Bug Bytes #113 – MS Exchange pre-auth RCE, Burp Crawler demystified & SSO security thesis

BY ANNA HAMMOND · MARCH 10, 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.

This issue covers the week from March 1 to 8.

Intigriti News

Spectre's comeback, Exchange zero-days & Risky JSON parsing and Go packages

Our favorite 5 hacking items

1. Articles of the week

Web application cartography: mapping out Burp Suite's crawler
Security and Privacy of Social Logins & Thesis

The first article is about the internals of Burp's crawler. Whether you're a Burp user or interested in Web crawling in general, it is fantastic to discover how it does its magic and overcomes challenges of modern Web apps that make crawling them difficult.

The second article (or rather a brilliant series of three articles plus a full thesis!) are all about SSO security. Louis Jannett analyzed real-world implementations of SSO (including Apple, Google, and Facebook SSO) and shared common weaknesses and vulnerabilities found.

2. Writeup of the week

TryHackMe X HackerOne CTF WriteUp (Hacker Of The Hill)

This is a solid writeup for the recent "Hacker of the Hill" CTF. It shows some interesting Web hacking techniques that might be useful for real tests (e.g. path traversal leveraging RFC822).

3. Video of the week

Finding Your Next Bug: GraphQL Hacking – Katie Paxton-Fear (@InsiderPhd)

This is an excellent introduction to GraphQL hacking. The best part? Not only does @InsiderPhD tell you everything you need to start testing GraphQL implementations, she also provides a lab to practice (see the intentionally vulnerable Generic-University that has a newly added GraphQL API).

4. Tools of the week

BurpSuiteAutoCompletion
netz & Intro
fransr/logger.js

BurpSuiteAutoCompletion by @_StaticFlow_ is a Burp extension that adds header autocompletion to Repeater and Intruder tabs. This is a huge time-saver if you often need to change/add HTTP headers. The headers list used by default is from Seclist but you can customize it.

Netz is a Go tool for mass-scanning the Internet similarly to Shodan, Censys or ZoomEye, but with the ability to perform any custom checks. I haven't tried it but bookmarked it in case I need to run large scale scans.

Another interesting tool is logger.js, @fransrosen's reflection script that helps him find script gadgets for XSS. Worth a try if you're into DOM XSS!

5. Bugs of the week

@orange_8361 reently teased about a Microsoft Exchange pre-auth RCE, then shared a site and demo for the the bug called Proxylogon. It turned out to be part of a pretty bad RCE bug chain currently being exploited in-the-wild.

I didn't find a detailed writeup of all vulnerabilities but here a few resources to keep you up to date:

- List of Exchange Server Zero-Days (by Rapid7)
- Technical DFIR report (by Volexity)
- Nuclei template & proxylogscan (@dwisiswant0's Go scanner) both for CVE-2021-26855/ProxyLogon

Other amazing things we stumbled upon this week

Videos

- Why Your IDORs Get NA'd, Cookies Explained
- Full Free Course: Android Bug Bounty Hunting

- SQL Injection – Lab #1 SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
- $5,000 YouTube IDOR – Bug Bounty Reports Explained
- Dependency Confusion Pt. 1 | The Setup | Packages | Private Registry & Pt. 2 | Final Part | Exploiting Dependency Injection
- Impostor Syndrome and How we Talk about it in Infosec

Podcasts

- DAY[0] Episode 67 – Buggy Browsers, Heap Grooming, and Broken RSA?
- Hafnium – Dependency Confusion, Intel Side Channel Attacks, Crispy Subtitles From Lay's

Webinars

- Finding Your Next Bug: GraphQL Hacking – Katie Paxton-Fear (@InsiderPhd)
- Burp Suite Cheat Sheet & Tips and Tricks & Burp Suite Cheat Sheet v1.0
- BHIS | Sacred Cash Cow Tipping 2021 – John Strand & BHIS Testers

Tutorials

Medium to advanced

- Solving double/n hop with ssf – SOCKS/C2
- Reverse Engineering a Flutter app by recompiling Flutter Engine
- CSP Bypass Guidelines

Beginners corner

- RCE via war upload in Tomcat using path traversal.
- AWS WAF — Know Your Enemy
- Exploiting Exposed .git Directory Without GitTools
- Anatomy of the Authentication Tests
- Ultimate XXE Beginner Guide

Writeups

Pentest writeups

- Pentesting Cisco ACI: LLDP Mishandling

- BMC Patrol Agent – Domain User to Domain Admin – Part 2 – Securifera

Responsible(ish) disclosure writeups

- CyRC Vulnerability Advisory: Denial of service vulnerability in Jetty web server #Web #CodeReview
- Multiple Vulnerabilities in Micro Focus Operations Bridge Reporter #Web #CodeReview
- CVE-2020-28243 SaltStack Minion Local Privilege Escalation #PrivEsc
- SaltStack API vulnerabilities #Web #RCE

Bug bounty writeups

- Dangling DNS: Amazon EC2 IPs (Current State) (8×8)
- Adobe AEM Security Web Series Part 1 | From dispatcher filter bypass to XSS on 40+ Linkedin websites (video)
- Elastic Community Conference: Elastic Disclosure—Finding and Reporting Security Bugs to Elastic (video)
- Write Up – Google VRP N/A: SSRF Bypass With Quadzero In Google Cloud Monitoring
- The easiest $2500 I got it from bug bounty program
- Stealing user passwords through a VPN's SSO

See more writeups on The list of bug bounty writeups.

Tools

- Wingman: XSS scanner
- http2smugl: Go tool that helps detect and exploit HTTP request smuggling in cases it can be achieved via HTTP/2 -> HTTP/1.1 conversion by the frontend server
- dnspy: Find subdomain takeovers
- BurpFeed: Python and Go tool for feeding urls into Burp's Sitemap

Tips & Tweets

- XML WAF bypass: Use Intruder + Hackvertor to bruteforce charsets
- Use XInclude to test XML parsers for for SSRF & LFI
- Exploiting SSRF on Windows servers
- Exploiting CSRF with broken Referer validation on Chrome
- Tricks for generating client-specific wordlists

- XSS polyglot

Misc. pentest & bug bounty resources

- s0md3v/be-a-hacker
- How do I get Started in Cyber Security? — My Perspective & Learning Path! & Security Talks Slides
- What's happening in the Burp-verse – Issue #1

Challenges

- GitHub Security Lab – Capture The Flag
- Nahamsec's Intro To Bug Bounty Labs
- @atul_hax's RCE webChallenge

Articles

- Dependency Confusion Attack – What, Why, and How?
- Anatomy of an Exploit: RCE with CVE-2020-1350 SIGRed
- Bitsquatting Windows.com

Bug bounty & Pentest news

- NahamCon2021 is this Sunday! Check out the talks program, CTF and merch
- Burp Suite Professional – Feature Roadmap Questionnaire

Non technical

- Bug Bounty: What do the top bug hunters find?
- The 2021 Hacker Report
- Wholesome Curl Calls For Your Blog Posts
- Ask a hacker: ajxchapman & Ask a hacker: rpadovani
- 7 Life Lessons From Hackers On How You Can Make 2021 The Best Year Of Your Life

Community pick of the week

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.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com