Bug Bytes #137 – Weird proxies 2, JDBC attacks & A handful of RCEs

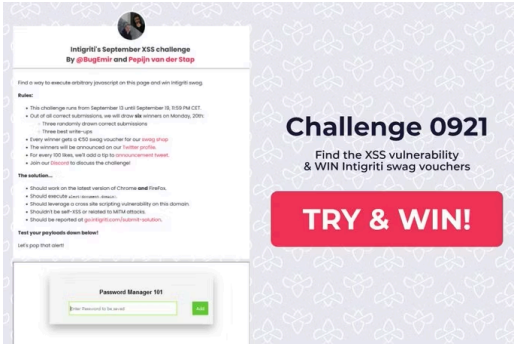
BY ANNA HAMMOND · SEPTEMBER 8, 2021 · LAST UPDATED ON MARCH 6, 2025

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 August 30 to September 6.

Intigriti news



Intigriti's September XSS challenge By @BugEmir and Pepijn van der Stap

Our favorite 5 hacking items

1. Vulnerabilities of the week

CVE-2021-26084 Remote Code Execution on Confluence Servers
RCE-0-day-for-GhostScript-9.50

CVE 2021-26084 is an OGNL injection on Confluence servers that leads to unauthenticated RCE. A few days after the vender advisory was published, @iamnoooob and @rootxharsh reversed the patch and published this excellent writeup/PoC.
The vulnerability is already being exploited en-masse, was successfully exploited on Jenkins, has a Nuclei template, a WAF bypass, and a root cause that goes back to 2020.

The other vulnerability that is making headlines is an RCE in GhostScript 9.50. @emil_lerner discovered it on several bug bounty programs and demonstrated the vulnerability at ZeroNights X. Then @ducnt_ published a PoC.

2. Writeups of the week

More secure Facebook Canvas : Tale of $126k worth of bugs that lead to Facebook Account Takeovers (Facebook, $126,000)
SSRF in PDF export with PhantomJs

Anyone who thinks there are no bugs left to be found on bug bounty programs should just @Samm0uda's writeups. The latest one is about three account takeovers he discovered on Facebook. Amazing findings and writeup!

The second writeup is about an SSRF found in a PDF export feature that used PhantomJs. Interestingly, LFI payloads were blocked so @xhzeem used an XHR request to read files.

3. Tools of the week

json2paths
RepeaterSearch & BurpSuiteAutoRepeaterNaming

@s0md3v's json2paths implements a cool idea by @imranparray101. It collects JSON keys from JSON responses in Burp's history, and uses them to create a wordlist of URL paths. This is a nice Python tool that can help find hidden API endpoints.

The other tools are new Burp extensions by @_StaticFlow_. RepeaterSearch adds a search bar to the Repeater tab. BurpSuiteAutoRepeaterNaming replaces repeater tab names with the URL path of the repeater request (instead of incremental numbers). So, both extensions can be useful if you find yourself opening dozens of Repeater tabs and in need of a way to manage them better.

4. Conferences of the week

Make JDBC Attacks Brilliant Again
Weird proxies/2 and a bit of magic (in Russian) & Slides

The first talk is about @pyn3rd and Chen Hongkun's latest research on JDBC attacks. They share new ways of exploiting JDBC including XXE, RCE, and vulnerabilities they found in Weblogic, Spring Boot H2 console, JBoss/Wildfly, Apache Druid and many others.

The second talk is a follow-up to @antyurin's research on reverse proxy related attacks. The talk is sadly in Russian but the slides and updates to the Weird Proxies are in English and full of new tricks for poking at reverse proxies.

5. Resource of the week

Samlists

Who doesn't like a well-curated wordlist for Web fuzzing? @SamuelAnttila's Samlists is a wordlist of ~47K parameter names collected from CommonCrawl data. It is based on recent data, uses several techniques to remove unuseful parameters and is sorted based on the likelihood of occurence.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Matthew Bryant (@IamMandatory) Talks About Doing Research, Blind XSS, Creating XSSHunter, and more!
- "Want To Find An RCE To Get Tattoo" with @Farah Hawa (Hacker Heroes #12)
- Aaditya Purani Talks about CTFs, Motivation, and successful cybersecurity Career tips
- Using curl better – with curl creator Daniel Stenberg
- Adding infinite funds to your Steam wallet – $7,500 bug bounty report
- Super Easy Subnetting – TikTok Edition?

Podcasts

- Web scanners are evolving to secure modern web applications and their APIs
- Takeover A Facebook, SnapChat or JetBrains Account
- Radio Hack Ep3: Security Engineering – Ibrahim Mosaad (in Arabic)

Webinars

- BHIS | Uncovering Secrets and Simplifying Your Life with CyberChef – BB King

Conferences

- HITB Singapore 2021 & Slides
- GrabCON 2021 | Day-1, Day 2 & Program
- Black Hat Asia 2021 & Presentation materials
- NoNameCon 2021
- ZeroNights X Main Stage & Web Village (in Russian)

Tutorials

Medium to advanced

- The complete GraphQL Security Guide: Fixing the 13 most common GraphQL Vulnerabilities to make your API production ready
- UNIX Shells dropping SUID rights in shellcodes
- PowerShell Obfuscation

- The Art of the Device Code Phish & Never had a bad day phishing. How to set up GoPhish to evade security controls.
- Using procdump on Linux to dump credentials

Beginners corner

- Android App Pentesting Quickstart
- KiteRunner – Hacker Tools: Next-level API hacking & Video
- How to perform static analysis of JavaScript files?
- iOS Pentesting 101
- The Application Sandbox
- SAML – what can go wrong? Security check

Writeups

Challenge writeups

- Alles CTF 2021
- CSRF – Lab #1 CSRF vulnerability with no defenses | Long Version
- Burp Suite Certified Practitioner Exam Prep Walk thru
- BND-Recruitment-2021-CTF-Web-Security

Pentest writeups

- Mozilla VPN Security Audit

Responsible(ish) disclosure writeups

- Ghost CMS 4.3.2 – Cross-Origin Admin Takeover #Web
- Anatomy and Disruption of Metasploit Shellcode #BinaryExploitation
- Security Advisory // Multiple vulnerabilities in EMC VNX NAS 8.1.9-232 #Web #CodeReview
- BRAKTOOTH: Causing Havoc on Bluetooth Link Manager #Bluetooth
- Crashing Sip Clients With A Single Slash #SIP
- Cracking the Victure PC420 Camera and IPC360 Platform: Remote Control And Cloud Misconfiguration Combined #IoT

Bug bounty writeups

- Improper Authentication – any user can login as other user with otp/logout & otp/login (Snapchat, $25,000)

- Eye for an eye: Unusual single click JWT token takeover (JetBrains)
- Dropping root shell in a Crypto Exchange for Fun and Profitn't ($1,000)
- CVE-2021-39165: A Bug Bounty Journey from a Laravel SQL Injection Vulnerability
- Burp Suite RCE (PortSwigger)
- 2 CSRF 1 IDOR on Google Marketing Platform (Google)
- Hunting for XSS with CodeQL (GitLab, $500)

See more writeups on The list of bug bounty writeups.

Tools

- dnstake: A fast tool to check missing hosted DNS zones that can lead to subdomain takeover
- iHide & Intro: A utility for hiding jailbreak from iOS applications
- ghidra2frida & Intro: The new bridge between Ghidra and Frida

Tips & Tweets

- CVE-2021-22885: Rails info disclosure / unintended method execution
- Risks of using Burp Collaborator as a disposable email address provider when registering with websites
- Commas in Shodan searches
- How to run Bash commands when you can't use lowercase characters
- JSONP endpoint on Wikipedia that can be used for CSP bypass
- LFI to RCE on Windows boxes running PHP

Misc. pentest & bug bounty resources

- ThinkstScapes
- Bug Bounty Reports Templates
- IT Security Lecture
- @0xAwali's methodolgy for bypassing Deny Lists
- Rana Khalil's Academy

Challenges

- Intigriti's September XSS challenge By @BugEmir and Pepijn van der Stap

Articles

- Go Fuzz Yourself – How to Find More Vulnerabilities in APIs Through Fuzzing [Whitepaper download]
- When automating wayback machine and ffuf is not the answer, or manual analysis ftw
- Reflections on trusting plugins: Backdooring Jenkins builds
- A deep-dive into the SolarWinds Serv-U SSH vulnerability
- From RpcView to PetitPotam & Fuzzing Windows RPC with RpcView
- DHCP Games with Smart Router Devices

Bug bounty & Pentest news

- Bug bounty
  - An Update on Facebook's Bug Bounty Program
  - Apple Security Research Device Program (Apply before October 1)
  - H1's 13th Million Dollar Hacker
- Cybersecurity
  - Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role
  - Haksec CreatorConnect
- Upcoming events
  - OWASP's 20th Anniversary Celebration (September 24)
- Tool updates
  - Nuclei v2.5.0 Release
  - Turbo Intruder 1.23

Non technical

- Lawyers, Bugs, And Money: When Bug Bounties Went Boom, Uprising In The Valley: Part Two & 'drive It Like You Stole It': Part Three