Bug Bytes #142 – Weird Google bugs, SAML padding Oracle & Apache path traversal continued

BY ANNA HAMMOND · OCTOBER 13, 2021 · LAST UPDATED ON JULY 16, 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 October 4 to 11.

Our favorite 5 hacking items

1. Conference of the week

4 Weird Google VRP Bugs in 40 Minutes – Hacktivity 2021

@xdavidhu talks about four vulnerabilities he found in Google products. This is a great watch if you like weird but very creative bugs (or video over written writeups).

2. Writeup of the week

SAML Padding Oracle

Compass Security researchers discovered a padding Oracle vulnerability in the SAML login flow of ArcGIS. They were able to decrypt an encrypted assertion, and use an XSW4 attack and the oracle to reencrypt and login as other users.

3. Vulnerability of the week

Apache advisory for CVE-2021-42013

Remember last week's CVE-2021–41773, a zero-day path traversal in Apache HTTP Server? It turns out it is also an RCE if mod-cgi is enabled, and the fix was incomplete which led to CVE-2021-42013. Here is a meme that sums it up, a Docker Playground and a couple new PentesterLab exercises to practice, as well as a Nuclei template for CVE-2021-42013 for automation.

4. Tips of the week

Use an array to bruteforce OTP without triggering rate limiting
HTTP header bruteforce

@EnesSaltk7 shared a creative idea that allowed them to bypass email verification and could be useful in other contexts too. They replaced the code for email verification (passed via JSON post data) with an array of codes. So, it is a way of bruteforcing codes with a single request, without triggering rate limiting.

Another handy tip by @nnwakelam is to bruteforce custom HTTP headers like x-FUZZ and x-FUZZ-internal. Also, keep a look at response lengths and status codes as they may indicate that you have found valid headers.

5. Tools of the week

Ghostinthepdf
reFlutter

Ghostinthepdf is a tool that embeds GhostScript exploits into PDF files that bypass signature checks. It can be used to first detect that a target is actually using GhostScript for PDF processing, then to run exploits against it.
Also, if you haven't seen @emil_lerner's previous work on GhostScript, it is worth checking out to see the type of vulnerabilities that he found with this tool.

Another helpful tool is @Impact_I's reFlutter, a framework for reverse enginnering Flutter apps. It can be used to repack Flutter apps and make them trust installed certificates, so you can intercept their traffic (without root).

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Automatic Vulnerability Scanner! Nuclei – Hacker Tools
- Nessus / Vulnerability scanning series by @HackerSploit
- Staying Sane in Cybersecurity – Dealing with Burnout and Stress & Accompanying blog post
- Video Essay about the Security Creator Scene

Podcasts

- Day[0]: SharePoint RCE & an Apache Path Traversal [Bounty Hunting Podcast]
- Radio Hack Ep6: Offensive Security – Mohammad Askar (in Arabic)

Webinars

- Detect complex code patterns using Semgrep
- CSAM 2021 – Secure Coding Standards : Avoiding Mistakes And Correct Them

- SANS Workshop – Reflection in C#

Conferences

- SnykCon 2021
- Practical Mobile App Attacks by Example

Slides & Workshop material

- JavaScript for Hackers & JavaScript for Hackers 2

Tutorials

Medium to advanced

- Hunting for Prototype Pollution and it's vulnerable code on JS libraries
- AWS Access Keys – A Reference
- Never put AWS temporary credentials in the credentials file (or env vars)—there's a better way
- Persistence Through Service Workers—part 1: Introduction And Target Application Setup & Part 2: C2 Setup And Use
- Offensive BPF

Beginners corner

- Practical strategies for exploiting FILE READ vulnerabilities
- DNS Records and Record Types: Some Commonly Used, and Some You Might Not Know About
- Testing Methodology for Insecure Deserialization Vulnerability
- GraphQL Security: The complete guide

Writeups

Challenge writeups

- SnykCon CTF – "Invisible Ink" Prototype Pollution, Sauerkraut – Python Pickle Vulnerabilities & "Random Flag Generator" Weak PRNG Seed
- CSRF – Lab #6 CSRF where token is duplicated in cookie

Pentest writeups

- Beyond SSTI

Responsible(ish) disclosure writeups

- Reverse engineering and decrypting CyberArk vault credential files #Crypto
- Misconfigured Airflows Leak Thousands of Credentials from Popular Services #Web
- 23andMe's Yamale Python code injection, and properly sanitizing eval() #Web
- Swimming Upstream: Uncovering Broadcom SDK Vulnerabilities from Bug Reports. #MemoryCorruption

0-day & N-day vulnerabilities

- PHP 7.0-8.0 disable_functions bypass [user_filter]
- CVE-2019-9053
- Bindiff and POC for the IOMFB vulnerability, iOS 15.0.2 (CVE-2021-30883) (Apple)

Bug bounty writeups

- How I got access to many PIIs through a source code leak
- Accessing Apple's internal UAT Slackbot for fun and non-profit (Apple)
- Stumbling across a DOM XSS on google.com (Google)
- [EN] Stored XSS in the administrator's panel due to misuse of MarkupSafe (pass Culture)
- Hacking Netflix Eureka!
- Zero-Day: Hijacking iCloud Credentials with Apple Airtags (Stored XSS) (Apple)
- CVE-2021-26420: Remote Code Execution In Sharepoint Via Workflow Compilation (Microsoft)
- Improper Validation at Partners Login (Zomato, $2,000)

See more writeups on The list of bug bounty writeups.

Tools

- vCenter SAML Login Tool & Intro: A tool to extract the IdP cert from vCenter backups and log in as Administrator
- kdigger & Intro: A context discovery tool for Kubernetes
- ReDoSHunter & Paper: A Combined Static and Dynamic Approach for Regular Expression DoS Detection

Tips & Tweets

- Use Get + Range header for fast fuzzing
- Trusted Types in jQuery

- SSTI to RCE using tplmap and requestbin
- ESI injection WAF bypass
- 403 bypass using %03 %08 %10 %83 etc

Misc. pentest & bug bounty resources

- pwny.cc & Repo
- Secure Coding Handbook & Repo
- snyk Learn
- 0xAwali's methodology for testing Request Smuggling & Privilege escalation
- iOS Pentesting / Hacking
- weakpass_3a
- initstring/passphrase-wordlist

Challenges

- soXSS challenge
- HTB University CTF (November 19-21)

Articles

- Protect Your GitHub Actions with Semgrep
- Safe DOM manipulation with the Sanitizer API
- Is It Post Quantum Time Yet?
- Always-on Processor magic: How Find My works while iPhone is powered off
- Life is Pane: Persistence via Preview Handlers
- Abusing Weak ACL on Certificate Templates

Bug bounty & Pentest news

- Cybersecurity
  - Microsoft to disable Excel 4.0 macros, one of the most abused Office features
  - Twitch Hack of 135 GB of Data Includes How Much Its Biggest Streamers Make
  - NSA warns of ALPACA TLS attack, use of wildcard TLS certificates
- Upcoming events

    - Visma Security Conference 2021 (November 11)
    - Pen Test HackFest FREE Virtual Summit (November 15-16)
- Tool updates
    - Burp Professional / Community 2021.9 (New asynchronous SSTI payloads amongst other things)
    - BurpSuiteSharpener 1.07
    - ZAP 2.11.0 (OWASP 20th anniversary release)

Non technical

- Map your hacking sessions- then execute
- Vulnerability Writeups: The Magical 5 Minute Formula (Video) & Blog post