Bug Bytes #83 – Web cache entanglement, SSRF via TLS, AST injection & New swag shop

BY ANNA HAMMOND · AUGUST 12, 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 31 of July to 07 of August.

Our favorite 5 hacking items

1. Conferences of the week

h@cktivitycon 2020

DEF CON Safe Mode, DEF CON 28Media server & Villages: AppSec Village, Red Team Village, Recon Village & Voting Village

Between these two conferences, there is enough videos and new research to keep anyone busy for weeks. There are so many valuable talks that I'm not sure where to start!

Just to give you an idea: @albinowax published his new research we're probably continue to hear about for months to come. @securinti presented an updated and longer version of his talk on pwning email systems. @jhaddix did a long version of his Bug Hunter Methodology workshop. @NahamSec and @_StaticFlow_ dropped some mindblowing knowledge on identifying assets in the cloud (although the video hasn't been shared yet). @heald_ben shared some cool findings on the Parse mobile app backend. @stokfredrik gave the ultime answer to "How to get started in bug bounties". @NotDeGhost and @ginkoid dived into WAF bypass techniques. @sajjadium and Seyed Ali demonstrated new Web Cache Deception techniques.

And this is just the tip of the iceberg!

2. Tool of the week

TLS Poison

SSRF is the golden goose of vulnerability classes. Just when you think everything has been said about it, someone comes up with a novel technique!

At the occasion of Black Hat and DEF CON, @joshmdx presented a new way to exploit SSRF via TLS (as well as CSRF via image tags). The method is similar to SNI injection but relies on behaviors inherent to TLS instead of bugs in a particular implementation.

To help exploit this new type of SSRF, @joshmdx released TLS Poison. This is definitely worth diving into and testing for!

3. Article of the week

Web Cache Entanglement: Novel Pathways to Poisoning, How to use Param Miner to detect fat GET cache poisoning & New "Web cache poisoning" topic on Web Security Academy

@albinowax dropped his new research, Web cache entanglement, that builds on his previous work on Web cache poisoning. It takes advantages of esoteric cache behaviors, and turns them into high impact exploit chains. Examples of attacks demonstrated include persistently poisoning every page of an online newspaper, and disabling Firefox updates by changing a single character in a legitimate request.

There is a lot to digest to understand Web cache entanglement (an article, a whitepaper, a talk, a Web Security Academy topics and labs, and a tool, param miner, updated to support testing for it)! But my gut tells me this will be the focus of a lot of bug hunters, just as Web cache poisoning has been the past year.

4. Writeup of the week

Vulnerabilities in the Openfire Admin Console

@shvetsovalex007 found an unauthenticated internal SSRF in Openfire. It is time to check your bug bounty notes for open ports 9090/http and 9091/https, to test for this!

5. Video of the week

Script Gadgets! Google Docs XSS Vulnerability Walkthrough

@LiveOverflow breaks down a very interesting XSS in Google spreadsheets. It is a complex finding that involves a chain of script gadgets and postMessage. An excellent example of a bug that is easily missed by automated tools.

Apart from technical details on the XSS, Google's security team provided some explanations on why the bug existed. And Nickolay, who found the bug, chimed in to answer questions on his background and why he specializes in a specific type of bugs and apps.

Other amazing things we stumbled upon this week

Videos

- BOUNTY THURSDAYS (CVE-2020-13379, Hackers Summercamp, Hackthebox, Bughunters Methodology 4, Nucleai)
- STÖK Chats! Bug bounties, hacking, content creation, fear, motivation, veganism, love and life
- What to do when you feel directionless
- @thedawgyg AMA

- HACKING OAuth 2.0 FOR BEGINNERS!
- Account Takeover: From zero to System Admin using basic skills
- Compromise any GCP Org Via Cloud API Lateral Movement and Privilege Escalation: Blackhat/Defcon 2020
- Pentest Story Time: My Favorite Hacks
- Windows and Linux Privilege Escalation – OSCP 2020

Podcasts

- Behind The Bounty – Matthew Bryant: XSSHunter
- The InfoSec & OSINT Show 19 – Tommy Devoss (Dawgyg) & Bug Bounty Hunting on Steroids
- Darknet Diaries EP 71: FDFF
- BootHole – Twitter Hackers Arrested, Garmin Hackers Get Ransom
- Risky Business #593 — China promises “mortal combat in the tech realm”
- The JerichShow Episode 15 – Supply Chain Side Effects and Data Leakage

Webinars & Webcasts

- CodeQL Roundtable stream w/@JLLeitschuh
- Webcast: What Can Docker Do for Me?
- Pwning Azure Deployments

Slides & Workshop material

- Black Hat USA 2020 presentations material

Tutorials

Medium to advanced

- Intercepting Request Which Requires VPN + Socks Proxy
- Password Spraying Secure Logon for F5 Networks
- Malicious Macros for Script Kiddies
- Kerberos Double-Hop Workarounds
- The Art of the Honeypot Account: Making the Unusual Look Normal
- IoT Security – Part 11 (Introduction To CoAP Protocol And Security)

- Implementing Secure Biometric Authentication on Mobile Applications

Beginners corner

- Second Order SQL Injection – Something Is Hidden Inside
- Debugging PHP code with vscode
- Building a lab with Server 2019 Server Core and PowerShell ...then attacking it!
- Debugging DLL's – 3 techniques to help you get started
- How To: Applied Purple Teaming Lab Build on Azure with Terraform (Windows DC, Member, and HELK!)
- Data Destruction 101
- Nmap -Pn (No Ping) Option Analysis
- RCE on Windows from Linux Part 6: RedSnarf

Writeups

Challenge writeups

- InCTF-2020 GoSQLv3 challenge writeup

Pentest writeups

- How i find Blind Remote Code Execution vulnerability
- Openvas Credentials Hunt — Part I
- The danger of world writable NFS shares

Responsible(ish) disclosure writeups

- Technical analysis: CVE-2020-15654 and a history of Firefox "Browser Lock" bugs #Browser
- Microsoft Teams Updater Living off the Land #Windows #SMB
- Remote Command Execution on RemotePC for Windows #RCE
- Hacking Cisco SD-WAN vManage 19.2.2 — From CSRF to Remote Code Execution #Router #RCE #Web
- X Site eScape (Part II): Look Up a Shell in the Dictionary #MacOS
- Exploiting an 'Unexploitable' SquirrelMail Bug for File Disclosure #Web
- SCP in OpenSSH 8.3p1 allows eval injection (CVE-2020-15778) #OpenSSH
- The Official Facebook Chat Plugin Created Vector for Social Engineering Attacks #Web

Bug bounty writeups

- Vulnerability in new TouchID feature put iCloud accounts at risk of being breached (Apple)
- The feature works as intended, but what's in the source?
- Refocusing in bug hunting, Bonus: An interestingly simple to test CSRF bypass
- CSRF PoC mistake that broke crucial functions for the end user/victim
- Apache Example Servlet leads to $$$$
- Blind SQL Injection at fasteditor.hema.com (HEMA)
- Reflected XSS at fotoservice.hema.nl (HEMA)
- Availing Zomato gold by using a random third-party `wallet id` (Zomato, $2,000)
- Account takeover in cups.mail.ru (Mail.ru, $1,500)
- Private list members disclosure via GraphQL (Twitter, $2,940)
- Improper use of "path" parameter can be used to trick testers into leaking their Front-End PoC (BugPoC, $1,000)
- Full Read SSRF on Gitlab's Internal Grafana (GitLab, $12,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Mole: A framework for identifying and exploiting out-of-band application vulnerabilities
- Link Lock: Distributed application to password-protect URLs using AES in the browser
- quoted-printable Parser: A Burp Suite extension to parse Content-Transfer-Encoding: quoted-printable emails received in Burpcollaborator's SMTP
- reNgine & Intro: An automated reconnaissance framework
- FestIn: S3 Bucket Weakness Discovery

More tools, if you have time

- Taser: Python3 resource library for creating security related tooling
- AutomatedHunter: Google Chrome Extension that automates testing fundamental Web Problems via Chrome
- Bucky: An automatic S3 bucket discovery tool
- Bug Bounty Recon (bbrecon) & Python library and CLI: Free Recon-as-a-Service API

- CWFF: Create your Custom Wordlist For Fuzzing
- rejig: An ansible+terraform suite to spawn and provision a virtual machine for attack purposes
- sshchecker: A ast dedicated SSH brute-forcing tool in Go, to check ssh login on a given list of IPs
- routopsy & Intro: A toolkit built to attack often overlooked networking protocols, like Dynamic Routing Protocols (DRP) & First-Hop Redundancy Protocols (FHRP)
- Smogcloud: Find AWS cloud assets that no one wants exposed
- PersistentJXA & Intro: Collection of macOS persistence methods and miscellaneous tools in JXA
- Aria Cloud & Intro: A Docker Container for remote pentesting over SSH or RDP, with a primary emphasis on cloud security tools and secondary on Active Directory tools
- ATTPwn: A Python tool designed to emulate adversaries conducting malware campaigns

Misc. pentest & bug bounty resources

- api.recon.dev
- Dynamic Labs & Intro
- Tenable Proof of Concepts
- Quick Tricks for Transferring Files & Big list of http static server one-liners
- wzrd: Repository of scripts designed to ease the execution of common tools with optimized commands while only requiring the basic input parameters
- The best hacking books for ethical hackers
- Week in OSINT's new website
- @hackerscrolls's 2FA & OAuth testing mindmaps
- Bonus security advice from attackers behind Ragnar Locker ransomware

Challenges

- Can you #spotthebug in this code?
- CONVEX (Cloud Open-source Network Vulnerability Exploitation eXperience)
- @SecurityMB's prototype pollution challenge
- @VULLNERAB1337's XSS challenge

Articles

- AST Injection, Prototype Pollution to RCE

- Unicode for Security Professionals & Interactive cheat sheet
- AWS Metadata Identity-Credentials Research
- Understanding Web Security Checks in Firefox (Part 2)
- Lights, Camera, HACKED! An insight into the world of popular IP Cameras
- Digging further into the Primary Refresh Token
- Preventing lateral movement in Google Compute Engine
- Reverse Engineering Starling Bank (Part I): Obfuscation Techniques & (Part II): Jailbreak & Debugger Detection, Weaknesses & Mitigations
- The OXID Resolver [Part 1] – Remote enumeration of network interfaces without any authentication, [Part 2] – Accessing a Remote Object inside DCOM & IOXIDResolver

News

Bug bounty & Pentest news

- The Official IEFT draft on OAuth 2.1 is out & OAuth Happy Hour Live Q&A (video)
- What's new in Burp Professional / Community 2020.8
- Swag for everyone: introducing our swag store!
- Microsoft Bug Bounty Programs Year in Review: $13.7M in Rewards
- Nuclei Unleashed – Quickly write complex exploits
- Metasploit 6 Now Under Active Development
- SECURITY@ 2020 CALL FOR SPEAKERS IS OPEN
- Virtual Cybersecurity Conferences
- OWASP AppSec Days (Free trainings): August 25 & 26

Reports

- DIY phishing kits dissected: Organizations urged to tackle the underground ecosystem that democratized cybercrime
- State of Open Source Terraform Security Report
- Apple is Most Imitated Brand for Phishing Attempts: Check Point Research's Q1 2020 Brand Phishing report
- Phishing campaigns, from first to last victim, take 21h on average
- Open source by the numbers at Google

Vulnerabilities

- An API Worm In The Making: Thousands Of Secrets Found In Open S3 Buckets.
- Smart locks opened with nothing more than a MAC address
- Researchers Warn of High-Severity Dell PowerEdge Server Flaw
- Team Pangu demonstrates unpatchable Secure Enclave Processor (SEP) chip vulnerability in iOS
- Twitter patches Android app to prevent exploitation of bug that can grant access to DMs
- Black Hat 2020: Web cache poisoning offers fresh ways to smash through the web stack

Breaches & Attacks

- Prototype pollution bug in popular Node.js library leaves web apps open to DoS, remote shell attacks
- Intel NDA blueprints – 20GB of source code, schematics, specs, docs – spill onto web from partners-only vault
- Hackers Broke Into Real News Sites to Plant Fake Stories
- Reddit hit by coordinated hack promoting Trump's reelection
- Twitter hacker's virtual trial 'zoom bombed' after ID leak
- Cluster of 295 Chrome extensions caught hijacking Google and Bing search results
- Ransomware: The tricks used by WastedLocker to make it one of the most dangerous cyber threats
- Iranian hacker group becomes first known APT to weaponize DNS-over-HTTPS (DoH)

Malicious apps/sites

Other news

- Google, WiCyS, SANS join forces to launch all-female information security scholarship
- Data breach notification website Have I Been Pwned? will be open sourced – Troy Hunt
- Microsoft and Google join industry coalition aimed at quashing open source security bugs & Threats, Risks, and Mitigations in the Open Source Ecosystem
- Here's the NSA's advice for reducing the exposure of cellphone location data
- China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI
- US government offers $10 million reward for information on cyber interference in elections
- Ohio becomes first state to release vulnerability policy for election-related websites
- Top voting vendor ES&S publishes vulnerability disclosure policy

- We give up, Progressive Web Apps can track you, says W3C: After 5 years, it decides privacy is too much bother & Demo of the issue
- Facebook open-sources one of Instagram's security tools
- BlackBerry releases new security tool for reverse-engineering PE files

Non technical

- Bug Business #7 – Get to know *jca*, Intigriti's Top Hacker in Q2
- Community Spotlight: Farah Hawa
- Hacker Spotlight: Interview with CDL
- Accessibility Within Application Security Tools
- 3 Tips to Avoid WFH Burnout
- How Attackers Bypass MFA and Conditional Access to Compromise Email Accounts
- Some proper chilled hacking vibes

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 07/31/2020 to 08/07/2020.