Bug Bytes #134 – SAML authentication bypass, RCE in PyPI & Lesser known XXE attack vectors

BY ANNA HAMMOND · AUGUST 6, 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 July 26 to August 2.

Our favorite 5 hacking items

1. Writeups of the week

Securing XML implementations across the web
Zimbra 8.8.15 – Webmail Compromise via Email

Mattermost researcher @jupenur disclosed round-trip vulnerabilities found in four XML parsers. Interestingly, they lead to authentication bypass in major SAML implementations.

The other writeup by @scannell_simon is about DOM-based stored XSS and authenticated SSRF. Chaining them increased their impact and would've allowed unauthenticated attackers to compromise Zimbra webmail servers.

2. Writeups² of the week

XXE Case Studies
Potential remote code execution in PyPI (pypi.org, $3,000)

The first writeup by @cinzinga_ has some interesting attack vectors for XXE, e.g. XXE via KML, proprietary, PDF and Excel files. They're worth knowing if you like to test for XXE.

The second writeup is the continuation of @ryotkak's work on supply-chain attacks. Static analysis of PyPI's source code revealed three vulnerabilities including RCE on pypi.org.

3. Tool of the week

hallucinate & Intro

Hallucinate allows you to inspect and manipulate TLS traffic using dynamic instrumentation. The difference with a Web proxy like Burp is that it does not replace certificates, so it is particularly useful when you want to analyze an app's encrypted traffic without bypassing certificate pinning.

4. Video of the week

DO NOT USE alert(1) for XSS & Blog post

If you use alert(1) when looking for XSS, you'll find this very informative. @LiveOverflow demonstrates why it can lead to false positives (e.g. if the XSS payload runs in a sandbox domain/iframe) and what other Proofs of Concept are generally better to use.

5. Resource of the week

Last Week in Security (LWiS) – 2021-08-02

Last Week in Security (LWiS) is @badsectorlabs's weekly summary of offensive security news, techniques and tools. It is similar to Bug Bytes but focuses more on the red team / internal pentest / Active Directory side. So if these are the topics you're most interested in, it is a great newsletter to follow.

I usually also include these topics in Bug Bytes but this week in particular, there have been too many noteworthy new tools and attacks. So exceptionally, this Bug Bytes will be almost only focused on Web / API / mobile hacking and for all the new AD and red teaming fun, please refer to LWiS.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Hacker Tools: NoSQLMap – No SQL, Yes exploitation & Blog post
- Learn with Rohit: Attacks and Defenses to Docker & Kubernetes!!.
- Print Nightmare AKA Domain Controller Domination
- Hacker Heroes #7 – @ceos3c (Interview)
- $50k bug bounty on Shopify explained (GitHub access token leaked via electron application)
- The Malicious Office 365 Application Experiment.. that went bad.. real bad..
- Radio Hack Ep2: Secure Code Review – Fady Othman (in Arabic)

Podcasts

- The BlackMatter Interview – Bad News for Firefox, DarkSide Return, Tailscale, Google to Assume HTTPS
- Hack'n Speak 0x09 – topotam | Une belle histoire, du TII et PetitPotam (Interview in French with PetitPotam's author)

Webinars

- DevOps for Hackers with Hands-On Labs w/ Ralph May (4-Hour Workshop)

Conferences

- Source Zero Con & Slides

Tutorials

Medium to advanced

- Advanced Recon Guide
- Cobalt Strike and Tradecraft
- How to Phish for User Passwords with PowerShell

Beginners corner

- Scanning your iPhone for Pegasus, NSO Group's malware
- Hackish Way to Capture Traffic of 'XMPP'(i.e. non-HTTP protocols) of Mobile Applications.
- How To Configure BurpelFish
- Step by Step. Automating multi-pass attacks in Burp Suite
- Pentesting Electron Applications

Writeups

Challenge writeups

- Intigriti / @RootEval's July XSS challenge winners and writeups
- Answer to the XSS Trick & Demystifying an XSS payload!

Pentest writeups

- Bypassing Defenses: Cylance

Responsible(ish) disclosure writeups

- Stealing Bitcoin with Cross-Site Request Forgery (Ride the Lightning + Umbrel) #Web
- Multiple Open Source Web App Vulnerabilities Fixed #CodeReview #Web
- Rotten Apples: Macos Codesigning Translocation Vulnerability #MacOS
- CVE-2021-27077: Selecting Bitmaps Into Mismatched Device Contexts #Windows #LPE

0-day & N-day vulnerabilities

- Developing an exploit for the Jira Data Center Ehcache RCE (CVE-2020-36239) #Web

Bug bounty writeups

- How to be popular (OkCupid)
- Gaining Access To GCP Of Google Stadia — 500$ Bounty (Google, $500)
- Facebook Email/phone disclosure using Binary search (Facebook)
- CVE-2020–15823: Server-Side Request Forgery (SSRF) in JetBrains YouTrack (JetBrains)
- Blast Radius: Apache Airflow Vulnerabilities ($13,000)
- Stealing SSO Login Tokens (snappublisher.snapchat.com) (Snapchat, $7,500)

See more writeups on The list of bug bounty writeups.

Tools

- dnsline: Tool for making it easy to collect dns results from the CLI
- Sanity: MXSS Fuzzer
- SaveBrowsingImages: Burp extension to save all browsed images to disk
- Revealin: Uncover the full name of a target on Linkedin
- Key-Checker: Go scripts for checking API key / access token validity
- reverse-apk: Quickly analyze and reverse engineer Android applications
- plution: Prototype pollution scanner using headless chrome

Tips & Tweets

- Forced directory indexing using range HTTP header
- Stored XSS using .xbl files
- Non-HTTP SSRF
- 403 bypass via “HTTP hop-by-hop request headers”
- SSTI polyglot
- If you could search through every subdomain on the internet what are some stuff you’d look for?
- Command to detect if a system is Windows or Linux (post-exploitation)

Misc. pentest & bug bounty resources

- Learn the fundamentals of Cloud Computing in 6 months
- traversal-archives
- @0xAwali's Online Shopping testing Checklist & Search engines queries
- OSCE^3 Study Guide by Joas
- Microsoft Wont-Fix-List (July 2021 Edition)

Challenges

- Template Engine Playground
- Attack AI systems in Machine Learning Evasion Competition (Aug 06 – Sep 17)
- VulWebaju

Articles

- Hacking naked Akamai ARL at scale, Weaponizing Apify for mass bug bounty $$$, Script to test open Akamai ARL vulnerability & V1/V2 ARL Change – Starting Aug 10, 2021
- How I Lost the SecurityTrails #ReconMaster Contest, and How You Can Win: Edge-Case Recon Ideas
- SAML is insecure by design

Bug bounty & Pentest news

- Bug bounty
  - h@cktivitycon 2021 Call For Papers
- Cybersecurity
  - The Pwnie Awards nominees
  - CISA Alert (AA21-209A): Top Routinely Exploited Vulnerabilities
- Upcoming events
  - A list of DEF CON villages streaming this weekend (free)
- Tool updates:
  - Nuclei: Option to disable templates auto-updates
  - @*StaticFlow*'s DirectoryImporter now supports ffuf
  - Changes for L0phtCrack & How to bypass licensing until an open source version is available
  - CrackMapExec v5.1.7dev – U fancy huh ?

- AutoRecon v2 (beta)

Non technical

- @iamthefrogy's bug bounty tips & motivation
- Bug Hunting Thoughts & Statistics
- Are you sharing your address on social media?
- Probably Are Gonna Need It: Application Security Edition
- Phishing Test Click-Rate Metrics: a Measure of Email Marketing, not Phishing Resilience

Community pick of the week

This is so inspiring! Make sure to check out @zseano's free methodology to see how these guys did it

Also tag us on social media to share your own bug hunting wins and joys, we love hearing from you!