Bug Bytes #112 – JSON parsers inconsistencies, Fuzzing for SSRF & Microsoft $50k account takeover

BY ANNA HAMMOND · MARCH 3, 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 February 22 to March 1.

Intigriti News

How to get hacked with Nginx or VMWare vCenter & A look at 2020's Top 10 Web hacking techniques

Our favorite 5 hacking items

1. Article of the week

An Exploration of JSON Interoperability Vulnerabilities & Labs

@theBumbleSec dropped excellent research on JSON parsing inconsistencies that can lead to serious business logic vulnerabilities. This is gold for bug hunters, a highly recommended read!

2. Writeups of the week

SSRF: Bypassing hostname restrictions with fuzzing
How I Might Have Hacked Any Microsoft Account (Microsoft, $50,000)
Unauthorized RCE in VMware vCenter & CVE-2021-21972 checker for Nmap NSE

What amazing findings!

@dee__see found inconsistencies in two NodeJS URL parsers that led to SSRF. The attack was discovered by fuzzing with radamsa and leverages parser differentials (parsers again). Though the impact was low, the techniques used are so interesting!

@ptswarm disclosed an unauthenticated RCE in VMware vCenter that's probably keeping some bug hunters busy.

@laxmanmuthiyah found an account takeover on Microsoft's Forgot password page. It involves decrypting a security code, bruteforcing it and leveraging a race condition to bypass anti-bruteforce protections.

3. Conference of the week

Black Hat USA 2020

Black Hat USA 2020 videos were just released and there is no less than 91! There's a lot to watch on all kinds of hacking topics. To easily navigate this, check the briefings for descriptions of each talk and links to slides.

4. Tutorials of the week

How to Break Your JAR in 2021 – Decompilation Guide for JARs and APKs
DOM XSS is Dead*, Long Live DOM XSS

Don't worry, DOM XSS isn't really dead! @InfoSecP4nda did some research on DOM XSS automation with Burp and shares the results. It's interesting to know the limits of Burp when testing for these vulnerabiilities.

The second tutorial is about decompiling JARs and APKs using including different decompilation approaches and tools. If like me you've only heard of JD-GUI and jadx, I highly recommend reading this. Next time these two tools fail to decompile obfuscated code for instance, you'll know of other decompilation options!

5. Video of the week

SQL Injection | Complete Guide

This is a nice introduction to SQL injection by @ rana__khalil. A great resource if you're interested in the topic and prefer videos for learning.

Other amazing things we stumbled upon this week

Videos

- How I Found My First Bug (and earned $1k!) – Business Logic Tips
- JavaScript Is A Goldmine For Bug Bounty Hunters & How To Test For Reflected XSS
- SQL Injection | Complete Guide

- Commonly Misunderstood Bugs: Authorization Based Vulnerabilities
- Bounty Thursdays #26 Bug Bounty Recon Automation FTW!
- Shopify Account Takeover $22,500 Bug Bounty
- Abusing unicode characters to PWN Intigriti XSS challenge [I WON!]
- MyLittleAdmin PreAuth RCE Vulnerability Analysis – Deep Dive – Exploitation

Podcasts

- CNAME Collusion – Seven Exchange 0-Days, Firefox Enhanced Tracking Protection, SolarWinds Password
- Darknet Diaries Ep 86: The LinkedIn Incident

Webinars & Webcasts

- null Ahmedabad Meet 28 February 2021 Monthly Meet: Automating reflected XSS using GXSS
- Android Hacking Workshop by @B3nac Sec

Conferences

- Enigma 2021
- NDSS 2021

Tutorials

- Downloading and Exploring AWS EBS Snapshots
- Got Cookies? Exploring Cookie Based Authentication Vulnerabilities in the Wild
- Graphql Exploitation – Part 1- Understanding Graphql & Enumeration Of Graphql Schema
- Intro to Bug Bounty Automation (pt.2): Port Scanning with Slack & slackexec.py

Writeups

Pentest writeups

- SSRF to RCE with Jolokia and MBeans
- Red Team Stories: The Gordian Lock
- Who Let the ARPs Out? – From ARP Spoof to Domain Compromise

Responsible(ish) disclosure writeups

- ServiceNow – HelpTheHelpDesk And The Hackers #Web
- WP GDPR Compliance <= 1.5.5 – Unauthenticated Cross-Site Scripting (XSS) #Web #CodeReview

Bug bounty writeups

- Build Pipeline Security (Amazon)
- SSRF to fetch AWS credentials with full access to multiple services
- Config override using non-validated query parameter allows at least reflected XSS by injecting configuration into state (Grammarly, $3,000)
- Big Bugs: Bitbucket Pipelines Kata Containers Build Container Escape
- config files with vpn pre-shared-key and other credentials in them (Tesla, $10,000)
- Jira Auth Bypass bug in Google Acquisition (Apigee)
- DNS Setup allows sending mail on behalf of other customers (Basecamp, $700)

See more writeups on The list of bug bounty writeups.

Tools

- 4-ZERO-3: 403/401 Bypass Methods
- pyndiff: Generate human-readable ndiff output when comparing 2 Nmap XML scan files
- posta: Cross-document Messaging security research tool
- 1u.ms: DNS utilities in Go to detect and exploit of SSRF & DNS Rebinding (existed as an online utility and was just open sourced)
- Endgame: AWS Pentesting tool that lets you use one-liner commands to backdoor an AWS account's resources with a rogue AWS account

Tips & Tweets

- How to enumerate a database (if you have breached creds) with sqlmap
- Have a possible XSS on AEM target, but app renders it in JSON?
- @ajxchapman's first command on low CPU VPS
- @s0md3v's tips to beat procrastination & start learning now
- @TomNomNom's biggest bounty & oneliner to grep Git repos for patterns

Misc. pentest & bug bounty resources

- Resources-for-Beginner-Bug-Bounty-Hunters v2021.01

- Intro to Bug Bounty Hunting and Web Application Hacking (@NahamSec's new paid Udemy course)
- Cookie Based Authentication Vulnerabilities
- #diodb search

Challenges

- @SecurityMB's XSS Challenge #5
- Winja CTF 2021: March 6

Articles

- Top 10 web hacking techniques of 2020
- Finding Evil Go Packages
- Anatomy of an Exploit: RCE with CVE-2020-1350 SIGRed

Bug bounty news

- Cybersecurity conferences 2021: A schedule of virtual, and potentially in-person or 'hybrid', events
- ZAPCon: March 9
- ffuf's moving to a sponsorware model & is partnering up with Kali Linux
- Kali Linux 2021.1 Release (Command-Not-Found)

Non technical

- Privilege Escalation in your Offensive Security Career
- DefCamp #11: Cosmin Iordache (Inhibitor181) on the mindset and discipline of being a bug bounty hunter
- Hacker Spotlight: Interview With Geekboy
- Bug Bounty- Finding The First Bug
- AMA – Katie/InsiderPhD, part-time educational cybersecurity youtuber and occasional bug bounty hunter
- #DoWeLookLikeHackers