Bug Bytes #93 – Discord RCE, Vulnerable HTML to PDF converters & DOMPurify bypass demystified

BY ANNA HAMMOND · OCTOBER 21, 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 11 to 18 of October.

Intigriti News

Security Snacks #2 – The Godzilla of bugs, The OST debate & The bug bounty of the year

Our favorite 5 hacking items

1. Article of the week

HTML to PDF converters, can I hack them?

Eduardo Muller evaluated a set of libraries that convert HTML code to PDF. He experimented with them to answer a series of questions and determine which ones are vulnerable to XSS, SSRF, Arbitrary file read or Denial of Service. If you're looking for ways to differentiate yourself as a bug hunter, this type of research is particularly interesting.

2. Writeups of the week

Discord Desktop app RCE (Discord, $5,000)
Showcasing the Importance of Secure Defaults with a PyYAML 0day

The firt writeup is a chain of three bugs that led to RCE in Discord: Missing contextIsolation, XSS and Navigation restriction bypass. Great findings and writeup especially for anyone interested in Electron

apps security.

The second writeup is an RCE in the PyYAML library. Applications that use this library to process untrusted input are vulnerable if they use load() instead of safe_load(). Ankur Sundara (@ankursundara) shows why secure defaults are important, as he convinces PyYAML to move to safe_load() as the default.

3. Video of the week

DOMPurify bypass via namespace confusion

This is a setp-by-step walkthrough of Michał Bentkowski's (@SecurityMB) mutation XSS / DOMPurify bypass. It helps demystify WAF bypasses that look like incomprehensible dark magic. So, highly recommended!

4. Tools of the week

TheCl0n3r
PPScan

TheCl0n3r is a Python tool for downloading and managing your git repositories. It allows you to download/delete/update repos and keep them organised. This is so handy considering that most open source tools for pentest and bug bounty are hosted on GitHub.

PPScan is a Prototype Pollution scanner. If you install it as a Chrome extension, it will passively detect vulnerable instances. It is interesting to try since Prototype Pollution is so prevalent these days.

5. Webinars of the week

Hacking Android Apps with Frida
Mobile Hacking Workshop – Community Day & Material

These webinars are an excellent start to get into practical mobile app hacking. Between the two, you'll learn about using Frida with bug bounty examples, and a series of vulnerabilities to look for by practicing on the intentionally vulnerable app InjuredAndroid. Excellent work by Richard Tan (@Sambal0x) and Kyle (@B3nac)!

Other amazing things we stumbled upon this week

Videos

- Finding Bugs in Mobile APIs
- New content discovery tools for FASTER recon (Pentesting webapps)
- The Ugly Truth about Bug Bounty Hunting
- @Insidephd Talks About Bug Bounties, HackerOne's Live Hacking Events & Creating Content for Hackers!

- Guessing vs. Not Knowing in Hacking and CTFs
- SQL Injection Prevention: Security Simplified

Podcasts

- Security Now: Well Known URI's – Carnival Cruise Hack, ZeroLogon, Five Eyes vs Encryption
- Risky Business #601 — Everyone's messing with TrickBot
- Darknet Diaries EP 76: KNAVES OUT

Webinars & Webcasts

- OWASP Chandigarh | October 2020 ONLINE MEETUP
- Infosec Mentoring | How to Find and Be a Mentor & Mentee
- ClueCon Weekly with Sandro Gauci, demonstration of SIP Digest Leak

Slides & Workshop material

- iOS Application Security

Tutorials

Medium to advanced

- Amass, go deep in the sea with free APIs
- Typical Wi-Fi attacks
- Who Needs NTDS.DIT for password hashes?
- Beware the Bad Neighbor: Analysis and PoC of the Windows IPv6 Router Advertisement Vulnerability (CVE-2020-16898) & CVE-2020-16898 – Exploiting "Bad Neighbor" vulnerability

Beginners corner

- A Pentester's Guide to HTTP Request Smuggling
- Hacking HTTP CORS from inside out: a theory to practice approach & hacking-cors lab
- Modifying React Native APK
- Recon using a questionable source of information — pastebin.com
- Where is Leonardo's Car – Using OSINT to trace vehicles
- OSINT & OPSEC: Short URLs

Writeups

Challenge writeups

- Extract, Research, Verify: Quiztime 6th October 2020. #OSINT

Pentest writeups

- Covert Web Shells in .NET with Read-Only Web Paths
- 403 to RCE in XAMPP

Responsible(ish) disclosure writeups

- Fortinet SIEM vulnerability allows us to get RCE on internet exposed hosts #RCE #Web
- WarezTheRemote: Turning Remotes Into Listening Devices #IoT
- Crouching T2, Hidden Danger #Apple
- SICK-2020-004 – Hindotech HK1 TV Box – Root Privilege Escalation – Improper Access Control #SmartTV #IoT #EoP
- CVE-2020-15157 "ContainerDrip" Write-up #Container
- LoRaWAN & MQTT: What to Know When Securing Your IoT Network #IoT
- Java deserialization vulnerability in QRadar RemoteJavaScript Servlet #Web
- Major Vulnerabilities Discovered in Qualcomm QCMAP #RCE
- Abusing Predefined Cookies to Account Takeover in FlowCrypt #Web

Bug bounty writeups

- GitHub – RCE via git option injection (almost) – $20,000 Bounty (GitHub, $20,000)
- GitHub Gist – Account takeover via open redirect – $10,000 Bounty (GitHub, $10,000)
- Leveraging XSS to Read Internal Files
- I had fun with this XSS
- [toolbox.teslamotors.com] HTML Injection via Prototype Pollution / Potential XSS
- Guest Blog Post: Rollback Attack (Mozilla)
- Weaponizing XSS For Fun & Profit ($2,200)
- Change the username for any Facebook Page (Facebook, $15,000)
- Getting New Invitations without Leaving Programs (HackerOne, $500)

See more writeups on The list of bug bounty writeups.

Tools

- amass-tools: @ITSecurityguard's scripts to extend Amass
- APICheck: The DevSecOps toolset for HTTP APIs. Environment for integrating existing HTTP APIs tools and create execution chains easily
- pdf-grep: Grep through PDF files
- host.io: A Comprehensive Domain Data API
- Burp Multiplayer: A Multiplayer Plugin for Burp. Sync's in-scope requests/responses, comments, and highlights in realtime.
- Mail-Swipe: Script to create temporary email addresses and receive emails, using the 1secmail API
- Driplane: Create an automatic alerting system or start automated tasks triggered by events. It allows you to keep under control a stream source as Twitter, a file, a RSS feed or a website

Misc. pentest & bug bounty resources

- wordpress-plugin-list: WordPress Plugins List for Bruteforcing
- LeakIX
- THC's favourite Tips, Tricks & Hacks (Cheat Sheet)
- 0xffsec Handbook – The Pentester's Guide

Challenges

- DamnVulnerableCryptoApp

Articles

- Recipe for a successful phishing campaign (part 1/2) & Part 2/2
- Running JXA Payloads from macOS Office Macros
- Don't Copy Paste Into A Shell
- Code execution via the Windows Update client (wuauclt)
- Red Team Tactics: Hiding Windows Services
- Exploring the WDAC Microsoft Recommended Block Rules: VisualUiaVerifyNative

Non technical

- Hacker Spotlight: Interview With Inhibitor181
- Infosec Bugbounty AMA with Michele Romano

- How to trick your brain into learning something new, faster & more effectively
- The Call for Applied Research on Offensive Security Tool Release

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 10/11/2020 to 10/18/2020.