Bug Bytes #81 – The new browser security ecosystem, MS Exchange attacks & HTML sanitization bypass

BY ANNA HAMMOND · JULY 29, 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 17 to 24 of July.

Our favorite 5 hacking items

1. Videos of the week

CDL Talks About Hacking, Bug Bounties, Recon, Gau (getallurls), Reversing CVEs, and more!

Beginners Guide to iOS Testing Jailbreak, SSL Bypass & Burp

The first video is a cool interview with Corben Leo (@hacker_). @NahamSec and him talk about all things bug bounty, tooling, recon, methodology, burnout... As always, it is interesting to hear about a fellow bug hunter's story and insights.

The second video is a cool demo by @InsiderPhD on setting up an environment for iOS testing.

2. Writeup of the week

HTML sanitization bypass in Ruby Sanitize < 5.2.1

WAF and HTML sanitizer bypasses can seem like black magic for anyone who does not understand how they work and only sees the final payload. So, this is a great learning opportunity.

@SecurityMB explains how Ruby Sanitize works and, step by step, how he built a bypass that introduced XSS.

3. Article of the week

Attacking MS Exchange Web Interfaces

This is an excellent article on attacking Exchange in the context of pentest / red team engagements. It goes over 5 known techniques that still work in 2020, with their pros and cons. Then it introduces a new technique and a new tool to connect to LDAP via MS Exchange from the Internet and access the Active Directory database.

4. News of the week

Towards native security defenses for the web ecosystem

This is an interesting read if you're into Web app security. It is about the latest security mechanisms being implemented in Chrome and Firefox (e.g. COOP, Fetch Metadata headers, CSP, Trusted Types...).

It is essential to get familiar with these concepts as they have an impact on vulnerabilities like XSS, CSRF, XS-leaks, etc.

5. Tool of the week

hack-pet & Intro

Hack-pet is a collection of snippets for bug hunters, to use with the command-line snippet manager pet.

It allows you to quickly search for and run tools like amass, adb, dirseach, subfinder... without the need to remember their syntax.

Other amazing things we stumbled upon this week

Videos

- Bypassing SAML Authentication for Beginners!
- Hunting for Javascript! (bug bounty, scripthunter, jsmon, getjswords, urltracker, wfuzz and more)
- HTTP Referer Leak
- Hack Club AMA: Tommy DeVoss
- Hacker101 Pentest Series
- F5 Vulnerability Burndown w/@sml555_ and @caseyjohnellis
- The JerichShow Episode 12 – A Tweetworthy Week
- TheBigBountyTube- My $15,000 Bug Bounty Microsoft Windows Insider Preview | How to Get Started
- API Penetration Test + Burp + Postman
- Introduction To Pentesting – Enumeration & Password Cracking

Podcasts

- Security Now – A Tale of Two Counterfeits – Twitter Hack, Cloudflare Outage, Zoom's Vanity URL Flaw
- Darknet Diaries EP 70: Ghost Exodus

- The InfoSec & OSINT Show 17 – Matthias Wilson & Using OSINT Against Nigerian Scammers
- 7MS #424: Cyber News – Everything is Pwned Edition
- SWN #52 – Wrap Up – Emotet Returns, BadPower Attacks, & Twitter Hack Follow Up

Webinars & Webcasts

- SSD Lil' Bytes – Jay Turla – Dirty CAN Bus Hacking: I CAN Fuzz my Car and Junks
- SANS@MIC -Get Involved! Use Your OSINT Powers for Good!

Conferences

- WWHF 2020 – Virtual Talks, especially:
  - Web Hacking: Beyond Alert ('XSS Found')
- Rooted CON 2020 – ENG

Tutorials

Medium to advanced

- Fastjson: exceptional deserialization vulnerabilities & FastJSON deserialization bug can trigger RCE in popular Java library
- PostMessage Vulnerabilities. Part II
- Container Breakouts – Part 1: Access to root directory of the Host
- Making the Perfect Red Team Dropbox (Part 2)
- Process Injection using DInvoke
- Alternative Execution: A Macro Saga (part 4)

Beginners corner

- Subdomain Takeover using readthedocs
- Exploiting Local File Inclusion (LFI) Using PHP Wrapper
- Secure Code Review Best Practices
- A Brief Look At 2 IdaaS Attack Paths
- Raspberry Pi as a Penetration Testing Implant (Dropbox)
- Performing port-proxying and port-forwarding on Windows

Writeups

Challenge writeups

- Lua SUID Shells
- InjuredAndroid CTF Writeup

Pentest writeups

- How I hacked into a Telecom Network
- Resetting Passwords – What Could Possibly Go Wrong?
- Denial of Service(DoS) By Regex

Responsible(ish) disclosure writeups

- Multiple vulnerabilities found in CDATA OLTs
- Shadow Attacks: Hiding and Replacing Content in Signed PDFs #PDF
- Adventures in Citrix security research #Web
- Raining SYSTEM Shells with Citrix Workspace app #RCE
- Why keep your Zoo doors closed #RCE
- SSD Advisory – Roundcube Incoming Emails Stored XSS #Web #CodeReview
- Kubernetes CVE-2020-8559 Proof of Concept PoC Exploit #PrivEsc #Kubernetes
- Advisory – web browser address bar spoofing #Browser #Web

Bug bounty writeups

- Hunting Android Application Bugs Using Android Studio. ($3,000)
- Unique Case for Price Manipulation | BugBounty | VAPT
- Creative Android pin bypass with Race conditon
- SAML Response Reuse on hackerone.com/users/saml/auth (HackerOne, $500)
- Denial of Service [Chrome] (Twitter, $560)
- Near to Infinite loop when changing Group's name that has API token as Team Member (HackerOne, $2,500)
- Business Logic Flaw – A non premium user can change/update retailers to get cashback on all the retailers associated with Curve (Curve, $1,000)
- Java Debug Console Provides Command Injection Without Privellage Esclation

- Ability to link a Google account to another staff account/store owner that isn't linked yet (Shopify, $2,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- ponieproxy: Simple proxy which captures all requests and responses and saves them in uniquely named files
- faviconer.go: Go script for grabbing favicon hashes (like Shodan does)
- SourceWolf: Amazingly fast response crawler to find juicy stuff in the source code
- CodeArgos: A python module for red teams to support the continuous recon of JavaScript files and HTML script blocks in an active web application
- Oralyzer: Open Redirection Analyzer
- Boomerang: A tool to expose multiple internal servers to web/cloud
- E4Enumerat10n: Python script that uses intelx.io to gather emails associated with any domain name
- PCWT: A app app with GUI for managing pentest/bug bounty projects and running port scans & subdomain enumeration tools
- Pollenisator: Collaborative pentest tool with highly customizable tools
- Rootend: A *nix Enumerator & Auto Privilege Escalation tool
- calebstewart/pwncat: Fancy reverse and bind shell handler
- dazzleUP: A tool that detects the privilege escalation vulnerabilities caused by misconfigurations and missing updates in the Windows operating systems

Misc. pentest & bug bounty resources

- Collab with dawgyg Slack channel
- Local PentestLab Management Script
- Bug Bounty Tips #3, #2 & #1
- wintrmvte/Citadel: Small collection of pentesting scripts
- Kerberos attack cheatsheet
- NSA on Securing VPNs

Challenges

- OOO archive | DEF CON CTF
- HHarder XSS Challenge by @terjanq

Articles

- Proxying Exfil Data Through Images
- SharePoint and Pwn :: Remote Code Execution Against SharePoint Server Abusing DataSet (CVE-2020-1147)
- Bug Bounty Failsx101[3]
- Let's Talk About TikTok
- My worst nightmare on discovering a Wi-Fi WPS vulnerability on my home router

News

Bug bounty & Pentest news

- What's new in Ffuf v1.1.0
- Google CTF Sponsorship 2020
- Apple Will Start Sending Special Devices to iPhone Hackers & Google's Project Zero team won't be applying for Apple's SRD program
- h@cktivitycon: July 31 – August 1
- HTTP/2 support in Burp
- Most hilarious xss vector

Reports

- Cybersecurity Perception vs Reality
- Rapid7's National / Industry / Cloud Exposure Report (NICER) 2020
- Dark Web Price Index 2020
- Shocked I am. Shocked to find that underground bank-card-trading forums are full of liars, cheats, small-time grifters

Vulnerabilities

- CVE-2020-3452 Cisco ASA / Firepower Read-Only Path Traversal Vulnerability: What You Need to Know & PoC

- Hide and replace: ‘Shadow Attacks’ can manipulate contents of signed PDF docs
- BadPower attack corrupts fast chargers to melt or set your device on fire
- Windows 10 Store ‘wsreset’ tool lets attackers bypass antivirus
- Django two-factor authentication plugin stored passwords in plain text
- Unpatched Tenda WiFi router vulnerabilities leave home networks wide open to abuse
- Academics smuggle 234 policy-violating skills on the Alexa Skills Store
- TrojanNet – a simple yet effective attack on machine learning models
- 5 severe D-Link router vulnerabilities disclosed, patch now
- GitHub security team finds remote code execution bug in popular Node.js changelog library
- App for Chinese DJI drones could give hackers full control of users’ phones, researchers say

Breaches & Attacks

- Ongoing Meow attack has nuked >1,000 databases without telling anyone why
- Slack credentials abundant on cybercrime markets, but little interest from hackers
- Twilio: Someone waltzed into our unsecured AWS S3 silo, added dodgy code to our JavaScript SDK for customers
- Bad: US govt says Chinese duo hacked, stole blueprints from just about everyone. Also bad: They extorted cash
- Mac cryptocurrency trading application rebranded, bundled with malware
- New BlackRock Android malware can steal passwords and card data from 337 apps
- Prometei botnet exploits Windows SMB to mine for cryptocurrency

Other news

- A vigilante is sabotaging the Emotet botnet by replacing malware payloads with GIFs
- Who is behind APT29? What we know about this nation-state cybercrime group
- UK.gov admits it has not performed legally required data protection checks for COVID-19 tracing system
- Magento adds 2FA to protect against card skimming attacks
- The Anatomy of a Cisco Counterfeit Shows Its Dangerous Potential

Non technical

- Can Docker containers replace VMs for bug bounty hunters and penetration testers?

- What Do Bug Bounty Platforms Store About Their Hackers?
- The Bug Bounty Mindset That Leads To Success
- Hacker Spotlight: Interview with hogarth45
- How to Create an Internal/Corporate Red Team
- The Human Obsession With Rarity
- Healthy Self-Doubt
- The Polymath Playbook
- Building the Ultimate Home Office (Again)
- A Socratic Outline for Discussing the OST Release Debate

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 07/17/2020 to 07/24/2020.