Bug Bytes #128 – GraphQL Autocorrect, Dangerous Dynamic code loading & How to audit Salesforce Lightning Components

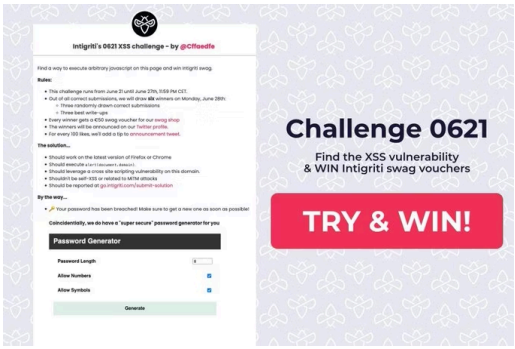
BY ANNA HAMMOND · JUNE 23, 2021 · LAST UPDATED ON MARCH 6, 2025

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 June 14 to 17.

Intigriti News



Intigriti's 0621 XSS challenge – by Physuru (@cffaedfe)

Our favorite 5 hacking items

1. Webinar of the week

Attacking GraphQL's Autocorrect – null Ahmedabad Meet

As part of the null Ahmedabad June Meet, @s0md3v presented a new attack vector against GraphQL. It leverages GraphQL's Autocorrect to reverse engineer GraphQL schemas when introspection is disabled. The tool that automates the attack, Tide, isn't public yet but will be soon hopefully.

2. Writeups of the week

Why dynamic code loading could be dangerous for your apps: a Google example (Google)
How I Found A Vulnerability To Hack iCloud Accounts and How Apple Reacted To It (Apple, $18,000)

The first writeup demonstrates why it is a bad idea for Android apps to load code dynamically: it enables escalating Intent Redirection vulnerabilities into arbitrary code execution, with the example of a vulnerable Google app. This prompted Google to issue a warning for developers about apps that contain Intent Redirection.

Another interesting writeup this week is an iCloud account takeover by @LaxmanMuthiyah. Using a combination of race condition, 2FA bypass and rate-limiting bypass, it was possible to change the password of any Apple ID with just their phone number.

3. Resource of the week

Lightning Components: A Treatise on Apex Security from an External Perspective & AppOmni Labs learning environment

@ConspiracyProof dives deep into the security of Apex (Salesforce's proprietary programming language), how to audit Lightning Components and find common vulnerabilities like SOQL injection. Interestingly, the outlined methodology allowed him to find most of his bug bounty findings.

4. Tutorial of the week

iOS App Testing Through Burp on Corellium

This is one of the most comprehensive tutorials I've seen on the topic. It answers questions like why you need a physical device if you're a bug hunter, how to set up Burp, jailbreak, bypass certificate pinning, decrypt apps, set up a Corellium instance, etc. Great work by @defparam!

5. Video of the week

Understand Security Risk vs. Security Vulnerability!

This is a must-watch for bug hunters. @LiveOverflow explains the difference between a security risk and a security vulnerability. This will clear up why open redirects are not accepted by many bug bounty programs, and why some reported "vulnerabilities" are fixed despite being rejected.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Hacker Heroes #1 – @samengmg (Interview)
- codingo_ Shares His Recon Approach Using SecurityTrails, FDNS, Whoxy and more!
- Live GitLab Ask a Hacker with Bug Bounty Hunter (vakzz) William Bowling (Public)
- Security Shorts: E08 – Job Hunting with Aseem Shrey
- Bug Bounties Using only Burp & Browser – 30 DAY RESULTS (UNEXPECTED)[CLICKBAIT]

- Hacking Android Deeplink Issues | Insecure URL Validation | Android Pentesting
- OSED Review – Offensive Security Exploit Developer
- Binary Exploitation Deep Dive: Return to LIBC (with Matt)

Podcasts

- The InfoSec & OSINT Show 61 – Robert Graham & Large Scale Port Scanning w/Masscan
- Cybr Podcast: How to get started and breakthrough in Bug Bounty Hunting with Hakluke
- Avaddon Ransonomics – Chrome 0-Day, Big Spinrite Update, iOS Wi-Fi Bug, Economics of Ransomware
- Darknet Diaries Ep 95: Jon & Brian's Big Adventure

Webinars

- ZAP DeepDive – Fuzzing
- Webinar: PenTesting Fails – What To Do When You Make (a Lot of) Mistakes in InfoSec

Conferences

- BSides SATX 2021 Track 1, Track 2, Track 2 & Track 2
- THCon 2k21 & Agenda (French & English)

Tutorials

Medium to advanced

- Digesting the Concept of Trusted Types
- Fetching API/Encryption Key from Android app secured by NDK (Native Development Kit)
- CloudFlare for IP Address Filtering

Beginners corner

- Django Templates Server-Side Template Injection
- Hacker tools: BBRF – organizing your recon
- in simple words: Pen-Testing Salesforce SAAS Application (Part 1 – The Essentials) & Part 2 – Fuzz & Exploit

Writeups

Challenge writeups

- CCC H1-CTF Write-Up
- Northsec CTF 2021 Write Up: "Impurity Assessment Form"
- GitHub Security Lab CTF – Call to Hacktion
- SQL Injection – Lab #12 Blind SQL injection with conditional errors #video

Responsible(ish) disclosure writeups

- CVE-2020-11110: Grafana Stored XSS #Web
- CVE-2021-31585: Accellion kiteworks – Web administrator to remote code execution #Web
- Research Shows Over 100,000 Libraries Affected By Maven Vulnerability CVE-2021-26291 #Web
- RetroArch for Windows – Versions 1.9.0 – 1.9.4 #RCE #Windows
- CiviCRM 5.22.0 – Code Execution Vulnerability Chain Explained #Web

Bug bounty writeups

- Unauthenticated Gitlab SSRF (GitLab)
- Part-1 Dive into Zoom Applications (Zoom, $22,000)
- Sanitizer bypass if the sanitized markup is assigned to srcdoc (Mozilla)
- Account takeover via stored XSS with arbitrary file upload
- CSP bypass via wrong inheritance (Chromium) & CSP bypass: How one Chrome XSS bug took 2.5 years and an HTML spec change to fix
- Brave Browser Tor Window leaks user's real IP to the external DNS server (Brave Software, $1,000)
- Second-order SOQL injection through email and campaign name parameter in Salesforce lead submission (HackerOne)

See more writeups on The list of bug bounty writeups.

Tools

- goverview: Get overview about list of URLs
- ZDNS: Fast CLI DNS Lookup Tool
- hakrevshell: A tool for easily generating reverse/bind shells via tcp/udp on your system
- namemash.py: Creating a user name list for brute force attacks

Tips & Tweets

- How to load large payload files in Burp Intruder without crashing it

- Bypassing IP-based 403
- SSRF in ASP apps
- Alternative way to upgrade TTY
- Lengthy filename reveals hidden upload location
- Parsing large files quickly

Misc. pentest & bug bounty resources

- XML attacks mindmap
- resources.harshbothra.tech
- Karanxa/Bug-Bounty-Wordlists
- Image Upload Exploits
- Nightmare: Intro to binary exploitation / reverse engineering course based around CTF challenges
- WiFi Adapter for Kali Linux – The Best WiFi Adapter for Hacking in 2021

Challenges

- Intigriti's 0621 XSS challenge – by Physuru (@cffaedfe)
- Get ready for the 2021 Google CTF (July 17-18)

Articles

- One Time Code Bypass With An Inverted Brute-Force Attack
- Certified Pre-Owned
- Microsoft ADCS – Abusing PKI In Active Directory Environment
- Shadow Credentials: Abusing Key Trust Account Mapping for Account Takeover & Whisker
- Quick Analysis for the SSID Format String Bug

Bug bounty & Pentest news

- Okta (virtual) Bug Bash: 2021! & Bug Bash 2021 Mentorship Application
- Upcoming events:
  - VSACC 2K21 (June 28 – July 1)
- Updates:
  - InjuredAndroid 1.0.11 release (new flag about File providers)

- BBRF v1.1.11 (new flags)
- codingo.com has a new feature to search the last 50 videos by every channel on https://securitycreators.video
- OWASP ZAP: Baseline Scan Changes

Non technical

- Meet the hacker: Samuel Eng
- Being Okay With Not Being Okay: Getting Candid with Ben Sadeghipour — NahamSec
- Infosec Bugbounty AMA with Akita, Arif Khan & Castilho, Harsh Bothra & Mikey
- (Not so serious) #cisotips

Community pick of the week

Beautiful, well done @iqimpz!

See this cool poster @Zwoltopia makes only for our 1337 hackers? If you want one too, you have 7 days left to try and get into our quarterly leaderboard!

Also if you 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!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com