Bug Bytes #131 – Credential stuffing in bug bounty, Hijacking shortlinks & Hacker shows

BY ANNA HAMMOND · JULY 14, 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 5 to 12.

Our favorite 5 hacking items

1. Tools of the week

ppmap
WILSON Cloud Respwnder & Intro

ppmap is a Go scanner to test for XSS via prototype pollution using known gadgets and existing research. Being 100% automated, it is a handy way to test for those low-hanging prototype pollution bugs.

WILSON Cloud Respwnder is an alternative to Burp Collaborator and Interactsh by @honoki. Why another tool? Because it allows you to continue receiving OOB requests for a long time (no need to keep Burp or an Interactsh session open). It can send notifications to Slack or Discord, allows block-listing domains from notifications and serving custom files.
If only it was named AlorsOnDNS!

2. Writeups of the week

Credential stuffing in Bug bounty hunting ($8,300)
Whose app are you downloading? Link hijacking Binance's shortlinks through AppsFlyer

It is interesting to see credential stuffing (usually more associated with pentest/red teaming) leveraged for bug bounties. @Krevetk0Valeriy shares how they did it and managed to score several bounties.

The second writeup is about exploiting a third-party app analytics platform. By overwriting shortlinks, it was possible to serve malicious apps to thousands of users. As usual, a very insightful writeup by @samwcyo.

3. Challenge of the week

SQHell & ep02 CTF TEARDOWN SQHELL on TryHackMe

SQHell is a free TryHackMe room by @adamtlangley. It covers 5 types including nested SQL injection / SQL inception that is interesting to practice. If stuck, check out the hour-long video walkthrough by the challenge's author himself.

4. Videos of the week

Hacker Tools – CyberChef & Blog post
Hacker Heroes #4 – @real_bitmap (Interview)

I love listening to interviews when I am walking outside, so this new Hacker Heroes series by @PascalSec comes at a perfect time.
If I'm at a mood for more technical content, @PinkDraconian's byte-sized tutorials (both blog posts and this new video format) always teach me something new.
Great job and not just because we're colleagues!

5. Tip of the week

XML SQL injection

Did you know that XML elements are a good place to test for SQL injection? It's worth remembering especially in cases where all your XXE attempts are failing.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Interview With @Base_64 : 19 Y/o | ~7000 Rep On Hackerone | Methodology, Mindset, Life & More...
- What is a Browser Security Sandbox?! (Learn to Hack Firefox)
- $20,000 RCE in GitLab via 0day in exiftool metadata processing library CVE-2021-22204

Podcasts

- REvil's Clever Crypto – Microsoft Fails to Patch PrintNightmare & Sodinokibi Malware's Crypto Design

Webinars

- Pushing Your Way In
- Interviewee Field Manual: Hack the Interview – Doug Brush

Conferences

- Padding Oracle Attacks: Dr. Henning Kopp (BSidesMesh21)
- Demystifying the state of kubernetes cluster security & Kubestriker
- Pass the SALT
- SANS Purple Team Summit 2021

Tutorials

Medium to advanced

- Two One-liners for Quick ColdFusion Static Analysis Security Testing #CodeReview
- Hacking Rendertron and Puppeteer— What to expect if you put a browser on the internet
- Long passwords don't cause denial of service when using proper hash functions

Beginners corner

- Backing up your BBRF data
- Hacking Microservices For Fun and Bounty
- JavaScript Code Review Guide for Bug Bounty Hunters
- Params — Discovering Hidden Treasure in WebApps
- Automating Microsoft Office to Achieve Red Teaming Objectives

Writeups

Challenge writeups

- @SecurityMB's Twitter quiz solution
- Full Stack Web Attack 2021 :: Zero Day Give Away (CVE-2021-28169)
- So many different techniques to learn here! [CTF walkthrough]
- SQL Injection – Lab #15 Blind SQL injection with out-of-band interaction

Pentest writeups

- ModSecurity v3 and URI Fragments

Responsible(ish) disclosure writeups

- A brief look at Gitpod, two bugs, and a quick fix #Web

- CVE-2021-28474: Sharepoint Remote Code Execution Via Server-side Control Interpretation Conflict #Web
- Solarwinds Serv-U 15.2.3 Share URL XSS (CVE-2021-32604) #Web
- Arbitrary File Read in Dell Wyse Management Suite (CVE-2021-21586, CVE-2021-21587) #Web
- CVE-2020-7387..7390: Multiple Sage X3 Vulnerabilities & Metasploit PoC #RCE
- Windows Defender Antivirus SYSTEM RCE #MemoryCorruption
- Old dog, same tricks #Network #RCE
- UDP Technology IP Camera vulnerabilities #IoT #RCE

N-day vulnerabilities

- PoC for SSRF in IBM QRadar SIEM (CVE-2020-4786)
- Exploiting the Sudo Baron Samedit vulnerability (CVE-2021-3156) on VMWare vCenter Server 7.0

Bug bounty writeups

- Account Takeovers — Believe the Unbelievable
- Part 2: Dive into Zoom Applications
- Reflected XSS Through Insecure Dynamic Loading
- FogBugz import attachment full SSRF requiring vulnerability in *.fogbugz.com (GitLab, $6,000)
- Stored XSS via Mermaid Prototype Pollution vulnerability (GitLab, $3,000)
- Removing parts of URL from jQuery request exposes links for download of Paid Digital Assets of the most recent Order placed by anyone on the store! (Shopify, $2,900)

See more writeups on The list of bug bounty writeups.

Tools

- AioResolver: Fast DNS resolver
- JiraScan: A simple remote scanner for Atlassian Jira
- roboXtractor: Extract endpoints marked as disallow in robots files to generate wordlists
- UserEnumTeams: User enumeration with Microsoft Teams API
- TokenTactics: Azure JWT Token Manipulation Toolset

Tips & Tweets

- @InonShkedy's July #bugbountytips

- Something to try if you find response header injection
- Weird alerts
- Prettifying JSON output of AEM pages

Misc. pentest & bug bounty resources

- rfc.fyi: Browseable, searchable RFC index
- Filesec.io & Intro: A catalog of the latest file extensions being used by attackers
- @0xAwali's methodologies for testing File upload & Login
- Prototype Pollution Exploits

Challenges

- Vuldroid: An intentionally Vulnerable Android Application

Articles

- #ProTips: Catching Bugs with Adrien Jeanneau
- Getting Partial AWS Account IDs for any Cloudfront Website
- Don't Be Rude, Stay: Avoiding Fork&Run .NET Execution With InlineExecute-Assembly & InlineExecute-Assembly
- Bypassing macOS TCC User Privacy Protections By Accident and Design

Bug bounty & Pentest news

- Ransomwhere project wants to create a database of past ransomware payments
- Microsoft Bug Bounty Programs Year in Review: $13.6M in Rewards
- 6 Steps To Securing Bonus Program Invites!
- Firefox becomes latest browser to support Fetch Metadata request headers
- Chinese government lays out new vulnerability disclosure rules
- Tool updates
  - Burp Suite roadmap update: July 2021
  - Nuclei v2.4.0 – Uniform, Stable & More Powerful
- Upcoming events
  - Critical Vulnerabilities in Network Devices: Past, Present & Future (July 17)

Non technical

- BugBountyHunter Chats — Getting to know 0xblackbird, YouGina, JTCSec and HolyBugx
- Think outside the box with Kunwar Atul
- Zwink's Tips And Tricks To Crush Bug Bounty

Community pick of the week

You're killing it! Congratulations @isira_adithya

If you too have bug bounty wins, swag and joys to share with other Bug Bytes readers, tag us on social media. We love hearing from you!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com