Bug Bytes #107 – Go for HTTP smuggling, Open source frameworks vs Cache poisoning & Practicing RCE in NodeJS apps

BY ANNA HAMMOND · JANUARY 27, 2021 · 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 18 to 25 of January.

Intigriti News

January XSS Challenge

A slew of Cisco bugs, Risks of DoH & DNSpooq (aka new proof that it's always DNS!)

Our favorite 5 hacking items

1. Videos of the week

Insecure Deserialization Attack Explained
Live Recon on Snapchat with @ITSecurityGuard (amass, FFUF, SecurityTrails Demo)

@PwnFunction is back with an awesome video tutorial on deserialization. It is concise and maybe the best explanation I've seen on this rather complex vulnerability class.

The other video is the first of a new series by @NahamSec where he hacks live with a fellow bug hunter (@ITSecurityGuard this time). This is a fantastic idea, like a practical interview or walkthrough to see how other hackers work.

2. Writeup of the week

The Secret Parameter, LFR, and Potential RCE in NodeJS Apps

This is an informative writeup by @0xCaptainFreak on Local File Read in NodeJS apps, when ExpressJS is used with hbs (view engine for Handlebars). Without spoiling it more, can you find the issue in this code that reproduces the bug?

3. Article of the week

Cache poisoning in popular open source packages

@snyksec dived into Web cache poisoning in open source packages and found several well known frameworks vulnerable. For example, Botlle, Tornado and Rack all use "parse_qsl" an insecure method in Python's source code that makes them vulnerable to cache poisoning attacks.

4. Tip of the week

Another way to do HTTP smuggling

@BitK_ shared a new HTTP smuggling technique that @albinowax interprets as "Golang's network stack attempting to "parse HTTP headers as ~UTF-8 even though everyone else treats them as ASCII". It is yet to be confirmed but looks like a very interesting area to explore.

5. Tool of the week

BurpSuiteSharpener

New week, new Burp customizer extension! This one from @irsdl adds cool features like the ability to change Burp's title and icon, to change the style of tabs and use pretty Gradient icons.

Other amazing things we stumbled upon this week

Videos

- Discovering Cloud Assets Externally, with CloudEnum
- Intro to CSRF (Cross-Site Request Forgery) – Security Simplified
- $15,000 Playstation Now RCE via insecure WebSocket connection – Bug Bounty Reports Explained

Podcasts

- DAY[0] Episode 61 – Snooping YouTube History and Breaking State Machines
- Security Now: Comparative Smartphone Security – Browser Password Managers, Adobe Flash Repercussions, SolarWinds
- Risky Business #612 — DPRK slides into researcher DMs

Webinars & Webcasts

- Bash and Recon & Slides
- ZAP Deep Dive: Active Scanning
- Jailbreaking iOS for Mobile Security Assessments – SANS@Mic
- Webcast: Move Aside Script Kiddies – Malware Execution in the Age of Advanced Defenses

Conferences

- How Variant Analysis helped secure the fight against COVID-19
- Security Talks by Harsh & Slides

Tutorials

Medium to advanced

- Bad Pods: Kubernetes Pod Privilege Escalation
- Hijacking connections without injections: a ShadowMoving approach to the art of pivoting
- The Anatomy of Deserialization Attacks

Beginners corner

- Everything You Need to Know About Web Socket Pentesting

- A @TomNomNom Recon Tools Primer
- Using Github Action for recon
- White Box Web Application Pentesting
- Android Pentest: Deep Link Exploitation

Writeups

Challenge writeups

- XSS: Bypassing CSP is Nonce-nse thanks to bugpoc.com cards challenge (video) & Unintended solution
- Can you find the open redirect?

Responsible(ish) disclosure writeups

- Unauthenticated XSS to Remote Code Execution Chain in Mautic < 3.2.4 #Web
- Security Advisory: MSRPC Printer Spooler Relay (CVE-2021-1678) #NTLM #Network
- Microsoft Teams and Skype Logging Privacy Issue #DesktopApp
- CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit) #Linux
- The State of State Machines #WebRTC
- DNSpooq – Kaminsky attack is back! #DNS
- CVE-2020-5144 – SonicWall Global VPN New Elevation of Privileges Vulnerability #LPE #Windows

Bug bounty writeups

- $10,000 for automatic email confirmation bug in Microsoft's Edge browser (Microsoft, $10,000)
- KindleDrip — From Your Kindle's Email Address to Using Your Credit Card (Amazon, $18,000)
- Chaining a self XSS to Account Takeover
- Let's know How I have explored the buried secrets in React Native application
- BitLocker Lockscreen bypass (Microsoft)
- ShazLocate! Abusing CVE-2019-8791 & CVE-2019-8792 (Apple, Google)
- Possible RCE through Windows Custom Protocol on Windows client (NordVPN, $500)

See more writeups on The list of bug bounty writeups.

Tools

- EIP Fishing: Go fish on AWS EIPs
- jwtXploiter: A tool to test security of json web token
- SpooNMAP & Intro: Python wrapper for NMAP and Masscan
- SAP_EEM_CVE-2020-6207: PoC for CVE-2020-6207 (Missing Authentication Check in SAP Solution Manager)

Tips

- Another way to do HTTP smuggling by @BitK
- @hunter0x7's $10,000 bounty: Exposed API key generation endpoint
- @secalert's preferred password for testing password fields
- Mutation points in \<a\> tags for WAF bypass
- Post-exploitation tip by @s0md3v

Misc. pentest & bug bounty resources

- Executable XSS cheat sheets for popular web frameworks #CodeReview
- OAuth 2.0 Authorization Server Issuer Identifier in Authorization Response
- The ultimate Github dorks list V3
- 0xn3va.gitbook.io cheat-sheets
- Awesome Bug Bounty Tools
- Burp Suite Cheat Sheet v1.0

Challenges

- Intigriti's January XSS Challenge
- @naglinagli's recon challenge
- Leading Cyber Ladies CTF

Articles

- VisualDoor: SonicWall SSL-VPN Exploit
- How to bypass the Cloudflare WAF using a padding technique
- Custom Static Analysis Rules Showdown: Brakeman vs. Semgrep #CodeReview

- MSSQL Lateral Movement & Squeak
- Credentials hiding in plain sight or how I pwned your http auth & httpcreds

Bug bounty & Pentest news

- Votes open for the Top 10 web hacking techniques of 2020
- Burp Suite roadmap for 2021

Non technical

- Offensive Anomaly Detection
- Hacker Spotlight: Interview With Filedescriptor
- OWASP Top-10 2021. Statistics-based proposal.

Community pick of the week

Nice beanie there @xsstnv!

We love hearing from you and celebrating your wins. Tag us if you also want to share your swag and bug hunting joys with other Bug Bytes readers.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com