Bug Bytes #78 – BIG-IP RCE, Azure account takeover & Hunt scanner is back!

BY ANNA HAMMOND · JULY 8, 2020 · 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 26 of June to 03 of July.

Our favorite 5 hacking items

1. Resource of the week

Cloud-ranges

Cloud-ranges is a collection of IP ranges owned by cloud providers (AWS, Azure, GCP, Godaddy, Linode, Rackspace...). The script used to pull this information is run everyday by @pry0cc, and the repo updated. So helpful for internet scanning research!

2. Writeups of the week

Taking over Azure DevOps Accounts with 1 Click (Microsoft, $3,000)

Story of a 2.5k Bounty — SSRF on Zimbra Led to Dump All Credentials in Clear Text ($2,500)

The first bug is a 1-click account takeover of Azure DevOps accounts. @seanyeoh intiallty found a subdomain takeover that didn't seem that critical. Except that he could exploit it to steal tokens used in another subdomain's authentication flow.

Lesson learned: Subdomain takeovers can not only be used to capture emails (by setting MX records) or create valid SSL certificates, but also to bypass whitelists in redirection parameters of authentication flows, and steal sensitive tokens.

The second finding is also pretty interesting. It is an SSRF exploiting Zimbra with memcached exposed. By changing the backend server IP in cache, @YShahinzadeh was able to redirect server traffic, perform a MiTM attack and steal credentials.

3. Tools of the week

Hunt Scanner

Bat

HUNT is an excellent Burp extension. It had only one fault: it did not work with Burp 2.0. This is not an issue anymore thanks to @OptionalValue who rewrote it for the current version of Burp.

The other tool I was really glad to discover this week is Bat. I wish I knew about it sooner because it truly is an upgrade of cat. It adds color, syntax highlighting for several programming and markup languages, shows non-printable characters, uses less for large files by default, plus lots of other cool features.

4. Tutorials of the week

Using SQL Injection to perform SSRF/XSPA attacks

Weaponizing favicon.ico for BugBounties , OSINT and what not , FavFreak & get-shodan-favicon-hash.py

The first article shows in detail how to leverage SQL injection to perform SSRF/XSPA. This is a fantastic ideas as it can help increase the impact of a SQL injection, and move from attacking the database to attacking cloud services (e.g. fetching sensitive metadata).

The second tutorial is also a nice technique to add to your recon arsenal. It is about using favicon.ico hashes for assets enumeration, with a Python script to automate the process.

5. News / Vulnerabilities of the week

RIFT: F5 Networks K52145254: TMUI RCE vulnerability CVE-2020-5902 Intelligence (includes PoCs) & How to find F5 BIG-IP instances

CVE-2020-2021 PAN-OS: Authentication Bypass in SAML Authentication, Additional info by author & CVE-2020-2021: Post Exploit Analysis

It is not everyday that a vulnerability so serious comes up and makes bug hunters stop anything they are doing to check it out. This week brought up not only one but two bugs of this kind.

The first one is an RCE on F5 BIG-IP. The initial advisory didn't disclose much, but it was reverse engineered and different Proofs of Concepts were published. The second bug is an SAML authentication bypass on PAN-OS (Palo Alto Networks). It was also reverse engineered, but the PoC developed by Randori is not public yet.

CVE-2020-5902 and CVE-2020-2021 dominated hacker conversations on Twitter. They are worth analyzing given their impact and how widespread is the affected software. But remember to give bug bounty programs some time to patch, before starting to test for and report such n-day vulnerabilities. A lot of programs mention this in their rules anyway!

Other amazing things we stumbled upon this week

Videos

- How to Take EFFECTIVE Bug Bounty Notes
- Live API Hacking Demo
- CORS Explained (By Example)

- 5 investments that help you become a better bounty hunter
- Getting Started with PoshC2 on Linux
- Hack The Planet 7_2_2020

Podcasts

- Security Now 773 – Ripple20 Too
- Risky Business #590 — REPOST: It turns out we're not SAML experts
- Undetected e.04: TomNomNom – Hacking things back together & Notes
- Podcast: "Stay out of your comfort zone!" & Bug Bounties on The Other End
- Cyber Security Sauna 041| The Ethics of Red Teaming
- We, The Red Episode 1 – Red Teaming & Automation
- The Infosec & OSINT show 13
- 7MS #420: Tales of Internal Pentest Pwnage – Part 17
- SWN #45 – TikTok Bans, Top 10 Bug Bounties, & BlueLeaks

Webinars & Webcasts

- SANS webinars (require free registration)
  - ICMP: A world beyond ping
  - Managing & Showing Value during Red Team Engagements & Purple Team Exercises
  - A Wolf in Sheep's Clothing: Dissecting Living off the Land Techniques

Conferences

- Modern Web Vulnerabilities 2020 – Erlend Oftedal
- Layer 8 Conference, especially:
- iHack 2020 (in French)
- OWASP Bay Area Meetups
  - SIP June 2020
  - Hacker Days: Kubernetes Goat
- Team Summercon Live Stream & Schedule
- DEF CON Delhi Group 0x03 SAFE MODE

Tutorials

Medium to advanced

- Security Issues in Import/Export Functionality
- Still Scanning IP Addresses? You're Doing it Wrong
- Getting Started with Frida : Hooking a Function and Replacing its Arguments
- 1-click meterpreter exploit chain with BeEF and AV/AMSI bypass
- IoT Security – Part 6 (ZigBee Security – 101)

Beginners corner

- Beginners Guide On How You Can Use Javascript In BugBounty. & JSFScan.sh
- Gemfury Subdomain takeover
- Kill 'em With Laughter: "The Billion Laughs" Attack Through Image Uploads
- Google Cloud Platform pentest notes — service accounts
- Saving Images from Google Maps and Street View
- Using PowerShell for Pentesting in Kali Linux

Writeups

Challenge writeups

- Digging into Local File Inclusion
- Solutions to @kinugawamasato's XSS challenge: 1 & 2

Pentest writeups

- Adventures in ATM Hacking
- How I stole ~2000 Emails from your email account.
- Escaping Restricted Shell through Insecure Consul API
- Bypassing CrowdStrike Endpoint Detection and Response
- FROM ZERO INFO TO ZERO-DAY

Responsible(ish) disclosure writeups

- Would you like some RCE with your Guacamole? (CVE-2020-9497 & CVE-2020-9498) #RCE #RDP
- CVE-2020–2033 Palo Alto Global Protect Remote Session Hijack #MiTM #VPN

- Local Privilege Escalation Discovered in GlobalProtect App #PrivEsc #Windows
- Mozilla Firefox URL mPath Information Disclosure Vulnerability #BrowserHacking
- OCS Inventory NG v2.7 Remote Command Execution (CVE-2020-14947) & PoC #RCE #CodeReview #PHP
- Resurrecting an old AMSI Bypass #Windows
- Microsoft Windows LNK Remote Code Execution Vulnerability — CVE-2020-1299 #RCE #Windows
- Technical Advisory – macOS Installer Local Root Privilege Escalation (CVE-2020-9817)
- Windows Telemetry service elevation of privilege #PrivEsc #Windows

Bug bounty writeups

- How I hacked a bank their application using it for hacking another bank company — 10K XSS ($10,000)
- Story of stealing mail conversation, contacts in mail.ru and myMail iOS applications via XSS (Mail.ru, $1,000)
- Patched Zoom Exploit: Altering Camera Settings via Remote SQL Injection (Zoom, $3,000)
- ZombieVPN, Breaking That Internet Security & Repo (Bitdefender & AnchorFree)
- Vulnerability in Electron-based Application: Unintentionally Giving Malicious Code Room to Run (Symbol) #CodeReview
- Mozilla sites vulnerable to HTTP Desync attacks
- Create any military unit in any age (InnoGames, $1,100)
- Keybase client (Windows 10): Write files anywhere in userland using relative path in “download attachement” feature (Keybase, $5,000)
- Tricking the “Create snippet” feature into displaying the wrong filetype can lead to RCE on Slack users (Slack, $1,500)
- Spoofing the redirect process using RTLO (Vanilla, $150)
- Cross-Site Scripting (XSS) on www.starbucks.com | .co.uk login pages (Starbucks, $500)

See more writeups on The list of bug bounty writeups.

Tools

If you don’t have time

- Abnormalizer: Python script that takes a unicode string and abnormalizes it by character replacement. Currently uses Latin & Greek character substitution
- ScriptHunter & Intro: Automated JS Discovery

- WStalker, Intro: HTTP/HTTPS Proxy with full Request/Response logging to support Web API assessments & How-to: Importing WStalker CSV (and more) into Burp Suite via Import to Sitemap Extension
- Turbo Data Miner: Burp extension for flexible and dynamic extraction, correlation, and structured presentation of information as well as the flexible and dynamic on-the-fly modification of outgoing or incoming HTTP requests using Python scripts
- patch-apk – App Bundle/Split APK Aware Patcher for Objection & Intro: An APK patcher, for use with objection, that supports Android app bundles/split APKs

More tools, if you have time

- Browsertunnel: A tool for exfiltrating data from the browser using the DNS protocol
- PUFF: Simple clientside vulnerability fuzzer, powered by puppeteer
- DumpCN: A simple script that reads a list of domains (starting with https:// or not) from standard input, grabs the certificate and prints the CN
- Takemeon & Intro: nxdomain subdomain enumeration. Helps in scaling the automation. Currently, it only helps to resolve the nxdomain if possible
- Behave!: A monitoring browser extension for pages acting as bad boys. Warns if a Web page performs port scanning, access to private IPs or DNS rebinding attacks
- TrashEmail: A hosted disposable email telegram bot
- Psalm & Intro: Vimeo's static analysis tool for finding errors in PHP applications
- OFJAAAH: Automated recon script
- FileSearcher & Intro: Unmanaged assembly file searcher for when a fully interactive beacon session is not opsec safe enough
- bof-NetworkServiceEscalate: Sample "Beacon Object File" (COFF really?) created with Mingw-w64 & Makefile : Can be used as a "getsystem" or to escalate to SYSTEM from NetworkService using Forshaw's shared logon session issue
- SpoolSystem: A CNA script for Cobalt Strike which uses the Print Spooler named pipe impersonation trick to gain SYSTEM privileges
- Leonidas: Automated Attack Simulation in the Cloud, complete with detection use cases

Misc. pentest & bug bounty resources

- Mobile Device Security and Penetration Testing Guide
- payloadbox/ssti-payloads
- OSWE cheat sheet (English translation)
- Conducting a Cloud Assessment in AWS

- redteaming.co.uk
- Azure Active Directory: Data Security Considerations

Challenges

- SSTI testbed by @H4rSh4D
- @soroush..'s quick quiz & Answers
- XSS challenge #1 – raumamix
- New @PwnFunction XSS challenge & Solution

Articles

- SQL Injection Double Uppercut :: How to Achieve Remote Code Execution Against PostgreSQL
- Community Powered Scanning with Nuclei
- Put your bash code in functions
- Intercepting and Saving $5,000 Worth of Phished Crypto
- Automating DLL Hijack Discovery & DLLHijackTest
- Baselining PassGAN: Adventures in the rhubarb
- Abusing the Windows Power Management API – Delaying malicious payload execution until the machine is asleep
- IoT Part 3: Fire!
- Living Off Windows Land – A New Native File "downldr"
- Paper: Thematic for Success in Real-World Offensive Cyber Operations – How to make threat actors work harder and fail more often

News

Bug bounty & Pentest news

- @DafyddStuttard AMA
- @HusseiN98D AMA
- Google Cloud Next – OnAir: Jul 14 – Sep 8
- @PortSwiggerRes has a new research site!
- Hackerone's Top 10 Bounty Programs 2020
- Reputation, Signal & Impact Calculation Enhancements

- Burp Suite now has experimental support for HTTP/2

Reports

- The more cybersecurity tools an enterprise deploys, the less effective their defense is
- Open IPP Report – Exposed Printer Devices on the Internet

Vulnerabilities

- Exploit developed for critical Palo Alto authentication flaw (CVE-2020-2021)
- F5 customers urged to patch systems as critical BIG-IP flaw is actively exploited (CVE-2020-5902 RCE & CVE-2020-5903 XSS)
- Why certain characters "glitch" Gmail, YouTube, and Twitter
- App generator tool JHipster Kotlin fixes fundamental cryptographic bug
- How public safety systems can be abused by nation state actors
- Unpatched Wi-Fi Extender Opens Home Networks to Remote Control
- After six months of stonewalling by Apple, app dev goes public with macOS privacy protection bypass
- Microsoft issues critical fixes for booby-trapped images – update now!

Breaches & Attacks

- The Perfect Art Heist: Hack the Money, Leave the Painting
- Incident: Re-generate API keys due to open Elasticsearch server
- Digital skimmer runs entirely on Google, defeats CSP: "CSP is practically worthless when you already have Google Analytics on your site"
- Lucifer: Devilish malware that abuses critical vulnerabilities on Windows machines
- Avaddon ransomware shows that Excel 4.0 macros are still effective
- California university pays $1 million ransom amid coronavirus research
- New Android Spyware Tools Emerge in Widespread Surveillance Campaign
- EvilQuest: Inside A 'New Class' of Mac Malware
- Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities
- Indian government hack exposes 80,000 coronavirus patients' data

Other news

- New Apple macOS Big Sur feature to hamper adware operations: “Apple has disabled the ability to silently install macOS profiles from the CLI in macOS 11, a measure that was widely employed by adware and malware gangs.”
- iOS 14 flags TikTok, 53 other apps spying on iPhone clipboards
- Infosec community disagrees with changing ‘black hat’ term due to racial stereotyping
- Inside the Plot to Kill the Open Technology Fund
- Barclays Bank appeared to be using the Wayback Machine as a ‘CDN’ for some Javascript
- What is Fetch Metadata? How to protect your web resources from information-stealing attacks
- 11 Weeks of Android: Privacy and Security
- Apple strong-arms entire CA industry into one-year certificate lifespans
- Apple tells app devs to use IPv6 as it’s 1.4 times faster than IPv4
- How Police Secretly Took Over a Global Phone Network for Organized Crime
- ‘Groundhog Day’ – Security experts decry latest US attempt to kill end-to-end encryption
- Guy Who Reverse-Engineered TikTok Reveals The Scary Things He Learned, Advises People To Stay Away From It
- AWS Facial Recognition Platform Misidentified Over 100 Politicians As Criminals

Non technical

- Things @sillydadddy learned in 6 months of bug hunting
- Bug Business #4 – Meet the Intigriti triage team: All your questions answered
- Mayonaise Joins The Ranks of The Seven-Figure-Earning Hackers
- YesWeHack Prophile on Sonny
- Researcher Spotlight: Caleb Kinney
- A summer learning list for better security awareness
- Obsession
- Digital Footprint – The first step in most offensive services
- How to stop Racists Pwning your mind

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You’re welcome to read them directly on Twitter: Tweets from 06/26/2020 to 07/03/2020.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com