Bug Bytes #125 – Nuclei for mobile, ImageTragick like it's 2016 & Intro to HTTP/2 and HTTP/3

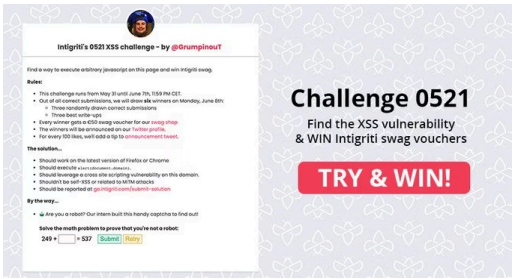
BY ANNA HAMMOND · JUNE 2, 2021 · LAST UPDATED ON MARCH 6, 2025

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 24 to 31.

Intigriti News



Intigriti's 0521 XSS challenge – by @GrumpinouT

Meet the hacker: p4fg, the Swedish master of Automation

Our favorite 5 hacking items

1. Tutorial of the week

Adventures into HTTP2 and HTTP3

This is an excellent introduction to the different HTTP specifications. @JCoertze took a look at HTTP/1.x, HTTP/2 and HTTP/3, their differences and what they mean in terms of security. With the increasing adoption of HTTP/2 and HTTP/3, it is essential for Web app testers to learn how they work and their risks.

2. Writeups of the week

AppCache's forgotten tales (Google, $10,000)
CVE-2021-33564 Argument Injection in Ruby Dragonfly

@lbherrera_ delved into the security of Chrome's AppCache before its deprecation and found two ways to leak sensitive information cross-origin. This is a great example of building on existing research to come up with new attacks.

ZX Security researchers discovered an argument injection vulnerability in the Ruby Gem Dragonfly, an image handling library used by multiple CMSs. Though it was possible to inject arguments, the library had filters against LFI and the usual command injection payloads. Remote code execution was achieved by exploiting ImageMagick's convert utility.
This writeup is full of details on techniques tried that both worked and didn't work, and interesting ImageMagick hacks.

3. Article of the week

Playing With Imagetragick Like It's 2016

While we're on the subject of ImageMagick, this article by @loadlow and @alexisdanizan covers interesting techniques to exploit it and obtain arbitrary file read and write. It focuses on the latest version available on Debian Buster repositories which is a legacy version.
The exploitation vectors mentioned are worth remembering the next time you're testing a file upload functionality.

4. Conference of the week

NorthSec 2021 Conference Day 1, Day 2, Schedule & Introduction to fuzzing, especially: You are not an idiot & Slides

There are so many interesting talks in this NorthSec edition, on all kinds of topics: GraphQL hacking, repo jacking, request smuggling, burnout, crypto best practices and many more.
@angealbertini's keynote in particular is of high relevance to hackers. It touches on difficulties a lot of us in InfoSec face including failure, burnout, imposter syndrome, manipulation, suicide... and how to protect ourselves.

5. Resource of the week

Mobile Nuclei Templates

Did you know Nuclei can also be used for mobile app tests? Its File requests feature allows you to check local files using matching/extracting. This makes it possible to use for finding dangerous patterns in mobile apps.
This repository provides good examples to get started with this type of scans.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- SecuriTEA & Crumpets – Episode 7 – Dr.-Ing. Mario Heiderich – DOMPurify
- How not to implement AWS S3 signed URLs? $25,000 bounty
- Security Shorts EP01 with Harsh Bothra, EP03 with Somdev Sangwan & EP05 with Chloé Messdaghi
- Learn with @Shre_yy : Managing Bug bounty and learning !!
- Interview With H13- : #1 Bug Bounty Hunter On Shopify | Methodology, Mistakes, Tips & More...

Podcasts

- Epsilon Red – Chrome 91, Emsisoft's Ransomware Decryption Tool, Revisiting Amazon Sidewalk

Webinars

- BHIS | Getting Started in Pentesting The Cloud: Azure | Beau Bullock (1-Hour) & Slides

Conferences

- Mayhem 2021 & Portuguese Track
- HITBSecConf2021 – Amsterdam: MAIN TRACK 1 – Day 2, MAIN TRACK 2 – Day 2, COMMSEC TRACK – Day 2, Agenda & Slides
- IEEE Security & Privacy 2021 & Slides

Tutorials

- Supercharge Your Bash Scripts with Multiprocessing
- Abusing LNK "Features" for Initial Access and Persistence
- WAF Fuzzing with Burp Intruder
- How To Make Sure Your Antivirus Is Working Without Any Malware
- Burp Macros: What, Why & How?
- Accessing Windows Systems Remotely From Linux
- HTTP Parameter Pollution (HPP)

Writeups

Challenge writeups

- Solution for the MessageKeeper challenge from Pwn2Win 2021

Pentest writeups

- A Red Team Operation Leveraging a zero-day vulnerability in Zoom

Responsible(ish) disclosure writeups

- Attacks on PDF Certification #PDF
- Write-up: Plone Authenticated RCE (CVE-2021-32633) #Web
- Overwolf 1-Click Remote Code Execution – CVE-2021-33501 #Web
- D-Link Router CVE-2021-27342 Vulnerability Writeup #Router
- My RCE PoC walkthrough for (CVE-2021–21974) VMware ESXi OpenSLP heap-overflow vulnerability #MemoryCorruption
- CVE-2021-21985 #RCE #VMware
- Fuzzing HTTP Proxies: Privoxy, Part 1 #MemoryCorruption #Fuzzing

Bug bounty writeups

- Bypassing restricted port protection in WebKit (Apple)
- How I hacked a Target again and again...
- The beauty of chaining client-side bugs
- Path Traversal in MobileSafari (Apple)
- Security: leak cross-site response size – countermeasure bypass (Google Chromium, $3,000)
- runc mount destinations can be swapped via symlink-exchange to cause mounts outside the rootfs (CVE-2021-30465) (Google)
- Bypass apiserver proxy filter (Kubernetes, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- ReServ: A set of simple servers (currently HTTP/HTTPS and DNS) which allow configurable and scriptable responses to network requests
- bnew: A more performant implementation of @TomNomNom's anew utility

- getAllParams.py: Burp extension that parses an already crawled sitemap to build a custom parameter list
- macOCR: Get any text on your screen into your clipboard
- UserWritableLocations.ps1 & Intro: A PowerShell script for finding writable folders and hijackable DLLs

Tips & Tweets

- Authentication bypass by entering wrong OAuth scope
- TIL: @CorelliumHQ arz offering free trials of their platform for security researchers
- Cracking NetNTLMv1/v2 using NT hashes with Hashcat
- @hakluke's flow for bug bounty success

Misc. pentest & bug bounty resources

- Browser Security Enhancement Tracker Project & Intro
- File Upload Vulnerability Tricks And Checklist
- Just some web hacking tools
- Rubyfu
- List of Cybersecurity Subreddits
- Attacking Active Directory: 0 to 0.9

Challenges

- Intigriti's 0521 XSS challenge – by @GrumpinouT
- Secure Developer Challenge: May '21
- InsecureShop: An Intentionally designed Vulnerable Android Application built in Kotlin
- ThreadsApp – A Vulnerable Web Application Lab

Articles

- Method Invocation in Go's builtin template modules lead to file read and RCE. #Web
- Taking Over Renamed GitHub Account Repositories
- Rm -rf is the root of all evil
- Abusing and Detecting LOLBIN Usage of .NET Development Mode Features #RedTeam

- The Attack Path Management Manifesto #RedTeam
- Saving Your Access #RedTeam

Bug bounty & Pentest news

- How Bugcrowd Sees Vulnerability Disclosure Programs And Points
- Upcoming events:
  - Pre-registration for DEF CON 29 is open + Price chart
  - Security BSides Athens 2021
- Tools updates
  - SecLists 2021.2
  - LoggerPlusPlus v3.19
  - Amass v3.13.0
  - Burp Professional / Community 2021.6 (brings back the hex view in the message editor)
  - httpx v1.0.7 (new follow-redirects flag to see destination URLs in the CLI output)
  - Proxify v0.0.4
  - New Impacket features
  - CrackMapExec updated with 3 new modules

Non technical

- Meet the hacker: p4fg, the Swedish master of Automation
- Spotlight On The Server-side
- Infosec Bugbounty AMA with Infosec Community
- The Full Story of the Stunning RSA Hack Can Finally Be Told
- Linux Command Line Tool Flags Standard

Community pick of the week

A warm welcome to @hacksplained who joined Intigriti this week!

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!

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com