Bug Bytes #86 – Stealing local files with Safari, Prototype pollution vs HTML sanitizers & A hacker's mom learning bug bounty

BY ANNA HAMMOND · SEPTEMBER 2, 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 21 to 28 of August.

Our favorite 5 hacking items

1. Resource of the week

GitLab's Red Team Tech Notes

GitLab's red team are sharing tech notes in this repo. It currently contains technical papers, talks, tools and red team exercises. The notes on testing Kubernetes and Google Cloud Platform are excellent resources.

They are also planning to share even more of their day to day work, so it is worth keeping an eye on this.

2. Writeup of the week

Stealing local files using Safari Web Share API

This is a writeup of a browser bug found in Safari. It leverages the Web Share API that allows for sharing links from the browser using other apps (e.g. mail and messaging apps in both iOS and Mac OS).

The bug works by publishing a malicious page containing a "Share with friends" button. When someone visits the page and shares it with someone, it automatically adds to the email or message local files mentioned in the malicious page's source code. @h0wlu shows proofs on concept for leaking /etc/passwd and Safari's browsing history.

This is not a critical bug. It requires user interaction and is similar to clickjacking. But I find interesting that it exploits the new Web Share API and allows for stealing local files from any malicious website.

3. Article of the week

Prototype pollution – and bypassing client-side HTML sanitizers & Prototype pollution: The dangerous and underrated vulnerability impacting JavaScript applications

@SecurityMB shares his new research on prototype pollution. Most existing examples of exploitation focus on getting RCE in NodeJS. He wanted to find out the client-side impact instead.

The answer, in a nutshell, is that prototype pollution allows you to bypass HTML sanitizers. This is why "if you ever find a prototype pollution in Google Search, then you have XSS in the search field!".

4. Tool of the week

mapCIDR

mapCIDR is a Go library and CLI tool for performing operations on subnet/CIDR ranges. Given a subnet, it can return the list of IP addresses it contains, or slice it into multiple subnets.

This is helpful if you want to do distributed scanning of large networks. Another handy tool by @pdiscoveryio!

5. Webinar of the week

Webcast: Pretty Little Python Secrets – Episode 1 – Installing Python Tools and Libraries the Right Way

This webinar is a gift to any hacker wondering about the best way to install Python, how to manage different versions and avoid a dependency hell, and how to create Python app portables (the equivalent of JARs files in Python).

And if you're thinking "Why don't you just use Docker?", there is an argument for other tools mentioned. @byt3bl33d3r does a great job of answering all these questions.

Other amazing things we stumbled upon this week

Videos

- Hacking postMessage() For Beginners!
- Teaching My Mum to Hack (15,000 subscriber special)
- Interview with Tomi Koski
- JavaScript Enumeration for ethical hackers: methodology and tools
- Guide to Failing at Bug Bounties
- Burp Macro Auto Authentication
- Attack Detect Defend
- Instant Threat Modeling – #06 SMS-based 2-FA

Podcasts

- Security Now: SpiKey – Ransomware Hits Jack Daniel's, Iranian Script-Kiddies, How Ransomware Happens
- Risky Business #596 — DoJ gives Uber breach response one star
- The InfoSec & OSINT Show 22 – Chris Kubecka & Hacking the World with OSINT
- SWN #59 – Zoom Crash, Dharma Ransomware, & Elon Musk's Neuralink
- SWN #60 – Zoom Outages, MITRE Shield Matrix, & 'SourMint' – Wrap Up

Webinars & Webcasts

- Webcast: Pretty Little Python Secrets – Episode 1 – Installing Python Tools and Libraries the Right Way
- Adopting the more effective Penetration Test Model : Assumed Breach & Assumed Breach Penetration Testing Model Deep Dive

Conferences

- HackFest Summit 2020

Tutorials

Medium to advanced

- How to use Surge.sh: The perfect host for XSS payloads
- IDOR through MongoDB Object IDs Prediction & mongo-objectid-predict
- Avoiding detection via DHCP options
- Red Teaming With Cobalt Strike – Not So Obvious Features
- Now you C me, now you don't: An introduction to the hidden attack surface of interpreted languages
- Extending The Value of Security Testing by Adopting Variant Analysis #CodeQL
- Soatok's Guide to Side-Channel Attacks

Beginners corner

- cut: command-line tools #2
- DQL injection
- DuckDuckGo Tips & Tricks

- XSS Attack Vectors in Laravel Blade
- Hakluke's Guide to Nmap — Port Scanning is Just The Beginning
- Hacking GSM: Building a Rogue Base Station to Hack Cellular Devices
- Part 2: Step-by-step iPhone Setup for iOS Research (via @bizzybarney)

Writeups

- Upload to the future

Challenge writeups

- All The Little Things & GoogleCTF – Cross-Site Scripting "Pasteurize"

Pentest writeups

- Forget Your Perimeter: RCE in Pulse Connect Secure (CVE-2020-8218)
- XSS: Arithmetic Operators & Optional Chaining To Bypass Filters & Sanitization
- A Tale of Escaping a Hardened Docker container
- Exploiting CVE-2019–3652 | Owning a networked software repository to PWN endpoints.
- XXE to SSRF to Windows Administrator Hashes
- Unexpected Deserialization Pt.1 – JMS

Responsible(ish) disclosure writeups

- Grafana <= 6.4.3 Arbitrary File Read #Web
- Malicious Apps Could Take Over Samsung Devices #Android
- Technical Advisory – wolfSSL TLS 1.3 Client Man-in-the-Middle Attack (CVE-2020-24613) #Network
- Chasing doorbells: Finding IoT vulnerabilities in embedded devices #IoT
- Windows .Net Core SDK Elevation of Privilege #Windows #PrivEsc
- GOG Galaxy Client Local Privilege Escalation Deuce #Windows #PrivEsc
- hide.me VPN Windows Client Privilege Escalation Vulnerability #Windows #PrivEsc

Bug bounty writeups

- Auth bypass: Leaking Google Cloud service accounts and projects
- My Hacking Adventures With Safari Reader Mode (Apple)

- Issue 795595: Security: chrome.devtools.inspectedWindow.eval executes within privileged pages (Google, $2,000)
- The Confused Mailman: Sending SPF and DMARC passing mail as any Gmail or G Suite customer (Google)
- From Copy&Paste XSS To Full Account Takeover!
- Remote Code Execution in Slack desktop apps + bonus (Slack, $1,750)
- Privilege escalation from any user (including external) to gitlab admin when admin impersonates you (GitLab, $10,000)
- An attacker can run pipeline jobs as arbitrary user (GitLab, $12,000)
- Ability to publish a paid theme without purchasing it. (Shopify, $2,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- gdb_2_root: Python script that adds some useful commands to stripped vmlinux image
- jf: A wrapper around jq, to help you parse jq output
- bbr: An open source tool to aid in command line driven generation of bug bounty reports based on user provided templates
- Wappylyzer: Implementation of Wappalyzer in Python

More tools, if you have time

- Monsoon & AMA: A fast HTTP enumerator that allows you to execute a large number of HTTP requests, filter the responses and display them in real-time
- ADBSploit: A python wrapper around ADB for exploiting and managing Android devices
- AWS Recon: Multi-threaded AWS inventory collection tool with a focus on security-relevant resources and metadata
- Google Account Finder: Website to look for info on Google accounts
- ReconSpider: Advanced OSINT Framework for scanning IP Address, Emails, Websites & Organizations. Also combines the capabilities of Wave, Photon & Recon Dog to do a comprehensive enumeration of attack surface
- slackcat: A simple way of sending messages from the CLI output to your Slack with webhook
- Bheem: A simple collection of small bash-scripts which runs iteratively to carry out day-to-day recon process and store output in an organized way

- Subrake: A Subdomain Enumeration and Validation tool for Bug Bounty and Pentesters
- Phirautee: A proof of concept PowerShell ransomware to use during internal infrastructure penetration testing or during the red team exercise to validate Blue Team/SOC response to ransom attacks
- Ansible-Red-EC2, Red-Route53-Interactive & Intro: Ansible roles for automating red team infrastructure
- PurpleSharp: C# adversary simulation tool that executes adversary techniques with the purpose of generating attack telemetry in monitored Windows environments

Misc. pentest & bug bounty resources

- @ofjaaah's XSS Payloads, KingOfOneLineTips Project @ Telegram channel
- @HusseiN98D AMA
- @k_v0 AMA, @ADITYASHENDE17 & @brutelogic AMA
- mySapAdventures: Quick methodology on testing/hacking SAP Applications
- Immortalising 20 Years of Epic Research
- Certified Red Team Professional Cheat Sheet
- The #AppSec 50: Top application security pros to follow on Twitter
- MITRE Shield #BlueTeam

Challenges

- CSAW'20 – Cybersecurity Games
- OVAA (Oversecured Vulnerable Android App)

Articles

- Prototype pollution – and bypassing client-side HTML sanitizers
- Bugcrowd LevelUp 0x07: How to Do Chrome Extension Code Reviews
- Attacking Azure & Azure AD, Part II
- Powershell Logging: Obfuscation And Some New(Ish) Bypasses Part 1
- The Current State of Exploit Development, Part 1 & Part 2
- Never Run 'python' In Your Downloads Folder & Reddit discussion
- A Guide to Reversing and Evading EDRs: Part 1
- Bypassing Credential Guard

- Exploring the Ubiquiti UniFi Cloud Key Gen2 Plus
- Reverse Engineering a Smart Lock&

News

Bug bounty & Pentest news

- New Intigriti feature: 90-day response statistics
- H1-2010: Sept. 10 – Oct. 20 | Virtual
- Recon.dev now has paid plans & API/SDK documentation
- Launch of the Hackerone Brand Ambassador Program

Reports

- Under the Hoodie 2020 Report
- China's Quest for Cyber Dominance: New Targets, New Tactics, and Information Warfare

Vulnerabilities

- Security researcher discloses Safari bug after Apple delays patch
- Slack fixes 'critical' vulnerability that left desktop app users open to attack
- Bridgefy, the messenger promoted for mass protests, is a privacy disaster
- Embedded security: wolfSSL can be abused to impersonate TLS 1.3 servers and manipulate communications
- Bcrypt hashing library bug leaves Node.js applications open to brute-force attacks
- Slack fixes 'critical' vulnerability that left desktop app users open to attack
- Academics bypass PINs for Visa contactless payments
- Denial-of-Wallet attacks: How to protect against costly exploits targeting serverless setups
- Vulnerability Spotlight: Remote code execution, privilege escalation bugs in Microsoft Azure Sphere

Breaches & Attacks

- Tesla employee foregoes $1M payment, works with FBI to thwart cybersecurity attack
- Report claims a popular iOS SDK is stealing click revenue from other ad networks
- The Kittens Are Back in Town 3
- Report: "No Need to Hack When It's Leaking:" GitHub Leaks of Protected Health Information

- US election 2020: The disinfo operations have evolved, but so have state governments
- Iran-Linked 'Newbie' Hackers Spread Dharma Ransomware Via RDP Ports
- North Korean hackers pwned cryptocurrency sysadmin with GDPR-themed LinkedIn lure, says F-Secure
- FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks (CISA alert)
- DDoS extortionists target NZX, Moneygram, Braintree, and other financial services

Other news

- "Chrome considered harmful" – the Law of Unintended Consequences
- What It's Like for a Hacker to Get Back Online After a Two-Year Internet Ban
- A quarter of the Alexa Top 10K websites are using browser fingerprinting scripts
- The Viking Snowden: Denmark spy chief 'relieved of duty' after whistleblower reveals illegal snooping on citizens
- Office 365 now opens attachments in a sandbox to prevent infections

Non technical

- Finding your first bug: bounty hunting tips from the Burp Suite community
- Hacker Spotlight: Interview With Todayisnew
- Bug Business #10 – Get to know Intigriti content creator PentesterLand
- Algorithmic vs. Faith-based Learning
- Why you shouldn't parse the output of ls(1)
- Why InfoSec Creators Should Move to Direct Support Monetization

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 08/21/2020 to 08/28/2020.