Bug Bytes #119 – AutoGraphQL, WhatsApp MitD & Desktop apps mishandling bad URIs

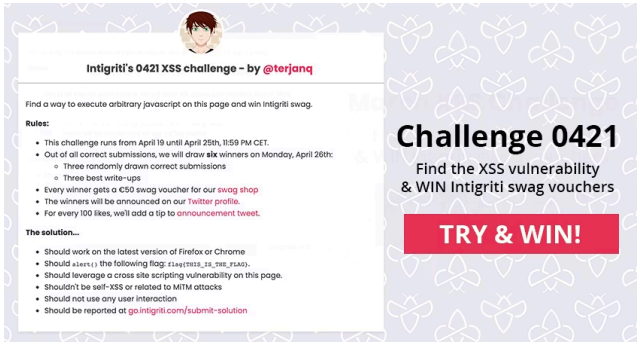
BY ANNA HAMMOND · APRIL 21, 2021 · LAST UPDATED ON MARCH 6, 2025

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 April 12 to 19.

Intigriti News



Intigriti's 0421 XSS challenge – by @terjanq

Our favorite 5 hacking items

1. Conference of the week

BSides Canberra 2021

BSides Canberra videos are up! You know what this means? AssetNote's presentation of KiteRunner and "Context Aware Content Discovery" is available to watch.

If you found the tool and blog post (featured in Bug Bytes 118) interesting but prefer video, you now have a great 50 min talk to catch up on.

2. Writeups of the week

Remote exploitation of a man-in-the-disk vulnerability in WhatsApp (CVE-2021-24027) (Facebook)
Allow arbitrary URLs, expect arbitrary code execution

The first writeup is about a Man-in-the-Disk vulnerability that CENSUS researchers found in WhatsApp messenger for Android. It is a pretty impressive bug chain involving Chrome SOP bypass to access files in

/sdcard, stealing WhatsApp's TLS secrets stored in /sdcard, and hijacking the download of a ZIP file to replace it with a malicious one and get RCE.

The second writeup is about 1-click code execution vulnerabilities @positive_sec found in Telegram, Nextcloud, VLC, Wireshark and other Desktop apps. It is interesting to see how different operating systems behave when insecure URLs (with different schemes) are opened, and how this can lead to so many RCE!

3. Videos of the week

Live Recon and Automation on Shopify's Bug Bounty Program with @TomNomNom
API Recon with Kiterunner – Hacker Toolbox

The only thing I enjoy more than a bug hunter's interview is a hands-on hacking session! In this one (first video), we get a sneak peek at @TomNomNom's approach of recon, automation, and how he uses some of the tools he's created that many of us use (waybackurls, httprobe, fg, meg, etc).

The second video by @InsiderPhD is an introduction to KiteRunner. If you're curious to know what makes this tool special and how to quickly start using it, this is the perfect guide.

4. Tools of the week

phpggc-generate-payloads.sh
AutoGraphQL & Video How-to guide

phpggc-generate-payloads.sh by @honoki is a Bash script that automatically generates RCE payloads for all gadget chains in PHPGGC. It's a time saver when you're testing PHP apps for insecure deserialization and want to quickly identify the RCE gadget chain that works.

AutoGraphQL is @ngalongc's online tool that helps speed up the process of GraphQL authorization testing. Given a schema URL and user credentials, it generates mutations and queries that you can quickly execute (using the different creds). This allows you to easily identify any authorization issues.

5. Challenge walkthroughs of the week

Hacking AWS: HackerOne & AWS CTF 2021 writeup
HackTheBox – Laboratory

The first writeup is about a realistic AWS/SSRF bug chain that @d0nutptr and @NahamSec encountered on a real target and recreated as a CTF. Whether you played the challenge or not, it's a good read to maybe learn something new about AWS exploitation.

The second walkthrough is a fun mix of exploiting an old GitLab instance, digging into a bug bounty report, escalating LFI to RCE, and privilege escalation. Note that the box is retired so if you have a paid HackTheBox subscription, it's better to attempt solving it before watching the walkthrough.

Other amazing things we stumbled upon this week

Videos

- What the Hack: What Is XSS and How to Find It
- Fundamentals of Bug Bounty Recon & The Most Misunderstood Element: Recon

- Hacking Facebook in 3 different ways for $54,800 – Bug Bounty Reports Explained
- Lineage OS, Rooting & Custom ROMs – Hacking Android – Sniffing Android '10' HTTPs traffic- Part – 03
- No BS Guide – Underrated Utility Tools for Bug Bounty

Podcasts

- Security Conversations 63 – Shubs Shah on finding riches (and lessons) from bug bounty hacking
- DAY[0] Episode 73 – Windows Bugs, Duo 2FA Bypass, and some Reverse Engineering
- Homogeneity Attacks – Is FLoC All That Bad?, Humble Bundle For Programmers, Chrome 90

Tutorials

Medium to advanced

- Creating A Custom View for WebSocket in ZAP
- JavaScript prototype pollution: practice of finding and exploitation
- Client-Side Encryption Bypass (3)
- Basic operational security when dropping to disk
- Escalating Privileges with DNSAdmins Group — AD

Beginners corner

- Exploiting weak configurations in Google Cloud Identity Platform
- Pentest Workflow — Leveraging Community-Powered Tools
- BITS For Script Kiddies
- Why Does Nmap Need Root Privileges?
- Rainbow Tables (probably) aren't what you think — Part 1: Precomputed Hash Chains & Part 2: Probability, Efficiency, and Chain Collisions

Writeups

Challenge writeups

- SQL Injection – Lab #7 SQL injection attack, querying the database type and version on Oracle (video)

Pentest writeups

- Using DVC to tunnel arbitrary connections inside of RDP
- An IDOR that could have led to stealing money from a Fintech company

- Doyensec Teleport Security Auditing Report 2020 #PentestReport
- When a Denial of Service matters: fighting with risk assessment guys

Responsible(ish) disclosure writeups

- Airstrike Attack – FDE bypass and EoP on domain joined Windows workstations (CVE-2021-28316) #Wifi #AD
- This WhatsApp vulnerability is pretty stupid, but it can lock you out of your account indefinitely
- xscreensaver can be used to run tcpdump without root on debian

Bug bounty writeups

- (POC) Remove any Facebook's live video ($14,000 bounty) (Facebook, $14,000)
- Remote exploitation of a man-in-the-disk vulnerability in WhatsApp (CVE-2021-24027) (Facebook)
- Allow arbitrary URLs, expect arbitrary code execution
- Google Photos : Theft of Database & Arbitrary Files Android Vulnerability (Google, $1,337)
- How I got 9000 USD by hacking into iCloud (Apple, $9,000)
- ELECTRIC CHROME – CVE-2020-6418 on Tesla Model 3
- RCE via unsafe inline Kramdown options when rendering certain Wiki pages (GitLab, $20,000)
- Ability to DOS any organization's SSO and open up the door to account takeovers (Grammarly, $10,500)
- Lets Learn English – Hacking 10M+ Users

See more writeups on The list of bug bounty writeups.

Tools

- HttpDoom: Validate large HTTP-based attack surfaces in a very fast way (inspired by Aquatone)
- AWS Service Enumeration: AWS service enumeration and information gathering for compromised AWS account credentials
- goop: Yet another tool to dump a git repository from a website
- GodSpeed: Fast and intuitive manager for multiple reverse shells
- Airstrike: Automatically grab and crack WPA-2 handshakes with distributed client-server architecture

Tips & Tweets

- @pudsec's XSS and two bypasses
- Login with Google even though it's restricted to a company's domain

- Unicode normalization in HTTP parameters
- Re-testing resolved dupe reports
- WAF SQL injection bypasses for when you can't use commas (,)

Misc. pentest & bug bounty resources

- No Sandbox: Apps that run Chromium without the sandbox
- XXE Study
- KNR-XSS-Payloads
- Playing With Chatbots
- Windows & Active Directory Exploitation Cheat Sheet and Command Reference
- So many blogs & Youtube channels!

Challenges

- Intigriti's 0421 XSS challenge – by @terjanq
- busk3r/genericuniversity: @InsiderPhD's Generic Universoty dockerized

Articles

- HTTPWTF
- SMASH
- Hiding Behind the Front Door #DomainFronting
- Named Pipe Pass-the-Hash
- PoshC2 – Introducing Native macOS Implants

Bug bounty & Pentest news

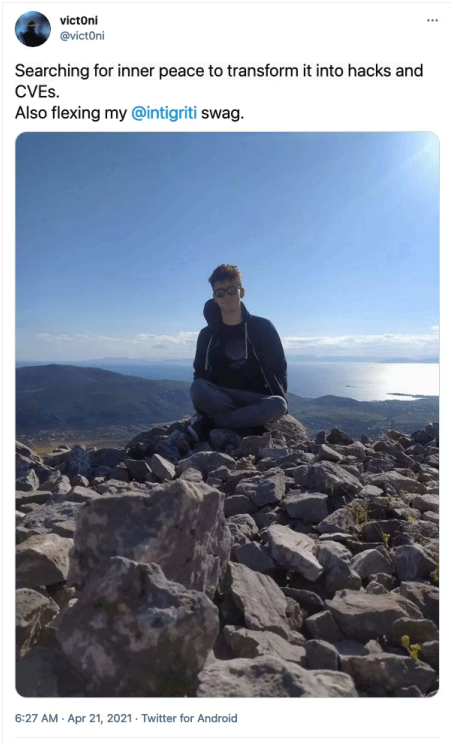
- Google Project Zero: Policy and Disclosure: 2021 Edition
- Rust in the Linux kernel & Cover letter
- Conferences:
  - DEF CON 29 with be both in-person & virtual
  - IsolationCon 2 (April 24-25)
  - The LevelUp CFP is open! Calling all speakers!
- Tools updates:
  - Burp Professional / Community 2021.4.1

- Did you know about BBRF's Custom execution hooks?
- Behind GitHub's new authentication token formats

Non technical

- Research Threats: Legal Threats Against Security Researchers
- Hey you, are you a misfit?

Community pick of the week



@vict0ni's secret to successful hacks and CVEs? Finding inner peace in nature while rocking our swag. Excellent advice!

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!