Bug Bytes #106 – THE blind SSRF reference, Apple & Microsoft RCEs & Scanning for logic flaws

BY ANNA HAMMOND · JANUARY 20, 2021 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:

https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-106-the-blind-ssrf-reference-apple-microsoft-rces-scanning-for-logic-flaws

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 10 to 17 of January.

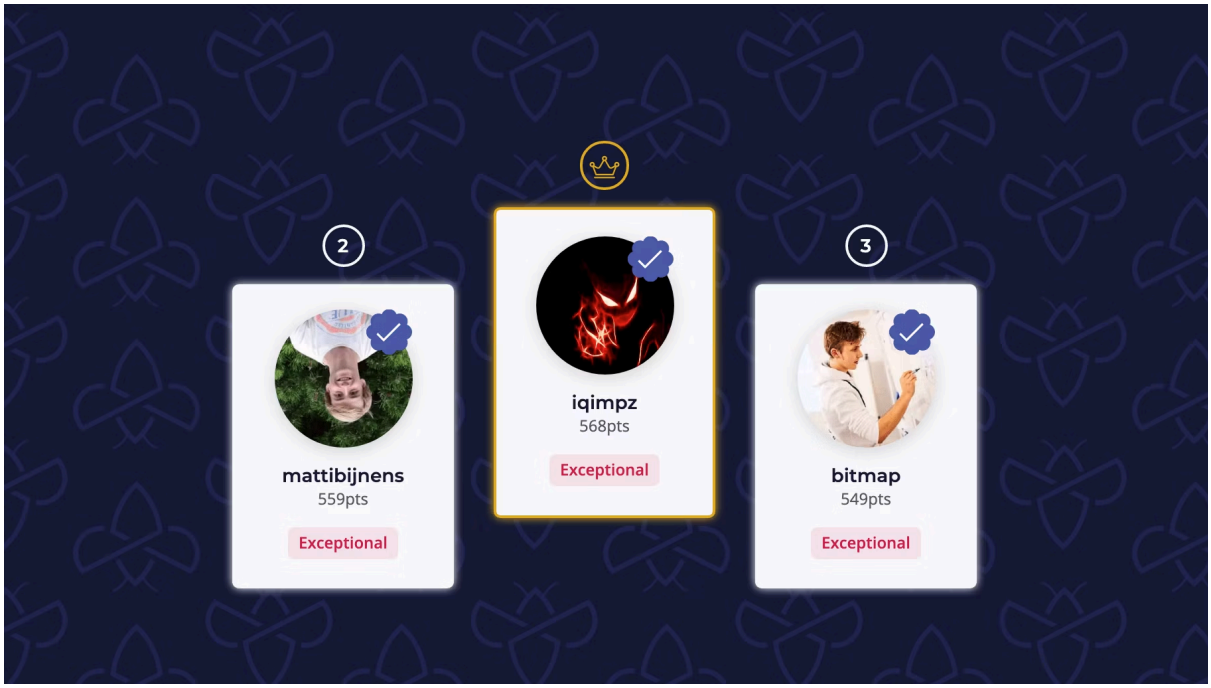
Intigriti News

Did you know that Bug Bytes is two years old? It is time to freshen it up a bit and you can help us by providing your feedback. We love to improve based on data and insights. So, your input is highly appreciated and will help us improve the quality of this newsletter.

Fill out the survey for a chance to win an Intigriti Swag voucher of € 50.

The winner of the Intigriti Swag voucher will receive a personal email before January 27.

Take the survey



Introducing report collaboration: split these bounties!

Google Titan 2FA keys cloned, Microsoft Exchange's unpatched RCE & Mimecast supply chain attack

Our favorite 5 hacking items

1. Resource of the week

A Glossary of Blind SSRF Chains & GitHub repo

This is a massive post on exploit chains that help escalate the impact of blind SSRF. This is simply a must see for bug hunters, a new amazing resource by @assetnote.

There is also a GitHub repo. You can contribute with additionl techniques by sending a pull request.

2. Writeups of the week

Finding 0day to hack Apple (Apple, $50,000)
Making Clouds Rain :: Remote Code Execution in Microsoft Office 365 (Microsoft)

There's a bunch of exceptional findings and excellent writeups that were published this week. Make sure to check out the entire writeups section below. These two are the one that caught my attention the most

for their impact and interesting technical details.

@rootxharsh and @iamnoooob got Remote Code Execution on three Apple subdomains by analyzing the CMS they use (Lucee). @steventseeley also popped shells but on Microsoft Office 365 and he also bypassed two different patches for the vulnerability.

3. Tools of the week

bbrf-burp-plugin

OpenAPI Security Scanner & Automating Permission Checks Using OpenAPI Security Scanner?

Remember BBRF, @honoki's Python tool for storing/querying bug bounty data in a CouchDB database? I've been using it and it is an excellent solution for easily handling assets and scopes. Now it also has a Burp plugin that allows you to add domains/URLs to your database from Burp! Fantastic, right?

The second tool is an innovative scanner for automating authorization tests. Logic flaws are notoriously difficult to automate but @ngalongc manages to do just that! His OpenAPI Security Scanner pointed to an API with a set of credentials monitors for changes in permissions and notifies you if any permissions have changed.

4. Video of the week

@Farah Hawa Talks About Learning How to Code, Javascript, Creating Content, Mentorship and more!

Anyone who thinks it is too late to start bug bounties or they don't have the right technical background should watch this interview. @Farah_Hawaa shares her story and how she got into Web hacking in a relatively short time. She went from journalism / mass media studies to becoming a hacker, triager for a bug bounty platform and content creator. Such an inspiration!

5. Podcast of the week

Day[0] Episode 60 – Breaking Lock Screens & The Great Vbox Escape

Day[0] is already at episode 60 and I've just heard of it! I love that it's not just about generic InfoSec news but also comments on very technical writeups and topics. A really nice discovery!

Other amazing things we stumbled upon this week

Videos

- BOUNTY THURSDAYS – 2021 + new tools + new stuff = COOL BUGS!
- @d0nutptr demoing his recon tool resync
- Hacking banks with race conditions
- Livestream – Common API bugs + QnA
- Watch me hack a bug bounty target from scratch. #bugbounty #hacking
- How to prevent PHP type juggling vulnerabilities

Podcasts

- Security Now: Where the Plaintext Is – 2021s First Patch Tuesday, Titan Security Key Side-Channel Attack, WhatsApp
- Cloud Security Testing In Aws – Pawel Rzepa – Cloud Security Podcast
- Darknet Diaries Ep 83: NSA Cryptologists

Webinars & Webcasts

- ZAP Deep Dive: Passive Scanning

Conferences

- How the Best Hackers Learn Their Craft

Tutorials

Medium to advanced

- Flutter based Mac OSX Thick Client SSL Pinning Bypass
- macOS Post-Exploitation Shenanigans with VSCode Extensions

Beginners corner

- Pentesting the ELK Stack
- Authorization Checks Made Easy
- Converting NMAP XML Files to HTML with xsltproc
- Cross-frame Scripting Attacks
- Android Penetration Testing: WebView Attacks

Writeups

Challenge writeups

- KringleCon #HolidayHack 2020 Write-ups

Pentest writeups

- Split XSS & Lab

Responsible(ish) disclosure writeups

- Laravel <= V8.4.2 Debug Mode: Remote Code Execution #Web
- LDAP Injection In OpenAM #Web

Bug bounty writeups

- How I hijacked the top-level domain of a sovereign state (Internet Bug Bounty)
- Attack of the clones 2: Git CLI remote code execution strikes back (GitHub)
- Guest Blog Post: Leaking silhouettes of cross-origin images (Mozilla, Chrome)
- The Embedded YouTube Player Told Me What You Were Watching (and more) (Google, $1,337)
- Insertion Of Malicious Links For Execution In Profile Picture – Unvalidated User Input In MS Sharepoint 2019 (CVE-2020-1456) (Microsoft)
- Weblogic Remote Code Execution (Exploiting CVE-2019-2725)
- Let's know How I have explored the buried secrets in React Native application
- @samwcyo's 2020 bugs
- Apache solr RCE via velocity template
- Access Token Smuggling from my.playstation.com via Referer Header (PlayStation, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- Metasploit Modules for RCE in Apache NiFi and Kong API Gateway
- whatislife_enum: File system enumerator and monitor for Android
- ssrf-king & Demo: Burp extension to automate detection

Tips

- Exploiting SSRF on exposed Selenium Grid hub
- @ngkogkos's walkthrough of Burp extension AutoRepeater
- Bypass XXE filters based on Content-Type
- @HolyBugx's File Upload Checklist
- @hunter0x7's File upload checklist: Part 1, 2 & 3

Misc. pentest & bug bounty resources

- leaky-paths
- JavascriptRecon.md
- @Farah_Hawaa's Web hacking Instagram reels
- PHPGGC: PHP Generic Gadget Chains

Challenges

- @0xCaptainFreak's Node/Express.js Web Security Challenge

Articles

- Insecure Features in PDFs
- How I stole the data in millions of people's Google accounts
- Breaking The Browser – A tale of IPC, credentials and backdoors & ChromeTools
- Sign over Your Hashes – Stealing NetNTLM Hashes via Outlook Signatures & Sigwhatever

Bug bounty & Pentest news

- Introducing report collaboration: split these bounties!
- Evading Detection – A Beginner's Guide to Obfuscation: January 23

Non technical

- Avoid Burnout as a Programmer or Hacker
- Hacker Spotlight: Interview With Samengmg
- Gamifying Security with Red Team Scores
- This is how you can deliver true value through your pentest reports

Community pick of the week

We'd love hearing from you and celebrating your wins! Tag us if like Stefan you're in swag heaven or want to share your bug hunting joys with other Bug Bytes readers.

Stefan Rows
@ceos3c

Thanks very much @intigriti to hook me up with all that stuff. I am in Swag heaven RN.

Appreciate it!

5:53 PM · Jan 14, 2021 · Twitter Web App

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com