Bug Bytes #97 – Breaking Site Isolation, Untrusted Types, SAD DNS & 31k Google SSRF

BY ANNA HAMMOND · NOVEMBER 18, 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 08 to 15 of November.

Intigriti News

Avalanche of security updates, Zoom snooping & The 2020 business threat landscape

Our favorite 5 hacking items

1. Videos of the week

The Act of Balancing: Burnout in Cybersecurity with Chloé Messdaghi!
10 GREAT habits for bug bounty hunters (and a productive life)

A lot of us bug hunters and pentesters have to deal with burnout. So, make sure to watch these two videos that are full of ideas to not only avoid it, but also to gain in productivity and general well-being. Fantastic tips by @ChloeMessdaghi and stokfredrik!

2. Writeups of the week

Smuggling an (Un)exploitable XSS
31k$ SSRF in Google Cloud Monitoring led to metadata exposure (Google, $31,337)
From SVG and back, yet another mutation XSS via namespace confusion for DOMPurify < 2.2.2 bypass

@david_nechuta goes over a blind SSRF in Google that was tricky to exploit. @MrTuxracer shows how he chained an uninteresting request smuggling vulnerability with a hard to exploit header-based XSS to escalate their impact. @bananabr's writeup details how he used LiveDOM++ to find a new DOMPurify bypass.

These are all great findings and highly recommended to read!

3. Tool of the week

Untrusted Types

Untrusted Types is a Chrome extension by @filedescriptor that abuses Trusted Types to log DOM XSS sinks. It is handy for tracing sink to source and source to sink when testing for DOMS XSS, and also for finding script gadgets to bypass the CSP.

4. Vulnerability of the week

SAD DNS & SAD DNS Explained

SAD DNS stands for "**S**ide-channel **A**ttacke**D DNS**" and is not just another vulnerability that get its own name and site. It bypasses mitigations for DNS Cache Poisoning attacks, and makes it possible again to poison DNS resolvers and forwarders using ICMP as a side-channel.

DNS providers are working on fixing it as it effectively breaks DNS. Anyone could exploit it to re-route traffic to their own servers. A fascinating dive into DNS security!

5. Tutorial of the week

Deep Dive into Site Isolation (Part 1)

This blog post explains how Site Isolation works in Chrome and mitigates attacks like Universal XSS and Spectre. Jun Kokatsu (@shhnjk) studied it and found 10+ bugs in the Chrome bug bounty program! An excellent read if you're into browser security, UXSS, or CORS / CORB testing.

Other amazing things we stumbled upon this week

Videos

- @John Hammond Talks About CTF vs Bug Bounty, Organizing CTS, CTF tools, Certificates, and more!
- @zseano Talks About bugbountyhunter.com, Recon, Reading Javascript, Getting Started in Bug Bounty
- How do i even get started doing Bug Bounty
- Prototype Pollution Attack Explained
- Hacking Skills Perspective

- Creating Sock Puppet Accounts
- Advice on Starting a Successful Business
- iOS Pentesting

Podcasts

- Security Now: NAT Firewall Bypass – SlipStream NAT Firewall Bypass, MS Police Use Ring Doorbell Cams
- Darknet Diaries EP 78: NERDCORE
- Risky Business #604 — Election-related cyber shenanigans fail to materialise
- CTF Radiooo: Education and CTFs with Fabian aka LiveOverflow
- Tianfu, Ghimob, Scalper Bots, Animal Jam, & Pay2Key – Wrap Up – SWN #82
- 'Platypus' Attack, IDOR DOD Bug, & 2 More Chrome 0-Days – ASW #130

Webinars & Webcasts

- The Secret Thoughts of a Successful Hacker | Nadean Tanner | 1 Hour
- 2020 Collegiate SECTF KeyNote: Chris Hadnagy, Webinar: How To OSINT by Chris Krisch & Webinar: Social Engineering Ask Me Anything
- File upload vulnerabilities & Slides/challenges (in Arabic)
- Kubernetes Security Workshop & Red Team KubeCTL Cheat Sheet

Conferences

- Visma Security Conference
- DEF Con 401 – Steve Campbell – The 10 (Unexpected) Ways I Pwned You!
- Unlock Your Brain Harden Your System 2020 (in French)

Tutorials

Medium to advanced

- Advanced MSSQL Injection Tricks
- XPath SQL Injection in OpenEMR
- Announcing PSReadLine 2.1+ with Predictive IntelliSense
- Customizing C2-Frameworks for AV-Evasion

Beginners corner

- A Pentester's Guide to Cross-Site Request Forgery (CSRF)
- Attacking JSON Web Tokens (JWTs)
- Common Nginx misconfigurations that leave your web server open to attack & Vulnerable-nginx
- Cobalt Strike: Red Team's Best Friend

Writeups

Challenge writeups

- Bypassing SQL Filters (picoCTF Web Gauntlet) (video)
- CloudGoat ECS_EFS_Attack Walkthrough

Pentest writeups

- Unique XXE to AWS Keys journey
- Bypassing Naxsi Filtering Engine

Responsible(ish) disclosure writeups

- How to get root on Ubuntu 20.04 by pretending nobody's /home #Linux #LPE
- Extraordinary Vulnerabilities Discovered in TCL Android TVs, Now World's 3rd Largest TV Manufacturer. #SmartTV #Android
- Apache OpenOffice RCE (CVE-2020-13958) #Web
- Silver Peak Unity Orchestrator RCE & SD-PWN Part 2 — Citrix SD-WAN Center — Another Network Takeover #Web #RCE
- A code signing bypass for the VW Polo #IoT #CarHacking
- TP-Link Takeover with a Flash Drive #Router #USB
- Intel, Please Stop Assisting Me #Windows #LPE

Bug bounty writeups

- Firefox for Android: LAN-Based Intent Triggering (Microsoft)
- How I Found The Facebook Messenger Leaking Access Token Of Million Users (Facebook, $16,125)
- Evernote: Universal-XSS, theft of all cookies from all sites, and more (Evernote)
- Optimizing Hunting Results in VDP for use in Bug Bounty Programs – From Sensitive Information Disclosure to Accessing Hidden APIs which can be used to Retrieve Customer Data ($4,750)

- Ticket Trick at https://account.acronis.com (Acronis, $750)
- Possibility to freeze/crash the host system of all Slack Desktop users easily (Slack, $500)
- Uninstalling Slack for Windows (64-bit), then reinstalling keeps you logged in without authentication (Slack, $500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- AWS User Data Secrets Finder: Search for secrets inside user data attached to EC2 instances on multiple AWS accounts
- CORS misconfiguration POC Builder
- SendPass: Securely* send passwords, URLs or other text data from any trusted computer with a camera (Phone, Laptop, Web Cam, etc.) to an un-trusted computer with ease

More tools, if you have time

- 4xxbypass: A tool that automates a number of well-known 403/401 bypassing techniques
- Asthook: Python tool for Android static and dynamic analysis
- 3klCon: Automation recon tool which works with large & medium scopes
- anewer: A rust version of TomNomNom's anew. It appends lines from stdin to a file if they don't already exist in the file
- xpcspy: Bidirectional XPC message interception and more. Powered by Frida
- Dredd: HTTP API Testing Framework. It's a language-agnostic command-line tool for validating API description document against backend implementation of the API.
- enum4linux-ng: A next generation version of enum4linux (a Windows/Samba enumeration tool) with additional features like JSON/YAML export. Aimed for security professionals and CTF players
- Apollo: A .NET Framework 4.0 Windows Agent
- PYTMIPE & TMIPE: Python library and client for token manipulations and impersonations for privilege escalation on Windows

Misc. pentest & bug bounty resources

- Remedy Cloud
- Low-cost fuzzer, using /dev/urandom and the Piper extension
- OpenID Connect in Detail

- Infosec Bugbounty AMA with JR0ch17 & BenkoOfficial
- Security Workbook on Application Security
- Bug Bounty Playbook 2: Exploitation ($25)

Challenges

- Damn-Vulnerable-Bank

Articles

- Duping AV with handles
- Exploring the Exploitability of "Bad Neighbor": The Recent ICMPv6 Vulnerability (CVE-2020-16898)
- On the Effectiveness of Time Travel to Inject COVID-19 Alerts

Bug bounty & Pentest news

- Burp Suite Release: Professional / Community 2020.11
- Announcing New Leaderboards: More Ways To Engage, Compete And Win

Non technical

- Hacker Spotlight: Interview With Fisher
- Your Computer Isn't Yours
- What it takes to find bugs in bounties!
- Cybercrime isn't the exciting career it's cracked up to be, say academics
- Past, Present and Future of Effective C
- Lessons on Burnout: How to Protect Yourself & Your Team
- Persevere: Trust your Struggle

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 11/08/2020 to 11/15/2020.