Bug Bytes #104 – Cache poisoning DoS, Burp themes & A couple of Facebook account takeovers

BY ANNA HAMMOND · JANUARY 6, 2021 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-104-cache-poisoning-dos-burp-themes-a-couple-of-facebook-account-takeovers

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.

This issue covers the week from 27 of December to 03 of January.

Intigriti News

> **Thank you @intigriti for these awesome awards. Your live-events are truly the best out there. Big thanks to my fellow team members @arneswinnen and @honoki! These wouldn't have been possible without them. Very proud to have earned both the best hacker & best team award! pic.twitter.com/qPaaiFJgfd**
>
> **— MattiBijnens (@MattiBijnens) December 30, 2020**

Congratulations to @MattiBijnens for winning four awards in our last Live Hacking Event!

SolarWinds authentication bypass, Corellium win for hackers & 2020 security retrospective

Our favorite 5 hacking items

1. Tools of the week

Burp Customizer
Lilly

ote (One Time Email)
BurpRequestCleaner

Here is a bunch of fantastic new tools you might find very useful!
@CoreyD97's Burp Customizer is a Burp extension that provides 58 new themes to customize Burp.
Lilly by @Dheerajmadhukar leverages favicon hashes to help find the real IP behind CDNs/WAFs.
@s0md3v's ote allows you to quickly generate temporary email addresses and get OTPs or confirmation links directly in your terminal.
Finally, BurpRequestCleaner by @StaticFlow is a Burp extension that redacts potentially sensitive information (e.g headers & parameters) using Shannon Entropy analysis. This is useful when you want to take and share screenshots without revealing your passwords or data.

2. Writeups of the week

Cache-Key Normalization – What could go wrong?
XSS on forums.oculusvr.com leads to Oculus and Facebook account takeovers (Facebook, $30,000)
Bad regex used in Facebook Javascript SDK leads to account takeovers in websites that included it (Facebook, $10,000)

The first writeup is about a new Denial of Service technique. @iustinBB leveraged Web cache poisoning to force a server to return 404 errors for existing pages, which is basically a DoS. A pretty smart and a very well explained finding!

The second writeup is about an account takeover @samm0uda found on Facebook. He discovered an XSS in an out of scope domain that can be chained with two other bugs to take over Oculus and Facebook accounts.

The last finding is also by @samm0uda. Web applications using the Facebook JavaScript SDK were vulnerable to information leaks and account takeovers because of a bad regex in the SDK's cross-origination communication checks.

3. Conference of the week

Digital OWASP AppSec Israel 2020

Here's a nice set of talks on a variety of Web security related topics: practical techniques to find bugs in GraphQL APIs, mutation XSS, Android hacking, CSP, race conditions, Web fuzzing, browser storage, etc.

4. Video of the week

Ziot Talks About Hacking Apple, Collaboration, Recon, and Getting Started in Hacking!

This is a cool interview with Brett Buerhaus (aka ziot aka @bbuerhaus)! @NahamSec and him chat about the usual topics, his background, bug bounty collaboration, recon, mentorship, bug hunting stories, imposter syndrome, etc. If you want to relax while getting inspired to hack, this is the perfect thing to watch.

5. Tutorial of the week

The Burp Extension No One Told You About & Burp-Send-To-Extension

burp-send-to is a Burp extension that allows you to send requests to any command line tool. If this reminds you of something, it might be piper but the two extensions work differently. Piper allows to run CLI tools and view the results inside Burp, while burp-send-to runs tools in a terminal. It saves you the

hassle of copy-pasting requests from Burp to the terminal when you want to pass them to tools like sqlmap or ffuf.

Since burp-send-to when unnoticed when released, @fyoorer is sharing how he uses it and why you may want to!

Other amazing things we stumbled upon this week

Videos

- What Operating System do I need to hack?
- Pentest / Red Team Audit Logging
- Why Is Validating URLs So Hard?
- Cool Features of the DuckDuckGo Search Engine
- {{SSTI}} From Developing Side
- Server-Side Template Injection Workshop
- My Learning Workflow as a Developer & Content Creator

Podcasts

- Darknet Diaries Ep 82: Master of Pwn
- Security Now: Sunburst & Supernova – Ransomware Task Force, Chrome 87, Firefox Caches, Preserving Flash Video & SolarBlizzard – SolarWinds' Orion Software, Swatting Goes IoT, PHP Zend Framework Vulnerability
- Risky Business #609 — It's not NotPetya
- Kubernetes Clusters, Microsoft Solarigate, & Apple's Security DIY – ASW #135
- ElectroRAT, Zyxel Vulnerability, Ticketmaster, & Section 230 – SWN #91
- Cyber Security Saun 048| The Year in Cyber: 2020

Webinars & Webcasts

- Offensive Recon – Bug Hunter's Playbook & Slides
- SEC554: Blockchain And Smart Contract Security – How To Lose $280 Million With A Single Line Of Code

Conferences

- Hackfest Holidays 2020, especially:
  - Hacking Android & iOS apps with Deep Links and XSS

- Remote Chaos Experience
- OWASP IL Meetup 2020

Tutorials

Medium to advanced

- Exploring Nmap #1: Automating the process of decoy scanning and source spoofing
- Bypassing Windows protection mechanisms & Playing with OffensiveNim
- Bypassing User-Mode Hooks and Direct Invocation of System Calls for Red Teams

Beginners corner

- Finding The Origin IP Behind CDNs
- Burp Suite for Pentester: Turbo Intruder
- OSINT – Scraping Deep Web Databases with Python
- Make Your Own Internet Archive With Archive Box

Writeups

Responsible(ish) disclosure writeups

- Solarwinds_Orion_LFD local file disclosure PoC #Web
- Tenda Malformed HTTP Request Header Processing Vulnerability #Routers
- Latest Joomla Exploit 'CVE-2020-35616' – Joomla ACL Security Vulnerabilities #Web
- CVE-2020-35489: Unrestricted File Upload Vulnerability found in Contact Form 7 plugin affects 5M+ websites #Web

Bug bounty writeups

- Sensitive data leak using IDOR in integration service
- Expose the email address of Workplace users (Facebook, $5,000)
- Read-only application can publish/delete fleets (Twitter, $7,700)
- Chromium Issue 1116280: Self-XSS / Crash via window.open and delayed navigation (Google, $5,000)
- Patch. Bypass. Repeat: Story of a FaceBook Page Admin Disclosure bug worth $5000 (Facebook, $5,000)

See more writeups on The list of bug bounty writeups.

Tools

- Burp Customizer: Because just a dark theme wasn't enough!
- ote (One Time Email): Generate Email, Register for anything, Get the OTP/Link
- burp-piper-custom-scripts
- Mapper: A tool to help the distributed scannning of hosts
- BurpRequestCleaner: Burp extension that redacts potentially sensitive header and parameter values from requests using Shannon Entropy analysis
- blackrock-go: Golang port of the BlackRock cipher from the Masscan project
- Clairvoyance: Obtain GraphQL API schema despite disabled introspection!
- Lilly: Tool to find the real IP behind CDNs/WAFs like cloudflare using passive recon by retrieving the favicon hash. For the me hash value, all the possible IPs, PORTs and SSL/TLS Certs are searched to validate the target in-scope.
- Javascript security analysis (JSA): A program for javascript analysis
- Eyeballer Pytorch version: A reimplementation of Bishop Fox's Eyeballer in PyTorch
- Tamper DEV / Tamper Chrome: Extension by Google that allows you to intercept and edit HTTP/HTTPS requests and responses as they happen without the need of a proxy. Works across all operating systems (including Chrome OS).
- Soxy: Multi-threaded socks proxy checker written in Go!
- bountyRecon v2: Framework to automate Bug Bounty Reconnaissance
- OpenCVE: Platform that alerts you about new vulnerabilities related to the CVE list (formerly known as Saucs)
- ctf-collab: Create a collaborative programming environment inside GitHub Actions – like Google Docs for hacking competitions

Misc. pentest & bug bounty resources

- Why is Turbo Intruder slow?
- Search engine for cloud storages/buckets by @nightwatchcyber
- Web-Attack-Cheat-Sheet
- Public release: Android Security Repository
- Top 10 Most Critical CVEs Added in 2020
- Cybersecurity & Tech Content I Discovered in 2020
- So You Want To Be A Hacker: 2021 Edition
- Default Credentials Cheat Sheet

- Humble Book Bundle: Cybersecurity & Cryptography By Wiley

Challenges

- Vulnerable Kext: A WIP "Vulnerable by Design" kext for iOS/macOS to play & learn *OS kernel exploitation
- 2020 OSINT Quiz
- SSD Secure Disclosure 2nd December – 2020 challenge

Articles

- The Story of the Million Dollar Bounty
- Deep Dive into Site Isolation (Part 2)
- Cast me an alert(1)
- Breaking the Google Audio reCAPTCHA with Google's own Speech to Text API
- Bring Your Own VM – Mac Edition
- IoT Security – Part 21 (Famous IoT Attacks & Vulnerabilities)
- Spoofing JARM signatures. I am the Cobalt Strike server now!

Bug bounty & Pentest news

- Survey on reliability of CVSS (30 min on average)
- FortyNorth Half Price Training Competition
- Metasploit 2020 Wrap-Up
- Top 10 web hacking techniques of 2020 – nominations open
- Burp Suite user survey

Non technical

- Around the World in 2021 Hacker Predictions
- How can you benefit by sharing your knowledge?
- Learning from your mistakes as an offensive security professional
- 100 Tips for a Better Life
- Kali Linux + Mr. Robot ARG Society
- My quest to project Undeniable Competence

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 12/27/2020 to 01/03/2021.