Bug Bytes #153 – New PHP LFI technique, Cache poisoning at scale & Null byte attacks are still alive!

BY ANNA HAMMOND · JANUARY 5, 2022 · 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 December 20, 2021 to January 03, 2022.

Intigriti news

Visma's "Mother of Hackers" speaks to Intigriti about running a successful virtual live hacking event

Our favorite 5 hacking items

1. Article of the week

PHP LFI with Nginx Assistance

Bruno Bierbaumer discovered a new LFI technique while creating CTF challenges.
The conditions is that the app is deployed with PHP-FPM and Nginx, and Nginx runs as the same user as PHP. Both are very common.

The attack exploits temporary files that Nginx creates for buffering. A GET request for a non-existent page, with a huge parameter value will force Nginx to create a temporary file containing that value.
The attack, basically, is to put a PHP shell in that parameter, then bruteforce Nginx's temporary file names/paths to find the one where the web shell was written before its deletion. Reading it will execute the shell and result in RCE.

If you want to practice, there are links to two challenges, and to an additional example in the article.

For an additional explanation of the technique, you can also check out this CTF writeup.

2. Writeups of the week

Cache Poisoning at Scale
Turning bad SSRF to good SSRF: Websphere Portal

@iustinBB shares the techniques he used to find and report more than 70 web cache poisoning vulnerabilities, for about $40,000 bounties. This is amazing research if you want to know more about this topic.

@assetnote's writeup is a great read if you are interested in SSRF, Open redirect, XXE or RCE via Zip Based Directory Traversal. It is full of details not only about the vulnerabilities but, most importantly, the process for finding them (code review, failed attempts, etc).

3. Video of the week

Multi-host payloads in Burp Intruder

If you are a Burp user, there is a great feature that was added in a recent update that is worth knowing. Starting Burp Pro and Community 2021.12, it is possible to run a single Intruder attack against several hosts.
The video demonstrates how to do that, with the example of a login brute force attack run against different subdomains.

4. Tool of the week

Osmedeus Next Generation & Documentation

@j3ssiejjj completely rewrote Osmedeus and this new version looks lit. It allows you to write custom recon workflows using YAML files.
If you are looking for a way to efficiently organize your recon process, leveraging both custom and public tools / wordlists, with multiple workflows, Osmedeus might be what you need.

5. Tweet of the week

Mini writeup of Instapage and HubSpot vulnerabilities

@samwcyo shares a couple of interesting vulnerabilities discovered by him, @bbuerhaus, @sshell_ and @xEHLE_ on Hubspot and Instapage.
They discovered a legacy API that allowed uploading HTML files to Hubspot's CDN, exploited it to serve XSS payloads, and coud steal HTTPOnly cookies using a diagnostics endpoint that reflects all cookies.
The other bug is that any Instapage live domain could be claimed by registering a domain with the same name to which you append a null byte. Null byte attacks are still alive!

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Log4j Lookups in Depth // Log4Shell CVE-2021-44228 – Part 2
- Interactive Pentest by @infinitelogin
- The (Hacker YouTuber) Grift is Real
- Breaking Into Buildings Is Way Too Easy (A Hacker's Physical Pentest Toolkit)
- Insanely fast parameter enumeration! Arjun – Hacker Tools
- Attacking Active Directory – GPP Credentials
- Ethical Hacking in 12 Hours – Full Course – Learn to Hack!

Webinars

- OWASP Timisoara #20 – AI, Bug Bounty & Web Fuzzing

Conferences

- KringleCon 2021
- HITBCyberWeek 2021 – Hack Track, Break Track, Make Track & Build Track
- Bsides London 2021 Rookie Track, Clappy Monkey Track & Track 2

Tutorials

- Ultimate Reconnaissance RoadMap for Bug Bounty Hunters & Pentesters
- Console Wars Part 1: Hacks for Hackers & Part 2: SQL injection
- Subdomain Takeover Via Flywheel
- How To Get Hacked By Accidentally Copy Pasting
- How to leverage security frameworks and libraries for secure code

Writeups

Challenge writeups

- Hacker Simulator Walkthrough series
- Homoglyph XSS?! Solution to December '21 XSS Challenge

- Bugv CTF Writeup – Pwning Thawang Shield
- UHC – LogForge
- What is Directory Traversal? & Advanced Directory Traversal Techniques!

Pentest writeups

- Bypassing HttpOnly with phpinfo file
- Inside A PBX – Discovering A Firmware Backdoor

Responsible(ish) disclosure writeups

- How I found (and fixed) a vulnerability in Python #Web
- Proctorio Chrome extension Universal Cross-Site Scripting #BrowserExtension #Web
- Yes, fun browser extensions can have vulnerabilities too! #BrowserExtension #Web
- Phishing With Spoofed Cloud Attachments #Cloud #Phishing
- Where's the Interpreter!? (CVE-2021-30853) #MacOS

Bug bounty writeups

- Fixing the Unfixable: Story of a Google Cloud SSRF (Google, $4133.70)
- MS Teams: 1 feature, 4 vulnerabilities (Microsoft)
- NotLegit: Azure App Service vulnerability exposed hundreds of source code repositories (Microsoft, $7,500)
- Bounty Evaluation GitHub = $15,000 US Dollars | Rate Limit (GitHub, $15,000)
- Bug Hunting Journey of 2021
- Here's How I Could Read Anyone's Apple ID Metrics Remotely. (Apple)
- Story of a weird CSRF bug

See more writeups on The list of bug bounty writeups.

Log4J

- CVE-2021-44832 – Apache Log4j 2.17.0 Arbitrary Code Execution Via JDBCAppender Datasource Element: New variant of Log4J
- Another Log4j on the fire: Unifi & Log4jUnifi
- How to exploit Log4j vulnerabilities in VMWare vCenter & Log4jCenter
- Exploiting CVE-2021-44228 using PDFs as delivery channel – PoC

- AWS/Cloudfront WAF bypass
- Log4J 2.15 TOCTOU Vulnerability Illustrated by GoSecure Researchers
- Examining Log4j Vulnerabilities in Connected Cars and Charging Stations
- Why we haven't seen a Log4j worm yet
- Google: Understanding the Impact of Apache Log4j Vulnerability
- google/log4jscanner

Tools

- Sourcerer: Ruby utility to apply rules to URL datasources and filter interesting content
- fq: jq for binary formats
- elasticpwn & Intro: Quickly collect data from thousands of exposed Elasticsearch or Kibana instances and generate a report to be reviewed
- vortex: All-in-one tool to attack Microsoft OWA/ADFS/LYNC/O365, vendor specific VPN Web Logins and more
- Needle & Intro: A Python tool to find Windows registry files in a blob of data
- ADExplorerSnapshot.py: An AD Explorer snapshot ingestor for BloodHound

Tips & Tweets

- @osiryszzz's idea for exfiltrating data using blind SSRF
- How to see the issues (in Burp) pertaining to a specific set of hosts
- Quickly detect CVE-2021-45232 Apache APISIX Dashboard Unauth Vulnerability using fofax and httpx
- Tips for beginner bug hunters:
  - @Samm0uda: Learn and read a lot, apply by doing serious CTFs and labs for some time then do VDP hunting then do Bug Bounty Hunting. Focus on quality/severity over quantity. Do what no one is doing.
  - @jtcsec: Build a repeatable methodology for your target. Do a lot of content discovery. Watch videos from people like @InsiderPhD and @stokfredrik. Practice on @bugbountyhunt3r.
  - @mcipekci: Do not rely on automated scans, do not run default configurations and create your own methodology. It's not just about 0-days, very old issues are often found on targets.
  - @nnwakelam: Go through @PentesterLab and get curious from there. Read writeups from people like @samwcyo and @infosec_au.
  - @nnwakelam: Learn to be persistent.

Misc. pentest & bug bounty resources

- Top 20 bug bounty YouTube channels to follow in 2021!
- rahulbhichher/SourceCodeReview
- learngo: A Huge Number of Go Examples, Exercises and Quizzes
- Reverse Engineering For Everyone!

Articles

- Fuzzing for XSS via nested parsers condition
- Attacking Java RMI via SSRF
- Fun with Cypher Injections
- Cloud Security Breaches and Vulnerabilities: 2021 in Review
- Responder and IPv6 attacks

Challenges

- xss.pwnfunction.com (with source code)
- ctf-mystiko.com (24x7x365 CTF)

Bug bounty & Pentest news

- Bug bounty
  - Bug bounty platforms handling thousands of Log4j vulnerability reports
  - Ask TomNomNom Anything
- Cybersecurity
  - State-of-the-art EDRs are not perfect, fail to detect common attacks
  - Security done right: Celebrating infosec wins in 2021
  - Swig Security Review 2021 – Part I & Part II
- Tool updates
  - PowerZure 2.1 Update

Non technical

- Free PDF journals by @InsiderPhD
- What to Do Instead of New Years Resolutions

- A Different Kind of Root – How a Dentist Passed the OSCP