Bug Bytes #82 – Timeless timing attacks, Grafana SSRF, Pizza & Youtube delicacies

BY ANNA HAMMOND · AUGUST 5, 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 24 to 31 of July.

Our favorite 5 hacking items

1. Videos of the week

How to start & 10 Tips For Crushing Bug Bounties in the First 12 Months

YES! @hakluke started a Youtube channel, and already released five videos including these two about getting started (and crushing it) in bug bounty. He offers actionable advice in a very direct but nice tone.

2. Writeups of the week

CVE-2020-13379 – Unauthenticated Full-Read SSRF in Grafana

h@cktivitycon – Pizza Time (Web 750)

Using XAMPP and Burp Intruder when scanning for subdomains to look for interesting behaviour & code

Three excellent writeups from three awesome bug hunters: @Rhynorater tells the story of a 0-day unauthenticated SSRF in Grafana. He found it by analyzing Grafana's source code, then applied his research to bug bounty programs.

@buerhaus wrote an impressive writeup of the "Pizza Time" challenge from the HacktivityCon CTF. It involves a blind SQL injection via chat bot, blind XSS via file upload, some JS and API magic, SSRF, and path traversal!

@zseano shared a sweet information disclosure. I generally love his writeups because they show how creative thinking and a straightforward methodology enable him to find unique bugs that most hunters miss. This writeup is no exception!

3. Articles of the week

XSS Exploitation in Django Applications

Timeless Timing Attacks: Exploiting Concurrency to Leak Secrets over Remote Connections & h2time.py

The first article is about XSS in the context of Django apps. It goes over specifics of the Django templating engine, the XSS protections it offers, and why it does not prevents all XSS attacks with different examples. @anthonypjshaw also shows a fuzzer he wrote to automate the detection of stored and reflective XSS in Django apps.

The second paper is about a new timing attack technique based on HTTP/2 multiplexing. It targets HTTP/2 webservers, Tor onion services, and Wi-Fi (EAP-pwd authentication). With Burp now supporting HTTP/2, this seems like a really interesting area to explore for bug hunters. There is also a Python implementation that helps test for this new attack.

4. Tutorial of the week

A Pentesters Guide – Part 5 (Unmasking WAFs and Finding the Source)

This is an excellent piece on bypassing WAFs like CloudFlare by finding your target's Origin IP. It sums up not only several known techniques, but also others I've never heard about like Crobat reverse lookups, or inducing the server to make a request to Burp Collaborator (revealing its real IP).

5. Tool of the week

GraphQL API Monitor

This is a node.js tool by @dee__see for monitoring GraphQL APIs. It takes as input URLs that return GraphQL schema files or APIs that support introspection. If the URL contents change, it does a comparison with *git diff* and sends the results to your pre-configured Discord webhook. Handy!

Other amazing things we stumbled upon this week

Videos

- HOURS & HOURS OF FREE CYBER SECURITY TRAINING??? (im loosing it)
- Casey John Ellis Interview
- HTML5 XSS attack vectors explained
- Getting Low Hanging Bugs With Nuclei
- The C2 Matrix | Golden Age of C2
- Nmap – Firewall Evasion (Decoys, MTU & Fragmentation) & Nmap – Scan Timing And Performance
- Bash Tricks
- $1,000 django CSRF protection bypass – Hackerone
- XSS Testing methodology demonstrated & 5 ways to test for IDOR demonstrated

Podcasts

- Security Now – rwxrwxrwx – Garmin Outage, Twitter Hack Update, GnuTLS
- Risky Business #592 — We're back. Did we miss anything?
- 7MS #425: DIY Pentest Dropbox Tips – Part 2
- The InfoSec & OSINT Show E18 – Simon Bennetts & Headless Automated Scanning with ZAP
- OSCP Certification: All you need to know & Blog post
- Tribe of Hackers Podcast @_sn0ww – Social Engineer RedTeamer
- Encryption Under 'Full-Frontal Nuclear Assault' By U.S. Bills

Webinars & Webcasts

- Webcast: Atomic Purple Team Framework and Life Cycle
- SANS webinars
  - No SQL Injection in MongoDB applications
  - Women in Cybersecurity Forum, presented by SANS Summits
  - Social Engineering Your Way to Success

Conferences

- OAuth Security Workshop 2020
- BsidesTLV 2020 – Hybrid Edition
- #HITBLockdown 002 & Schedule
- HOPE 2020 & Schedule

Tutorials

Medium to advanced

- Real-world JS 1
- Thycotic Secret Server: Offline Decryption Methodology
- So I Heard You Want to Learn Kafka
- Abusing Azure AD SSO with the Primary Refresh Token
- RANGE REQUEST DOS: AN UNCONTROLLED MEMORY CONSUMPTION VECTOR IN GO'S NET/HTTP
- In-Memory shellcode decoding to evade AVs/EDRs

- Covert Login Alerting

Beginners corner

- Building hacking tools in Windows using Docker
- Wayback Machine — A way forward in finding bugs (plus waywayback & waywayback-ffuf scripts)
- Second Order SQL Injection – Something Is Hidden Inside
- Do you trust your cache? – Web Cache Poisoning explained
- Are You Really Scanning What You Think?
- Almost everything about Browser Security for beginners- Part2
- Make the most out of BloodHound
- The Regular Expression Denial of Service (ReDoS) cheat-sheet
- Protecting Your Apps From Link-based Vulnerabilities: Reverse Tabnabbing, Broken-Link Hijacking, and Open Redirects

Writeups

Challenge writeups

- 3kCTF 2020 / WWWW

Responsible(ish) disclosure writeups

- Sometimes they come back: exfiltration through MySQL and CVE-2020-11579 #Web
- Hacking Node.js with buffer overflows #JavaScript
- Critical Arbitrary File Upload Vulnerability Patched in wpDiscuz Plugin #Web
- Local privilege escalation & Information disclosure in Origin #PrivEsc #Windows
- Missing signature validation of JWT when alg=none (in dp3t-sdk-backend) #Web
- IZI IZI, PWN2OWN ICS MIAMI #ICS #RCE
- Hacker, 22, seeks LTR with your data: vulnerabilities found on popular OkCupid dating app #Mobile #Web
- Windows Server Containers Are Open, and Here's How You Can Break Out #Windows

Bug bounty writeups

- New features means new bugs
- Stealing your Paytm information using XSS (Paymt, $1,261))

- Authorization bypass in Google's ticketing system (Google-GUTS) (Google)
- CVE-2020–9934: Bypassing the macOS Transparency, Consent, and Control (TCC) Framework for unauthorized access to sensitive user data (Apple)
- StillDNS Attack – Abusing of DNS interaction via CNAMEs loop – CloudFlare/Quad9 and PayPal DoS PoC (video writeup)
- Exploiting popular macOS apps with a single ".terminal" file.
- An unreproducable bug due to the load balancer, an unusual Open Redirect bug
- Zoom Security Exploit – Cracking private meeting passwords (Zoom)
- One Click to Compromise — Fun With ClickOnce Deployment Manifests (Microsoft)
- Exposed Docker Registry (U.S. Dept Of Defense)
- Bypass the CSP when popup with "javascript:" (Chromium, $500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- puredns: Wrapper around massdns, for accurately handling wildcard subdomains and DNS poisoning, and using clean public resolvers
- pentesterland-writeups-cli: Querying Pentester Land's curated collection of bug bounty writeups from command line

More tools, if you have time

- Winstrument & Intro: An Instrumentation Framework for Windows Application Assessments
- Xkeys: A Burp Suite Extension to extract interesting strings (key, secret, token, or etc.) from a webpage
- Urinteresting: Go script that takes URLs as input & returns a list of interesting ones
- IsCloudflare: Go script to check if an IP is owned by Cloudflare
- fastr3porter: Auto report generator for bug bounty hunters
- wzrd: A repository of scripts designed to ease the execution of common tools with optimized commands while only requiring the basic input parameters
- revp: Reverse HTTP proxy that works on Linux, Windows, and macOS
- Invoke-WordThief: A Powershell tool that extracts text from opened Microsoft Word and sends it over TCP to remote Python listener

- Chalumeau: An automated,extendable and customizable credential dumping tool based on powershell and python
- Mailpl0it: A small utility that hunts the homepage of exploit-db looking for user supplied quer(y/ies) and notifies the user via email if an exploit is found for the supplied query
- Depthcharge & Intro: A U-Boot hacking toolkit for security researchers and tinkerers

Misc. pentest & bug bounty resources

- Android Dynamic Analysis— using FrinJa Generic Scripts
- bounty-targets-data updated to support Intigriti & YesWeHack
- @thecybermentor AMA
- The State of the Kubernetes Ecosystem
- Kubernetes Primer for Security Professionals
- API Testing Checklist
- TRACE LABS OSINT VM
- Guide To Regular Expressions & Regexper
- @mubix's list of Repositories
- SANS pivoting cheat sheet

Challenges

- @trouble1_raunak's Hacking Sunday lab
- RatCTF2020: September 5

Articles

- Executing non-alphanumeric JavaScript without parenthesis
- Exploiting Electron Applications using Debug Feature
- Abusing Privilege Escalation in Salesforce Using APEX
- Automating search for websites having Bug Bounties
- DJI Privacy Analysis Validation
- Pentesting User Interfaces: How To Phish Any Chrome, Outlook, or Thunderbird User
- Analysis of the GnuTLS Session Ticket Bug (CVE-2020-13777)
- Sparkling Payloads

- Kubernetes Vulnerability Puts Clusters at Risk of Takeover (CVE-2020-8558)
- Get-AzPasswords: Encrypting Automation Password Data
- No, You Are Not Getting a CVE for That

News

Bug bounty & Pentest news

- Vulnhub joins the OFFSEC family
- Levelup0x07 Hack Another Day: August 22
- Hacker Jeopardy: Register before August 5/6
- Updates to the Windows Insider Preview Bounty Program
- New Web Security Academy topic: Information disclosure vulnerabilities
- End of the EU-FOSSA 2 Bug Bounty Program for Open Source Software

Reports

- Google: Eleven zero-days detected in the wild in the first half of 2020
- 30 app sec stats that matter
- France tops blue-chip cybersecurity maturity index
- Today's 'mega' data breaches now cost companies $392 million to recover from

Vulnerabilities

- Researchers exploit HTTP/2, WPA3 protocols to stage highly efficient 'timeless timing' attacks
- BootHole (CVE-2020-10713)
  - New bug in PC booting process could take years to fix, researchers say
  - BootHole fixes causing boot problems across multiple Linux distros
  - Grubbing Secure Boot the Wrong Way: CVE-2020-10713
- Attackers Exploiting High-Severity Network Security Flaw, Cisco Warns
- Fun fact: If you noticed a while ago Zoom's web client going AWOL for a week, it's because someone found a passcode-cracking hole
- New VPN flaws highlight proven pathway for hackers into industrial organizations & Remote Code Execution Risks in Secomea, Moxa, and HMS eWon ICS VPN Vulnerabilities: What You Need to Know
- WordPress plugin vulnerability exposes 80,000 sites to remote takeover

- KDE archive tool flaw let hackers take over Linux accounts
- If you own one of these 45 Netgear devices, replace it: Kit maker won't patch vulnerable gear despite live proof-of-concept code
- ASUS Home Router Bugs Open Consumers to Snooping Attacks
- Infosec bod: I've found zero-day flaws in Tor's bridge relay defenses. Tor Project: Only the zero part is right

Breaches & Attacks

- Theoretical technique to abuse EMV cards detected used in the real world
- Sneaky Doki Linux malware infiltrates Docker cloud instances
- Hackers stole GitHub and GitLab OAuth tokens from Git analytics firm Waydev
- UK and US warn QNAP owners to upgrade firmware to block malware
- Kaspersky: North Korean hackers are behind the VHD ransomware
- US defense and aerospace sectors targeted in new wave of North Korean attacks
- Garmin Pays Up to Evil Corp After Ransomware Attack — Reports

Other news

- Three people have been charged for Twitter's huge hack, and a Florida teen is in jail
- How the FBI tracked down the Twitter hackers
- Cerberus banking Trojan team breaks up, source code goes to auction
- Secure by design: ClassNK updates maritime cybersecurity guidelines
- Security professionals lose 'central watering hole' with demise of Peerlyst
- FBI warns of new DDoS attack vectors: CoAP, WS-DD, ARMS, and Jenkins
- EU sanctions Russian espionage unit, Chinese and North Korean firms

Non technical

- Hacker Spotlight: Interview with zlz
- 3 Things to be aware of to design the best Bug Bounty program
- So you want to be a pentester and/or red teamer?
- Career advice by @snyff
- The Four Quadrants of Conformism

- Zero Trust Model: What's a Zero Trust Network in Cyber Security?
- The Updated Security Pro's Guide to MDM, MAM, and BYOD

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 07/24/2020 to 07/31/2020.