Bug Bytes #111 – Finding your first bug, Middleware misconfigurations & Breaking Java XML parsers

BY ANNA HAMMOND · FEBRUARY 24, 2021 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-111-finding-your-first-bug-middleware-misconfigurations-breaking-java-xml-parsers

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 February 15 to February 22.

Intigriti News

Our favorite 5 hacking items

1. Video of the week

How to Find Your First Bug & TL;DR

Struggling to find your first bug? @InsiderPhD has some sensible tips that might help, including technical skills to learn and what to focus on. Make sure to watch the whole video, the note-taking tip at the end will help you maximize learning when reading writeups.

2. Writeup of the week

Enumerate internal cached URLs which lead to data exposure (Facebook, $4,800)

This writeup is about an issue in server-side caching on Facebook. @Samm0uda discovered an endpoint on developers.facebook.com that returned whether a URL (or partial URL) was present in the cache or not. The bug looks so obvious after reading about it! It sounds like a feature, I'm not sure I would've considered it a weakness leading to serious information disclosure (e.g. disclosure of URLs containing access tokens).

So, this is a great example that shows why it is important to always keep in mind business and technical impacts when assessing the security of a Web app.

3. Articles of the week

Misconfigurations in Java XML Parsers
Middleware, middleware everywhere – and lots of misconfigurations to fix

The first article is an amazing read if you're interested in XXE or SSRF (via XXE). It goes over different scenarios that make Java XML parsers vulnerable. For instance, if HTTP(S) and FTP are blacklisted, you can still find a blind XXE by making an FTP request with a file:// URL!

The second article sums up some new misconfigurations in middleware for Nginx (for example HTTP splitting against misconfigured proxies that use cloud storage solutions). This type of misconfigurations are very interesting to learn and test for! They bypass current mitigations and can still be found even on hardened targets.

4. Tutorials of the week

Top 10 Tips for Burp Suite
Client Side Encryption Bypass Part-2 & Part-3

The first tutorial presents ten really practical Burp tips. Power users might already know them, but it takes only a minute to go through them and maybe learn a new useful feature that'll change your Burp experience.

The other tutorials are about bypassing client-side encryption. You might've seen part 1 in a previous Bug Bytes. With these follow-ups, @sameer_bhatt5 plunges us deeper into the world of encrypted JavaScript, tools that help save time when debugging it, and how to automate decryption.

5. Tool of the week

Mubeng

Mubeng is a fast proxy IP rotator that will help bypass any type of IP ban (WAF, rate-limiting, bruteforce protection, etc). It's in Go, supports HTTP and SOCKSv5 protocols, supports all HTTP(S) methods, and includes a proxy checker to make sure your proxy IP is still alive.

What I like the most about it is its ease of use. You just give it a list of proxy IPs, it randomly rotates between them after a certain number of requests. It can also be chained with Burp and ZAP as an upstream proxy.

Other amazing things we stumbled upon this week

Videos

- Creating a Recon Database For Recon At Scale & recon_db_scripts
- $130,000+ Learn New Hacking Technique in 2021 – Dependency Confusion – Bug Bounty Reports Explained
- How to intercept traffic from Android apps with Objection and Burp
- Axiom Demo – Resolving 6 million domains in 5 minutes with 100 instances!
- Future of Exploit Development – 2021 and Beyond

Podcasts

- DAY[0] Episode 65 – PDF Exploits, GPGME Making Mistakes EZ and Favicon Tracking

- Dependency Confusion – SHAREit's Security Update, Solorigate, Brave's "Private Window With Tor"

Webinars

- Format String Vulnerabilities – The Impact of A Leaky Program

Tutorials

Medium to advanced

- Detecting JEXL injections with CodeQL
- All your input are belong to me – 3rd party web security
- Android Task Hijacking Using Movetasktoback() And Excludefromrecents
- Reading DPAPI Encrypted Keys with MimiKatz

Beginners corner

- How To Find XXE Bugs: Severe, Missed And Misunderstood
- A Pentester's Guide to File Inclusion

Writeups

Challenge writeups

- @holme_sec's http://challenge-0221.intigriti.io challenge winners and writeups
- Cryptopals: Exploiting CBC Padding Oracles

Pentest writeups

- A Journey Combining Web Hacking and Binary Exploitation in Real World!
- Exploiting Out-Of-Band XXE on Wildfire

Responsible(ish) disclosure writeups

- Smarty Template Engine Multiple Sandbox Escape PHP Code Injection Vulnerabilities #Web
- SHAREit Flaw Could Lead to Remote Code Execution #Android
- RCE in NPM VSCode Extention #Web #RCE
- Into the rabbit hole: Exploitation process of Redis and RabbitMQ #RCE #Redis
- Exploiting crash handlers: LPE on Ubuntu #Linux #LPE
- ZDI-21-171: Getting Information Disclosure In Adobe Reader Through The ID Tag #MemoryCorruptionBug #PDF

Bug bounty writeups

- Hunting for bugs in Telegram's animated stickers remote attack surface
- Is Math.random() Safe? from missing rate limit to bypass 2fa and possible sqli
- Leaking Facebook user information to external websites / Setting some cookies values (Facebook, $2,000)
- RCE on a Laravel Private Program
- CVE-2021-23827: Sakura Samurai discover cleartext pictures in Keybase Desktop Client; Windows, macOS, Linux (Keybase, $1,000)
- Dangling DNS Records leading to Sub-domain Takeover on api.techprep.fb.com! (Facebook, $500)

See more writeups on The list of bug bounty writeups.

Tools

- iframe-broker: Chrome / Firefox extension to log iframe and cross window communications
- MoneyScope: A Simple Tool to Pull Paid Bounty Scopes for Wide Recon Actvities
- MacHound & Intro: An extension to the Bloodhound audting tool allowing collecting and ingesting of Active Directory relationships on MacOS hosts
- AzureC2Relay & Intro: Azure Function that validates and relays Cobalt Strike beacon traffic by verifying the incoming requests based on a Cobalt Strike Malleable C2 profile

Tips & Tweets

- Wanna run Burp Collaborator in a Docker container?
- Original subdomain enumeration technique

Misc. pentest & bug bounty resources

- Apple Platform Security – February 2021
- Resources for learning Java insecure deserialization
- Awesome Vulnerable Applications
- Bug Bounty: De profesión "cazarrecompensas" (€24,04)

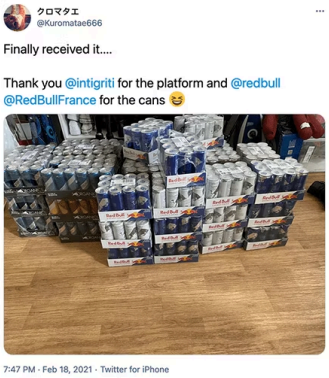
Challenges

- NahamCon CTF 2021
- Thunder CTF

Articles

- Dependency Confusion: When Are Your npm Packages Vulnerable?
- Terrible inet_aton in glibc
- Farming for Red Teams: Harvesting NetNTLM & Farmer

Community pick of the week



Well done @Kuromatae666!

We'd love to hear from you too about your bug bounty wins, swag and joys. Tag us on social media if you want to share them with other Bug Bytes readers.