (Overview, Custom setup, Caplets)
- Covert Channel Discovery: Understanding Network Extrusions
- Attacking a real VoIP System with SIPVicious OSS
- IPv6 Exploitation in AD environment
- Active Directory Lab for Penetration Testing

Writeups

Challenge writeups

- NahamCon 2020 CTF Writeup
- NahamCon – Trash the Cache Write-up (Web 1000)

Pentest writeups

- Analyzing an RFID scanner: bad habits never die
- Local file reading using PDF generation via user cookie

Responsible(ish) disclosure writeups

- SMBleedingGhost Writeup Part II: Unauthenticated Memory Read – Preparing the Ground for an RCE #SMB #RCE
- Cisco WebEx Memory for the Taking: CVE-2020-3347 #Windows #MemoryLeak
- Examining a Phishing Vector in Plex Media Server #Web
- Composr CMS Remote Code Execution #PHP #Deserialization #Web
- Aprima PRM (EHR) patient portal security bypass #Web #JWT
- Pulse Secure Client for Windows <9.1.6 TOCTOU Privilege Escalation (CVE-2020-13162) #PrivEsc #VPN
- A Click from the Backyard | Analysis of CVE-2020-9332, a Vulnerable USB Redirection Software #USB
- MZ-20-03 – New security advisory regarding vulnerabilities in .Net #.NET #Windows
- DigDash Enterprise: Versions 2018R2-2020R1 #Web
- Security Advisories: D-Link DSL-2640B #Router #Web
- SSD Advisory – Mimosa Routers Privilege Escalation and Authentication bypass #PrivEsc #CodeReview #Python
- Technical Advisory – ARM MbedOS USB Mass Storage Driver Memory Corruption #CodeReview #C++ #MemoryBugs
- Striking Back at Retired Cobalt Strike: A look at a legacy vulnerability #Web

Bug bounty writeups

- Bug bounty bout report 0x01 – WebRTC edition
- A subtle stored-XSS in WordPress core (WordPress)
- Guest Blog: From File Upload to RCE
- GHSL-2020-099: mXSS vulnerability in AngularJS (GitHub Security Lab)
- SQL injection on contactws.contact-sys.com in TScenObject action ScenObjects leads to remote code execution (QIWI, $5,500)

- Remote Code Execution on contactws.contact-sys.com via SQL injection in TCertObject operation "Delete" (QIWI, $1,000)
- SSRF – Guard – Unchecked HKP servers (Open-Xchange, $400)
- Rack parses encoded cookie names allowing an attacker to send malicious `__Host-` and `__Secure-` prefixed cookies (Ruby on Rails)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Smuggler: An HTTP Request Smuggling / Desync testing tool written in Python 3
- Tsunami & Intro: Google's general purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence
- gDork: A Mozilla Firefox extension which allows quick access to your google-dorking result
- Whoareyou: A tool to find the underlying technology/software used in a list of websites passed through stdin (using Wappalyzer dataset)

More tools, if you have time

- Redirector: Redirects any request with which ever http status code you want to a location of your choice (useful for SSRF exploitation)
- PatchChecker & Online version: Web-based check for Windows privesc vulnerabilities
- SearchOutlook: A C# tool to search through a running instance of Outlook for keywords
- Get All Links – [gal]: Get all the links for target websites using href / src / url / etc.
- Nipe: An engine to make Tor network your default gateway
- WebTLSProfiler & Intro: Web interface for the TLS Profiler Python package
- Get-RBCD-Threaded
- Azure/container-scan: A GitHub action to help you scan your docker image for vulnerabilities

Misc. pentest & bug bounty resources

- CloudPentestCheatsheets
- Hidden parameter finder in source code
- The Hitchhiker's Guide to Web App Pen Testing
- @netbiosX's collection of battle-tested Aggressor Scripts for Cobalt Strike 4.0+
- devhints.io
- Applied Purple Teaming

- Chromium Disclosed Security Bugs & @BugsChromium

Challenges

- Kubernetes Goat & Guide
- Awesome Vulnerable Goat Projects
- @BenHayak 2020 XSS challenge
- JWT None algorithm challenge by @digininja

Articles

- YAA: An Obscure MacOS Compressed File Format: Includes steps to create an Eicar YAA archive
- Exfiltrating User's Private Data Using Google Analytics to Bypass CSP & Reddit discussion
- Broken phishing accidentally exploiting Outlook zero-day
- Adventures in Phishing Email Analysis
- A survey of recent iOS kernel exploits
- Office 365 Phishing Campaign Exploits Samsung, Adobe and Oxford Servers
- CVE-2020-1181: SharePoint Remote Code Execution Through Web Parts
- Passive host OS fingerprinting from an USB device during enumeration (Summary by MaMe82)
- Curl vs Wget

News

Bug bounty & Pentest news

- Hashcat v6.0.0 update
- Burp Suite Pro/Community 2020.5.1 released, with fixes for bugs in HTTP message editor and a security fix.
- Training to be a hacker with zseano
- GrinningSoul, the first iOS emulator designed for bug bounty hunters, is officially coming in Q3 2020!

Reports

- Boffins find that over nine out of ten 'ethical' hackers are being a bit naughty when it comes to cloud services
- Microsoft: COVID-19 malware attacks were barely a blip in total malware volume
- Ransomware: Hackers took just three days to find this fake industrial network and fill it with malware

Vulnerabilities

- Ripple20 vulnerabilities will haunt the IoT landscape for years to come
- How Hackers Use An Ordinary Light Bulb To Spy On Conversations 80 Feet Away
- Bug in 'USB for Remote Desktop' lets hackers add fake devices
- DTA fixed COVIDSafe Bluetooth vulnerability 21 days after it was notified
- Old GTP protocol vulnerabilities will also impact future 5G networks
- Cisco fixes severe flaws in Webex Meetings for Windows, macOS & New Cisco Webex Meetings flaw lets attackers steal auth tokens
- D-Link leaves severe security bugs in home router unpatched
- Netgear Zero-Day Allows Full Takeover of Dozens of Router Models
- Configuration loophole triggers XSS in Sanitize Ruby Gem
- SSB-Server vulnerability reveals contents of private messages

Breaches & Attacks

- South African bank to replace 12m cards after employees stole master key
- AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever
- How spies used LinkedIn to hack European defense companies
- Attackers impersonate secure messaging site to steal bitcoins
- Chrome extensions are 'the new rootkit' say researchers linking surveillance campaign to Israeli registrar Galcomm
- Extortionists threaten to destroy sites in fake ransom attacks
- Security surprise: Four zero-days spotted in attacks on researchers' fake networks
- North Korea's state hackers caught engaging in BEC scams
- Hackers use Google Analytics to steal credit cards, bypass CSP
- Copy-Paste Threat Actor in the Asia Pacific Region
- CoinMiner exploits Apple APSDaemon vulnerability to evade detection

Other news

- eBay staff charged with cyberstalking, sending fetal pig and spiders
- Masked arsonist might've gotten away with it if she hadn't left Etsy review
- Zoom will offer proper end-to-end encryption to free vid-chat accounts – not just paid-up bods – once you verify your phone number...

- Theft of CIA's 'Vault 7' Secrets Tied to 'Woefully Lax" Security
- Amnesty calls out countries with 'most dangerous' contact tracing apps
- Intel will soon bake anti-malware defenses directly into its CPUs
- Adversarial attacks against machine learning systems – everything you need to know

Non technical

- The Security Practitioner's Intro to the Cloud: Everything You Ever Wanted to Know But Were Afraid to Ask
- Workflow Improvements for Pentesters
- Researcher Spotlight: Nizam Abdallah
- Hacker Spotlight: Interview with Corb3nik
- Hacking the Singapore Government: Q&A with Hacker Personality Samuel Eng
- Q & A With Singaporean Hacker @Kactros_n
- Embedded security fails in ICS
- Let's discuss 2-Factor Authentication
- The importance of personal documentation
- What happens if your AWS Credentials are leaked on GitHub.

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 06/12/2020 to 06/19/2020.