Bug Bytes #173 – JDBC attacks reloaded, RCE via email & Benchmarking port scanners

BY ANNA HAMMOND · JUNE 8, 2022 · 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.

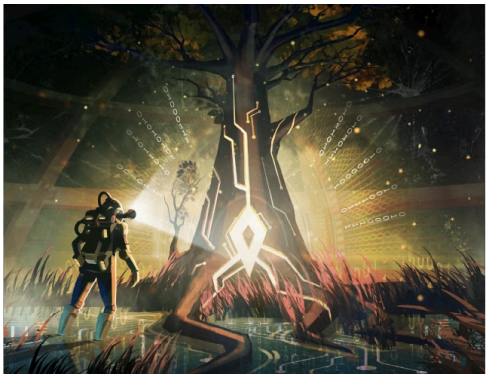
CLICK HERE TO SUBSCRIBE

This issue covers the weeks from May 30 to June 6.

Intigriti news

The Ethical Hacker Insights Report 2022

Keep up with Intigriti's events in June



Apply to Intel's Project Circuit Breaker live hacking event

Our favorite 5 hacking items

1. Articles of the week

Arbitrary File Upload Tricks In Java
Make JDBC Attacks Brilliant Again II
Port Scanner Shootout

In the first article, @pyn3rd shares some tricks to bypass WAFs when testing for file upload vulnerabilities in Java apps. One of them is also useful for SSRF and XXE.

The second article is a new addition to @pyn3rd's research on JDBC attacks. It focuses on PostgreSQL databases which were not included in the "Make JDBC Attacks Brilliant Again" talk .

"Port Scanner Shootout" is a benchmark of port scanning tools by @s0cm0nkeysec. They compare nmap, masscan, naabu and rustcan, with details on each tool's capabilities and pros/cons.

2. Writeup of the week

Horde Webmail – Remote Code Execution via Email

@SonarSource's R&D team describe a cool RCE they discovered in Horde Webmail's default configuration. It is triggered when a user authenticated on the webmail server opens the attacker's email (containing a CSRF exploit), and results in RCE on the server and stealing the victim's clear-text credentials.

3. Video of the week

Could I Hack into Google Cloud?

Google recently announced the winners of the 2021 GCP VRP Prize.
In this video, @LiveOverflow dissects their writeups, trying to understand the bugs, if he could've found them, and what differentiates the winning writeup.

4. Challenge of the week

NotSoCereal-Lab

@notsosecure released this new playground for practicing insecure deserialization. It includes four web apps vulnerable to Java, PHP, Python and Node deserialization, with solutions.
If you want to play with this trendy vulnerability, import the VM in VirtualBox and put your hacker detective hat on!

5. Vulnerability of the week

CVE-2022-26134 – Confluence Server and Data Center unauthenticated RCE

- Atlassian advisory
- Volexity advisory
- Technical analysis by Rapid7
- Nuclei template
- @Junior_Baines's "Through the Wire" PoC

New week, new critical 0-day. CVE-2022-26134 is an unauthenticated RCE in all versions of Confluence. It was first discovered as a 0-day being exploited in the wild.
If you are new to OGNL injection, this is a good opportunity to learn about it with this real-life example.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty 101: #20 – Rapidly Testing APIs for Broken Access Control
- Live com Jason Hadix
- Command Injection | Complete Guide
- Best Hacking Podcast in the world?
- Why You Shouldn't Be an Ethical Hacker

Webinars

- Attacking Thick Client Application by @j33n1k4

Conferences

- Security Fest 2022 – Day 1 & Day 2
- The Hitchhiker's Guide to Pod Security – Lachlan Evenson, Microsoft & A Treasure Map of Hacking (and Defending) Kubernetes

- Introducing the Latest Ghostwriter v2.3.0 @ Black Hat Asia 2022 – Christopher Maddalena & BloodHound @ Black Hat Asia 2022 – Andy Robbins
- SSTIC 2022 (Click on talk titles to see slides and videos)

Tutorials

Medium to advanced

- Securing Cloud Services against Squatting Attacks
- SetUID Rabbit Hole
- Blocking ISO mounting
- Impacket Offense Basics With an Azure Lab

Beginners corner

- Hunting Sourcemaps On Steroids
- Pending Intents: A Pentester's view
- From Zip Slip to System Takeover
- Security Source Code Review – Manual Approaches
- How to find Log4j Vulnerabilities in Every Possible Way

Writeups

Challenge writeups

- Prototype pollution is everywhere! Solution to May '22 XSS Challenge & Challenge winners and community writeups
- HackTheBox – Timing
- CA CTF 2022: Exploiting LFR and forging Cookies – Mutation Lab
- AASLR: Antisyphon Address Space Layout Randomization (MetaCTF walkthrough)
- A Detailed Approach to Solving Oversecured (OVAA) Vulnerable App (For Android Application Security Enthusiasts)

Pentest writeups

- Hacking an AWS hosted Kubernetes backed product, and failing
- Enumeration and lateral movement in GCP environments
- Your cloud? My cloud now

- Public Report – Lantern and Replica Security Assessment

Responsible(ish) disclosure writeups

- hoot hoot pwn – Meeting Owl security disclosure report #IoT
- PoC for a Post-Auth SQL-Injection (CVE-2022-0757) in Nexpose Vulnerability Scanner <= 6.6.128 #Web
- Multiple vulnerabilities in Zyxel zysh #MemoryCorruption #LPE

Bug bounty writeups

- Microsoft Dynamics Container Sandbox RCE via Unauthenticated Docker Remote API 20,000$ Bounty (Microsoft, $20,000)
- Bug bounty reports from Core Rule Set live hacking event (Core Rule Set)
- Hijacking Over 100k GoDaddy Websites (GoDaddy)
- Is Exploiting A Null Pointer Deref For LPE Just A Pipe Dream? (Microsoft)
- Steal private objects of other projects via project import & Bypass (GitLab, $40,000)

See more writeups on The list of bug bounty writeups.

Tools

- npmdomainchecker: Checks all maintainers of all NPM packages for hijackable domains
- websitewatcher: Monitor sites for changes with email notifications
- dsieve: Take a list of urls and filter or extract domains by level
- Astra-Bot: Python based Discord bot which allows you to run tools like nmap and amass from Discord
- Reverse SSH: SSH based reverse shell

Tips & Tweets

- Practical tips for long-running Turbo Intruder attacks
- Don't limit yourself to Git when checking for exposed source code
- Keywords to grep for in a list of URL page titles
- How to tag each request with the corresponding browser profile (within Burp's embedded browser) & Using Sharpener
- Some of the best new infosec GitHub projects
- Does using JWTs make an app not vulnerable to CSRF?

See more tips on this week's Twitter collection.

Misc. pentest & bug bounty resources

- trickest/containers & Intro: Automated privilege escalation of the world's most popular Docker images
- HideAndSec
- cheat/cheatsheets
- PROMPT# Issue: Better Together
- Container security Learning Path bundle by AppSecEngineer ($59 until June 17)

Articles

- Javascript Hoisting in XSS Scenarios
- Leveraging AWS QuickSight dashboards to visualize recon data
- Searching SMB Share Files
- DeepPass — Finding Passwords With Deep Learning
- Abuse and replay of Azure AD refresh token from Microsoft Edge in macOS Keychain

Reports

- 66% of cybersecurity talent are considering bug bounty hunting as a full-time career

Challenges

- The DEF CON CTF 2022 Qualifier

Bug bounty & Pentest news

- Bug bounty
  - Announcing the winners of the 2021 GCP VRP Prize
  - MetaMask Awards Bug Bounty for Clickjacking Vulnerability
- Cybersecurity
  - US export ban on hacking tools tweaked after public consultation
  - 6 'nightmare' cloud security flaws were found in Azure in the last year. Does Microsoft have work to do?
  - Discord Is the World's Most Important Financial Messenger, and a Hotbed for Scammers
  - The Surreal Case of a C.I.A. Hacker's Revenge

    - WhatsApp accounts hijacked by call forwarding
- Tech
    - Firefox Security & Privacy Newsletter – 2022 Q1
- Upcoming events
    - Networking Fundamentals by @TomNomNom (Leeds PHP Meetup) (June 15)
- Tool updates
    - Nuclei v2.7.2

Non technical

- How to get into bug hunting
- 10 Practical Pentesting Tips (from HTB's Staff Hackers!)
- Just Copy What Works