Bug Bytes #167 – AWS RDS Local File Read & Are you making these learning mistakes or misusing Burp's predefined lists?

BY ANNA HAMMOND · APRIL 13, 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 week from April 4 to 11.

Our favorite 5 hacking items

1. Conference of the week

How to Get Better at Hacking | Louis Nyffenegger

This isn't one of @snyff's usual technical talks, but I found it is hilarious and eye-opening. He points out many mistakes that (aspiring) hackers make in their learning journey.
If you are struggling with a plateau or just want to grow your hacking skills from good to amazing, there is probably something mentioned in this talk that will help you out.

2. Writeup of the week

AWS RDS Vulnerability Leads to AWS Internal Service Credentials (Amazon)

@LightspinTech's director of security research, @gafnitav discovered a Local File Read on AWS RDS. It involves an interesting mix of path traversal and PostgreSQL injection.
A great writeup that details the whole thought process including what did not work.

3. Resource of the week

Recon.Cloud

In addition to the previous writeup, @LightspinTech also released recon.cloud, a free search engine for AWS cloud assets.
It references 220,866 assets, and can be a good addition to your recon.

If you are interested in cloud hacking or Kubernetes security, I also recommend following @LightspinTech's Twitter account and blog. They have been releasing many cool tools, articles and tips on these areas of security.

4. Video & Tool of the week

Bypassing a WAF by Finding the Origin IP & CF-Bypass

@0xLupin released a new tool and video on bypassing WAFs (specifically Cloudflare) by finding the Origin IP using Security Trails's historical data.
What I like about CF-Bypass is that it does not just look for the Origin IP but also tries to validate it and reduce false positives. So, even if you already have your own WAF bypass tool or do not want to use Security Trails, reading the code of this tool might give you some cool ideas to add to your own tooling.

5. Tip of the week

Burp Intruder's predefined lists have placeholders that must be replaced with your custom settings

Are you using Burp Intruder's predefined payload lists without additional configuration?
If you do, you may have missed vulnerabilities because these lists have placeholders that must be replaced with your own domain, email, nameserver, etc.
A small tweak that may easily cause you to miss out-of-band vulnerabilities!

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty Redacted #2: Third Party Subdomain Takeover & Exposed Admin Interfaces
- Dangerous Code Hidden in Plain Sight for 12 years
- Exchange Server Vulnerability – CVE Deep Dive
- Tips for Getting Started in Cybersecurity
- Hacking Linux // Linux Privilege escalation // Featuring HackerSploit
- How To Create Your Own Pentesting Distribution
- Executing Linux Binaries Without Touching Disk – Living Off The Land with DDExec and Dirty Pipe Demo

Podcasts & Audio

- AMA session with Harsh Bothra @harshbothra_

Webinars

- BHIS | Introduction to Pentesting with Mike Felch
- Live Workshop – Attacking AWS Elastic Kubernetes Service (EKS)

Conferences

- Keynote NDC Security 2022 – The Abridged History of Application Security – Jim Manico
- ComfyCon AU 2022 – Day 1 & Day 2

Slides & Workshop material

- Making of: The Sanitizer API

Tutorials

Medium to advanced

- Introducing Code Review Hotspots with Semgrep
- Azure Dominance Paths
- Learning Machine Learning Part 1: Introduction and Revoke-Obfuscation
- SID filter as security boundary between domains?
- Cloud-native security (container security Cheat Sheet) – Part 1

Beginners corner

- Expanding the attack surface with Shodan's lesser known filter
- Configuring an out-of-band callback listener and notification service in under 10 minutes using AWS Lambda function URLs and Discord webhooks
- Create your own Discord BOT for Recon – Bug Bounty
- A Detailed Guide on Cewl
- A Detailed Guide on Responder (LLMNR Poisoning)

Writeups

Challenge writeups

- HackTheBox – Backend
- HackTheBox – Overflow & Blog post
- LovelyKittenPictures – to root – 1337UP LIVE CTF challenge writeup
- soXSS (Same Origin XSS) – writeup

Responsible(ish) disclosure writeups

- VMware Workspace ONE Access – Freemarker SSTI (CVE-2022-22954) PoC & Nuclei template

- Securing Easy Appointments and earning CVE-2022-0482 #Web #CodeReview
- CVE-2021-4119: [Bookstack] Email harvesting via SQL "LIKE" clause exploitation #Web #PHP #CodeReview
- MacOS SUHelper Root Privilege Escalation Vulnerability: A Deep Dive Into CVE-2022-22639 & PoC #MacOS #LPE

Bug bounty writeups

- Integer overflow in table extension (GitHub, $40,000)
- SVG SSRFs and saga of bypasses
- How a YouTube Video lead to pwning a web application via SQL Injection worth $4324 bounty ($4,324)
- HTTP Request Smuggling on business.apple.com and Others.
- Meta's SparkAR RCE Via ZIP Path Traversal (Meta / Facebook, $2,500)

See more writeups on The list of bug bounty writeups.

Tools

- ipcdn: Check which CDN providers an IP list belongs to
- checkip: Get quick info on an IP address
- Jeeves: Go tool that looks for time-based blind SQL injection through recon
- TrashCompactor:
- spring4shell-scan: A fully automated, reliable, and accurate scanner for finding Spring4Shell and Spring Cloud RCE vulnerabilities
- bore: A simple CLI tool for making tunnels to localhost

Tips & Tweets

- Story of how 19-year-old @hacker_ gained ADMIN access to a Trans-Atlantic cable & Accessing 302 Military FTP servers
- Lessons for more effective code review
- Something to try if you find URL shortened links in pentests
- Two free IPinfo tools to quickly look at your target domain's IP space
- Jhaddix's threads on Stealing checks worth millions & pwning a bank, Inspecting out-of-scope mobile apps & Finding SQL injection on a blog

See more tips on this week's Twitter collection.

Misc. pentest & bug bounty resources

- Insiders: Archive of Potential Insider Threats
- @Jhaddix's Xmind Hunt template (for starting a bounty hunt)
- ZAP vs Websites Vulnerable to SSTI
- Hashcat-rules
- Semgrep ruleset for C/C++ vulnerability research

Articles

- Round Two: An Updated Universal Deserialisation Gadget for Ruby 2.x-3.x
- Making Smb Accessible With NTLMquic
- Performing And Preventing Attacks On Azure Cloud Environments Through Azure Devops
- Abusing Azure Hybrid Workers for Privilege Escalation – Part 1

Challenges

- NahamCon CTF 2022 (April 28 – 30)
- Can you spot the vulnerability in @C0okies3's code snippet?
- cicd-goat: Deliberately vulnerable CI/CD environment
- Nullcon Berlin 2022 HackIM-CTF (source code)

Bug bounty & Pentest news

- Cybersecurity
  - GitHub can now auto-block commits containing API keys, auth tokens
  - F5 investigating reports of NGINX zero day
  - OpenSSH 9.0 bakes in post-quantum cryptography to future proof against attacks
- Upcoming events
  - Bounty Thursdays – Live (Thursday 14/4 16:00 CET)
- Tool updates
  - Param Miner 1.4c now includes hover-tooltips documenting all the settings
  - Burp Scanner can now crawl static sites between 6x – 9x faster
  - SpiderFoot 4.0 Open Source Release & YAML correlation rules
  - ffuf 1.5.0

- Arjun v2.1.5
- unfurl v0.3.1
- Feroxbuster v2.6.2
- QLinspector (For finding Java gadget chains with CodeQL)

Non technical

- The #100DaysOfHacking Challenge : A Game Changer for Me