Bug Bytes #136 – GraphQL fingerprinting, Building new SSTI payloads & A HTTP/2 request smuggling lab

BY ANNA HAMMOND · SEPTEMBER 1, 2021 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-136-graphql-fingerprinting-building-new-ssti-payloads-a-http-2-request-smuggling-lab

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 August 23 to 30.

Our favorite 5 hacking items

1. Video of the week

Dan Miessler Talks About Recon/Automation, Seclists, Certifications, Mental Health & More!

This interview with @DanielMiessler is a must watch if you are into hacking and personal growth. One of @NahamSec's best interviews or like he says: "If you're going to watch only one of my videos, this should be it".

2. Writeup of the week

Vulnerability in Bumble dating app reveals any user's exact location

@RobJHeaton discovered a way to disclose the exact location of Bumble users using trilateration. It is a nice read if you like creative findings and fun writeups (it's written like a detective story).

3. Tutorials/Resources of the week

Python context free payloads in Mako templates & Python vulnerabilities : Code execution in jinja templates
How to set up Docker for Varnish HTTP/2 request smuggling & Repo

SSTI payloads for RCE can be complex and look like magic to beginners. If you wonder how they are constructed, the first couple of tutorials will be helpful. @podalirius_ created several new payloads for Mako and Jinja, and explains the methodology used to construct them.

The second tutorial and accompanying repository will be useful if you want to practice finding HTTP/2 request smuggling vulnerabilities. The dockerized lab deploys a local environment that is vulnerable to CVE-2021-36740 (HTTP/2 request smuggling in Varnish).

4. Article of the week

API Tokens: A Tedious Survey

You may have heard of OAuth 2.0, JWT, PASETO and Protobuf Tokens, but have you heard of Macaroons, Biscuits and Facebook CATS? This article compares these different types of API tokens from a security standpoint. It is addressing developers but knowing the weaknesses of each type of token provides good insights for anyone who has to test API security.

5. Tools of the week

uro
graphw00f
Interactsh Collaborator

There is a common problem bug hunters face when fuzzing a list of URLs: How to avoid testing similar/duplicate or uninteresting URLs? @s0md3v released uro, a handy Python script that solves this issue using pattern matching (e.g. to remove blog pages) and extensions (to remove js/pdf/png... files).

@dftrace's graphw00f is a Python tool that takes a GraphQL endpoint as input and tries to fingerprint the server engine behind it. It doesn't just return the detected engine's name, but also its default defense mechanisms (useful to know when you're trying to attack it!).

If you use Project Discovery's Interactsh and Burp, you might love @wdahlenb's interactsh-collaborator. It is a Burp extension that acts as an Interactsh client. So, you get free out-of-band testing directly from Burp.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Cross-Site Request Forgery (CSRF) | Complete Guide
- HTTP Desync Attack Explained With Paper
- "You Changed My Life" with @John Hammond (Hacker Heroes #11)
- Common Open Redirection Bug Bounty Mistakes
- Creating a YouTube TV that could steal your private videos – $6,000 CSRF
- How To Setup Your Terminal For Penetration Testing

Podcasts

- Finding bugs in Google VRP without recon – David Schütz – BBRD #01
- Radio Hack Ep4: Client-Side Bugs – Youssef Sammouda (in Arabic)

Webinars

- Kubernetes Security: Attacking and Defending K8s Clusters & Kubernetes Gotchas – Hacking and Defending Kubernetes
- SiegeCast "The Way of the Spray" with Security Consultant Jason Downey & Slides

Conferences

- BSides LV 2021 Day 1 Stream 1, Day 1 Stream 2, Day 2 Stream 1 & Day 2 Stream 2, especially:
  - Breaking The Giants With Logic
  - Repo Jacking: How GitHub exposes over 70,000 projects to remote code injection
- Rotem Bar – Hacking OSS (BSidesTLV 2021)

Tutorials

Medium to advanced

- Python context free payloads in Mako templates & Python vulnerabilities : Code execution in jinja templates
- Illogical Apps – Exploring and Exploiting Azure Logic Apps
- Understanding Salesforce Flows and Common Security Risks
- AWS ReadOnlyAccess: Not Even Once

Beginners corner

- How to set up Docker for Varnish HTTP/2 request smuggling & Repo
- Hacker Tools: ReNgine – Automatic recon & Hacker Tools: WPScan – Your WordPress isn't safe!
- Introduction to postMessage() Vulnerabilities
- Burp Suite and Beyond: Exploring non-HTTP protocols using MITM_RELAY
- Exploration of Native Modules on Android with Frida & Getting started with Frida on Android Apps

Writeups

Challenge writeups

- A method for escaping the default docker environment
- Python Web Hackin' on PortSwigger's Web Security Academy
- Crack Me If You Can 2021

Responsible(ish) disclosure writeups

- Stored XSS to RCE Chain as SYSTEM in ManageEngine ServiceDesk Plus #Web

- Finding Insecure JWT Signature Validation with CodeQL #Web #CodeReview
- Tampering with arbitrary packages in @types scope of npm #Web
- Technical Advisory: Pulse Connect Secure – RCE via Uncontrolled Archive Extraction – CVE-2021-22937 (Patch Bypass) #Web
- Fortinet FortiWeb OS Command Injection #Web
- McAfee Enterprise ATR Uncovers Vulnerabilities in Globally Used B. Braun Infusion Pump #IoT

0-day & N-day vulnerabilities

- [CVE-2021-22902] Rails ActionPack DoS
- Exploit script for SAP Business Objects SSRF (CVE-2020-6308)

Bug bounty writeups

- How MarkMonitor left >60,000 domains for the taking
- ChaosDB: Critical Vulnerability in Microsoft Azure Cosmos DB (Microsoft, $40,000)
- By Design: How Default Permissions on Microsoft Power Apps Exposed Millions (Microsoft)
- Pwn2Own Vancouver 2021 :: Microsoft Exchange Server Remote Code Execution (Microsoft)
- Proxytoken: An Authentication Bypass In Microsoft Exchange Server (Microsoft)
- The Nomulus rift (Google)
- Two account takeover bugs worth $4300
- Cache Poisoning (Squid Cache (IBB), $6,000)

See more writeups on The list of bug bounty writeups.

Tools

- BatchQL & Intro: GraphQL security auditing script with a focus on performing batch GraphQL queries and mutations
- hakluke/dumpcn: Get all the CNs and SANs from a list of domains
- deeplink-fuzz.sh: A Bash wrapper for radamsa that can be used to fuzz exported activities and deep links
- wmkick & Intro: MITM MS-RPC, WMI, WinRM to Capture NetNTLMv2 Hashes

Tips & Tweets

- CSRF against APIs with a solid CORS config
- Symfony's Profiler DEV tools

- Parameter Pollution #2 & PHP drops any header if it finds nullbyte value in the header
- Using JSON response to build API endpoints wordlist
- Get directory and files from urlscan.io public scans
- Local File Inclusion vs Local File Disclosure
- How to download Windows legally for pentesting or malware analysis

Misc. pentest & bug bounty resources

- MobileHackingCheatSheet 1.0
- Cybr
- 0xAwali's methodology for testing GraphQL & Redirection Response
- Demystifying Cookies and Tokens Security
- Kotlin-SCP
- pwdec/payloads

Challenges

- Google CTF Beginners Quest 2021
- Pentesting lab by @0xConda
- GCP Goat & Guide

Articles

- Bypassing Cloudflare using Cloudflare
- What We Learned from 200,000 OpenAPI Files
- Blast Radius: Mapping, Controlling, and Exploiting Dynamic Self-Registration Services
- AWS privilege escalation: exploring odd features of the Trust Policy
- URL Filter Subversion

Bug bounty & Pentest news

- Bug bounty
  - Facebook Bug Bounty: Introducing Researcher Collaboration Payouts
- Cybersecurity
  - Widespread credential phishing campaign abuses open redirector links
  - The Dan Kaminsky Fellowship: Supporting open source projects to strengthen this Internet

    - Google: Why we're committing $10 billion to advance cybersecurity
- Upcoming events
    - GrabCON 2021 (September 2)
    - Pwn2own Austin 2021: Phones, Printers, NAS, And More! (November 2-4)
- Tool updates
    - SecLists 2021.3.1
    - ReconFTW v2.0
    - Nuclei v2.4.3 (Added support for using environment variables directly in templates)
    - Notify v1.0.0 (New flags & new providers supported)

Non technical

- How to optimize your hacking by understanding your mind.
- Hacker-Powered Security and DeFi: How Human Intelligence Improves Cryptocurrency Security
- TCM Security's Practical Network Penetration Tester (PNPT) Certification – Seven Days of Authentic Penetration Testing