Bug Bytes #127 – IPv6 for recon, OpenID 2FA bypass & New threats of Service Workers Caches

BY ANNA HAMMOND · JUNE 16, 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 7 to 14.

Intigriti News

Community Code of Conduct

Intigriti's new Community Code of Conduct

Illustrating Hackers: Changing perceptions by changing how we see hackers

Our favorite 5 hacking items

1. Webinar of the week

How to Analyze Code for Vulnerabilities

I know a bug hunter who earned thousands of bounties by focusing on source code review on a single target. He'd ask for demos of apps and perform code review on them. I was shocked when I heard this as at that time the black box approach seemed to be the most common and at first glance the target's main asset was just a Web app. This illustrates how effective code reviews can be.

If you want to acquire this skill, this webinar is an excellent start. @vickieli7 does an amazing job of explaining how to get started and what to focus on.

2. Writeups of the week

Exploiting outdated Apache Airflow instances ($13,000)
Bypassing 2FA using OpenID Misconfiguration

@iangcarroll discovered vulnerabilities in Apache Airflow and automated testing for them and for an old public CVE on bug bounty programs. The first writeup details this research and how it resulted in $13,000 bounties.

The second writeup is a great read for anyone interested in 2FA bypass or OpenID security. @justinBB shows an interesting OpenID misconfiguration that can be used to bypass 2FA.

3. Tutorial of the week

The JavaScript Bridge in Modern Desktop Applications

When I hear about escalating XSS to RCE, the first thing I think about is: It must be an XSS in an Electron app. This tutorial shows that there are other frameworks used for developing Desktop apps that allow for escalating XSS to RCE, with concrete examples.

4. Conferences of the week

Improving Internet Wide Scanning with Dynamic Scanning & Active Scanning Techniques repo
WOOT 2021, especially: The Remote on the Local: Exacerbating Web Attacks Via Service Workers Caches, Slides & Paper/demo/PoC

These talks both introduce very interesting research. The first one is about several strategies for discovering assets. Some of them you might've heard about, but others like IPv6 scanning are less known. The second talk shows how the Cache API can be exploited to elevate the impact of vulnerabilities like XSS, allowing for a new class of attacks.

5. Resource of the week

Subdomain Enumeration Guide

This is a cool GitBook on subdomain enumeration. With the growing number of tools and techniques being published, it's nice to have this reference that sums up the most commonly used ones.
It's also a good introduction for anyone just starting out.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- How I take notes with Notion for learning and #ctf challenges
- Tips To Get A Job In Cybersecurity!
- $50,000 0-day RCE on Apple bug bounty program
- Security Shorts EP 06 | Talking Security with LiveOverflow
- Finding Buffer Overflow with Fuzzing
- API hacking with postman
- Fuzzing Web Applications with Jaeles Scanner

Podcasts

- TLS Confusion Attacks – TikTok Privacy, iOS 14.5 Tracking Permission, Industry-Wide Patch Tuesday

Webinars

- Advanced Web Application Penetration Testing JWT Security Issues & Slides
- Walking Your Dog In Multiple Forests – Breaking AD Trust Boundaries Through Kerberos Vulnerabilities

Conferences

- IoT Village Virtual Event 2.0

Tutorials

Medium to advanced

- The JavaScript Bridge in Modern Desktop Applications
- Proxy Windows Tooling via SOCKS
- Ordinal Values, Windows Functions, and C#
- Don’t use commands, use code: the tale of Netsh & PortProxy

Beginners corner

- 10 Most Common Security Issues Found in Login Functionalities

- Testing Two-Factor Authentication
- Secrets Scanning with Nuclei
- Hacker tools: Nmap – Next level port scanning
- I got 99 problems but my NAC ain´t one
- Updating Mimikatz in Metasploit
- Kerberoasting Attacks Explained: Definition, How They Work and Mitigation Techniques

Writeups

Challenge writeups

- @J0_mart's methodology during Firstblood
- SQL Injection – Lab #11 Blind SQL injection with conditional responses #video

Pentest writeups

- Rediscovering N Days: PAM360 information disclosure
- IDOR (Insecure Direct Object Reference)

Responsible(ish) disclosure writeups

- Privilege escalation with polkit: How to get root on Linux with a seven-year-old bug #Linux #LPE
- Jetty Utility Servlets ConcatServlet Double Decoding Information Disclosure Vulnerability #Web
- Abusing SIP for Cross-Site Scripting? Most definitely! #SIP #Web
- The walls have ears #IoT #RCE #MemoryCorruption
- About the Unsuccessful Quest for a Deserialization Gadget (or: How I found CVE-2021-21481) #Web
- So Many Ways to Own Dell EMC Networker #RCE #Network
- imCMS 4.3.7 – Multiple Vulnerabilities #Web

N-day vulnerabilities

- CVE-2021-31181: Microsoft Sharepoint Webpart Interpretation Conflict Remote Code Execution Vulnerability

Bug bounty writeups

- This is how I was able to see Private, Archived Posts/Stories of users on Instagram without following them (Facebook, $30,000)

- GitLab Arbitrary File Read & Write through Kroki – CVE-2021-22203 (GitLab, $5,600)
- Two weeks of securing Samsung devices: Part 1 (Samsung, $20,690)
- Stealing tokens, emails, files and more in Microsoft Teams through malicious tabs (Microsoft)
- Attacker can obtain write access to any federated share/public link (Nextcloud, $4,000)
- Hackerone is not properly deleting user id (HackerOne, $2,500)

See more writeups on The list of bug bounty writeups.

Tools

- mobsfscan: A static analysis tool that can find insecure code patterns in your Android and iOS source code
- Burpa: Burp Automator – A Burp Suite Automation Tool. It provides a high level CLI and Python interfaces to Burp Suite scanner and can be used to setup Dynamic Application Security Testing (DAST)
- purl: A Go script to proxy URLs from stdin through any HTTP proxy tool very quickly for analysis
- showSSID: Python tool that Generates continuous probe requests to identify hidden SSIDs
- SMERSH: A pentest oriented collaborative tool used to track the progress of your company's missions
- StandIn: Small .NET35/45 AD post-exploitation toolkit

Tips & Tweets

- An easily-overlooked vector for request smuggling attacks
- What to do with a blind SSRF that can only read images
- Piping lists into ffuf
- Burl or how to Curl through Burp
- Strict CSP + Perfect Types can't mitigate template gadget
- What makes you want to hack on a company/bug bounty program?

Misc. pentest & bug bounty resources

- Can I Take Over DNS?
- rockyou2021.txt – A Short Summary (Download Included)
- How To: Find WordPress Plugin Vulns
- BloodHound Cheat Sheet

Challenges

- New H1 CTF level: RTFM
- That's The Ticket (TryHackMe free room by adamtlangley) & Video writeup

Articles

- Decrypting VEEAM Passwords
- ALPACA Attack
- Phishing for AWS credentials via AWS SSO device code authentication
- Active Directory forest trusts part 2 – Trust transitivity and finding a trust bypass & Video
- Hacking Unity Games with Malicious GameObjects
- On how to access (protected) networks

Bug bounty & Pentest news

- CVE board slams Distributed Weakness Filing project for publishing 'unauthorized' CVE records
- Upcoming events:
  - Pwncon (June 19)
  - BSides Munich 2021 (June 20-22)
  - null Ahmedabad Meet 20 June 2021 Monthly Meet RSVP (Featuring a New GraphQL attack by @s0md3v, on June 20)
- Tool updates:
  - Burp Professional / Community 2021.6.1
  - bbrf.me now defaults to a demo server
  - ReconFTW v1.7.2
  - Impacket Release v0.9.23

Non technical

- How do bug bounty hunters use GitLab to help their hack?
- How Hackers Used Slack to Break into EA Games
- (Technical) Infosec Core Competencies

Community pick of the week

Woohooo! Amazing, enjoy your ride @dewcode91!

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