Bug Bytes #122 – ReDoS demystified, PayloadAllTheThings inside Burp & An $18k Instagram OAuth misconfiguration

BY ANNA HAMMOND · MAY 12, 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.

CLICK HERE TO SUBSCRIBE

This issue covers the week from May 3 to 10.

Intigriti News

Meet the hacker: Get to know sumgr0, The King of subdomain takeovers

Our favorite 5 hacking items

1. Tools of the week

HopLa

versionshaker

HopLa is a Burp extension that adds payloads to Burp with autocompletion. By default, payloads used are from PayloadAllTheThings but you can customize them. This makes it so easy to create your own custom payload library inside Burp.

Versionshaker is a handy Python tool for fingerprinting the exact version of open source software used on a site. Let's say for instance that you have trouble identifying the version of WordPress used on a site. Versionshaker takes the site's URL, the WordPress GitHub repo's URL and paths of static files to compares (e.g. JS or CSS files). It does its magic and returns which releases of WordPress have these exact files.

2. Writeups of the week

How I Hacked Google App Engine: Anatomy of a Java Bytecode Exploit (Google)

Account takeover of Instagram accounts due to unrestricted permissions of third-party application's generated tokens (Facebook, $18,000)

The first writeup is about an RCE in Google App Engine that the author found in a week during their internship at Google.
To be honest, I did not understand any of it but maybe you will! In any case, it is interesting to see what other hackers are working on and different areas to explore (in this case hacking with low level Java byte code).

The second writeup is much easier to digest but also impactful. @Samm0uda noticed that an Instagram OAuth flaw returned an access token with more permissions that it should. This allowed for taking over Instagram accounts.
Simple, but the difficulty lies in detecting the change in the access token's permissions.

3. Video of the week

Regular Expression DOS FOR BEGINNERS!

If you want to learn about RegEx and ReDoS, this is the best introduction to these complex topics. @Farah_Hawaa explains just what you need to understand their basics and a practical example of detection and exploitation.

4. Resource of the week

huntr hacktivity

This is a hacktivity for vulnerabilities found in open source software. More and more hackers are looking for bugs in 3rd-party software to leverage in bug bounties/pentest. So this is an interesting vulnerability database and collection of writeups on which to keep an eye.

5. Tutorial of the week

DNS Based Out of Band Blind SQL injection in Oracle — Dumping data

The first tutorial is all about DNS-based Out-of-Band SQL Injection. It explains techniques that are good to know in case you encounter this type of injection: How to ensure it is not a false positive, the type of

backend database, how to dump data from the database and bypass limitations of exfiltrating via DNS (no spaces, max 253 characters, DNS cache...).

Other amazing things we stumbled upon this week

Videos

- iOS Hacking – Inter-App Communication, App Transport Basics & Webviews
- What is Insecure Deserialization? | Security Engineering Interview Questions
- Open Source Bug Bounty
- ARE CTF CREATORS EVIL?! – A Conversation around realworld CTF's with Adam Langley.
- How Fuzzing with AFL works! & Blog post

Podcasts

- The InfoSec & OSINT Show 55 – Charlie Belmer & NoSQL Injection
- Hack Chat // Stok Fredrik // Bug Bounty Hunting Like A Boss
- DAY[0] Episode 76 – Fake Vulns, More Valve, and an AWS Cognito Issue
- News From the Darkside – Exim Email Server, Tor's Exit Nodes, TsuNAME, Project Hail Mary

Webinars

- GitDorker – GitHub Recon Simplified for Bug Bounty, Red Teams, and Penetration Testers

Tutorials

- Web App Pen Testing in an Angular Context
- Remote Potato – From Domain User to Enterprise Admin
- Phishing with fake meeting invite
- Demystifying Insecure Deserialisation on JSF Application
- Remote Code Execution – Insecure Deserialization
- Hacker tools: Nuclei, a YAML based vulnerability scanner

Writeups

Challenge writeups

- Doggo CTF Walkthrough (in Partnership with Amazon & BugPOC) #video
- SQL Injection – Lab #9 SQL injection attack, listing the database contents on non Oracle databases & SQL Injection – Lab #10 SQL injection attack, listing the database contents on Oracle #video

Responsible(ish) disclosure writeups

- Domain Hijacking Via Logic Error – Gandi And Route 53 Vulnerability #DNS
- tsuNAME – Vulnerability that can be used to DDoS DNS #DNS
- Mouse Trap #RCE #Android #Windows
- CVE-2021-32030: ASUS GT-AC2900 Authentication Bypass #Router #RCE
- 21Nails: Multiple Critical Vulnerabilities in Exim Mail Server #Web
- Password reset code brute-force vulnerability in AWS Cognito #Web

Bug bounty writeups

- Workplace by Facebook | Unauthorized access to companies environment — $27,5k (Facebook, $27,500)
- The False Oracle — Azure Functions Padding Oracle Issue (Microsoft)
- CVE-2021-1815 – MacOS Local Privilege Escalation Via Preferences (Apple)
- My first OOB XXE exploitation

See more writeups on The list of bug bounty writeups.

Tools

- Jenkins Attack Framework (JAF) & Intro
- Mystikal & Intro: macOS Initial Access Payload Generator
- Baserunner & Intro: A tool for exploring and exploiting Firebase datastores
- PyOracle2: A python-based padding oracle tool
- GDir-Thief & Intro: Red Team tool for exfiltrating the target organization's Google People Directory that you have access to, via Google's API

Tips & Tweets

- 403 bypass with ; on Java app
- 403 bypass on API endpoint with ;;
- Finding new (sub)domains in Web archived OAuth endpoints

- Bash alias to quickly check for status codes of different HTTP methods

Misc. pentest & bug bounty resources

- OneListForAll
- geeknik/the-nuclei-templates
- The Journey to Try Harder: TJnull's Preparation Guide for PEN-200 PWK/OSCP 2.0
- @theXSSrat's bug bounty notes
- Awesome Windows Potatoes
- SAMLZine

Articles

- Using UUIDs for Authorization is Dangerous (even if they're cryptographically random)
- Firebase Domain Front – Hiding C2 as App traffic
- Weird Ways to Run Unmanaged Code in .NET
- ExpLoading: A slightly new angle on an old problem

Bug bounty & Pentest news

- Google and Mozilla will bake HTML sanitization into their browsers
- Vulnerability Discovery For All
- Upcoming events
  - Hacking Battlegrounds live-streamed tournament (May 15)
  - SSTIC 2021 (June 2-4)

Non technical

- Meet the hacker: Get to know sumgr0, The King of subdomain takeovers.
- Think outside the box with Debangshu Kundu

Community pick of the week

Awww such a cutie, well done @_sebd!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!