Bug Bytes #72 – RCE in Google Cloud, Smuggling HTTP Headers & @filedescriptor's RPO Challenge

BY INTIGRITI · MAY 27, 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 15 to 22 of May.

Our favorite 5 hacking items

1. Tool of the week

Axiom

Project Axiom is a set of utilities for deploying and managing your own dynamic infrastructure on Digital Ocean. It includes different commands that you can use to work with VPS instances from the command line. Examples of actions available are launching a VPS instance, backing it up, connecting to it with SSH, deploying a VPN, etc.

An awesome, convenient project for bug hunters, red teamers and pentester!

2. Writeup of the week

RCE in Google Cloud Deployment Manager (Google, $31,337.00)

@epereiralopez found an SSRF that led to RCE on Google. Even though this finding required having a really good understanding of Google Cloud Manager, he does an awesome job of explaining everything in this pretty well written and descriptive writeup.

A very recommended read whether you want to learn about SSRF/RCE, getting max bounties on Google, testing Google Cloud Manager, or how to write great writeups!

3. Article of the week

Smuggling HTTP headers through reverse proxies

@RobinVerton shares a very interesting HTTP header smuggling technique. It exploits differences in how reverse proxies and WSGI frameworks (e.g. Django & Flask) handle header names.

If you're wondering how this relates to existing HTTP request smuggling research... @albinowax's techniques involved poisoning Web caches and desynchronizing systems. This new attack focuses on

smuggling HTTP headers with the goal of bypassing authentication or account takeovers. It is relatively easier, provided that you know/guess header names.

I'd also recommend checking out this article by The Daily Swig for a high-level summary.

4. Videos of the week

– @Agarri_Fr Talks About Burp Suite, SSRF, Security Research and Learning Web Application Hacking

– Filedescriptor solves Intigriti's XSS challenge | Exploiting an RPO attack on Firefox

These are two cool videos for anyone interested in Web app hacking and research. @NahamSec interviews @Agarri_FR who specializes in Web app hacking and fuzzing. Even though he does less bug hunting now, he is still well-known for his past research on SSRF and XML fuzzing that is still very relevant and referenced today, and for his unique Burp advanced training. So, it's nice to get to know him, his learning process, how we manages to find bugs without focusing on recon, how he picks research topics, etc.

In the video writeup, @filedescriptor solves Intigriti's May XSS challenge. He shows ho to trigger XSS by chaining Relative Path Overwrite (RPO) and Open redirect. A nice opportunity to learn about RPOs and less obvious XSS!

5. Tutorials of the week

– How to examine iOS network traffic over an iOS cable.

– Penetration Tester's Guide to Evaluating OAuth 2.0 — Authorization Code Grants

The usual method for proxying iOS traffic through Burp opens a Burp proxy listener that is exposed to the local network. But what if you're on a public network and do not want to expose it? @heald_ben shows how to do that by using a Jailbroken iOS device, an Apple cable, iproxy, and SSH tunneling.

The second tutorial is an introduction to OAuth security. It includes a summary of how OAuth 2.0 works (specifically the Authorization Code Grant), and how to test for some common security issues. I love how everything is structured. It provides a good basis to expand upon each time a new attack is discovered.

Other amazing things we stumbled upon this week

Videos

- How To Do Recon: Introduction to Recon
- Bug Hunting: Recon Methodology
- Bug bounty bits: Note taking
- PSW #652 – HTTP Security Headers In Action – Sven Morgenroth
- The Almost OnlyFans OSINT Challenge (and 100k subscribers!)

- SharpC2 Dev
- The Highest Paying Cyber Security Jobs (2020)
- Dynamic Analysis of Obfuscated Excel 4 Macros
- Auditing and Bypassing Windows Defender Application Control
- Stealing Hashes without Admin via Internal Monologue – Practical Exploitation

Podcasts

- Security Now 767 – WiFi 6
- Risky Business #584 — Nation-backed attackers own easyJet, jump airgaps, hack ports
- A Day in the Life of an Ethical Hacker Podcast Series: Interview with Nik Srivastava, Synack Red Team Member
- Cyberpunks Episode 9 – Penetration testing with Abartan Dhakal & 10 – Attack Surfaces with Abartan Dhakal
- Cyber Work Podcast – What's new in Ethical Hacking: Latest careers, skills and certifications
- 7MS #415: Cyber News
- SWN #35 – DEFCON Safe Mode, Ransomware Gangs, & SpaceX to ISS
- SWN #36 – Danny Trejo, Animal Crossing, Contact Tracing, & SaltStack – Wrap Up
- PSW #652 – Stuxnet, RCE's Everywhere, & Breach Chaos
- Naked Security Podcast S2 Ep 40: Demonic printers, a sleazy stalker and 10 reasons to patch

Webinars & Webcasts

- Attacking SQL Server CLR Assemblies
- Discord Hangout: Practical OAuth Attacks & Practical OAuth Abuse for Offensive Operations – Part 1
- Introduction to Secure Coding and OWASP Top 10
- ASC Webinars: CTFs and Bug Bounty Hunting and Their Relation To Professional Work – Ibrahim Mosaad
- Who's Your Hacker – Back on my Browser BBS Basic Browser Hacking- Charles "BSDBandit" Shirer
- Introduction to Certificates
- SANS webinars
    - Infosec Rock Star 2020: How to Accelerate Your Career

- SANS @MIC Talk – Using the OSINT Mind-State for Better Online Investigations
- SANS @MIC Talk – Moving Past Just Googling It: Harvesting and Using OSINT
- Building an Enterprise Grade Home Lab
- SANS @MIC Talk – Coalfire penetration testers charged with criminal trespass

Conferences

- Hacker RunDown 2020 & Schedule
- Detecting secrets in code committed to Gitlab (in real time) – Chandrapal Badshah
- Red Teaming DevOps – DEF CON Red Team Village Mayhem Summit

Slides & Workshop material

- EU ATT&CK Community Workshop

Tutorials

Medium to advanced

- Open Banking: Read/Write API & Tooling
- Unauthenticated SNS subscription removal
- iOS Swift Anti-Jailbreak Bypass with Frida
- When a CLI Falls for an Attacker
- Making the Perfect Red Team Dropbox (Part 1)
- Azure Web App Service For Offensive Operations
- Getting Started with Azure Automation DSC & Abusing Azure DSC — Remote Code Execution and Privilege Escalation

Beginners corner

- OAuth 2.0 Implementation and Security – Paper
- Seven Security (Mis)Configurations in Java web.xml Files
- Exploiting PHP deserialization
- Web Security 101: An Interactive Cross-Site Request Forgery (CSRF) Demo
- DOS File Path Magic Tricks
- RCE on Windows from Linux Part 3: Pass-The-Hash Toolkit

- Offensive Operations in Active Directory – #0 Taming Kerberos and making it our loyal companion & #1 Scatter the (h)ashes...

Writeups

Challenge writeups

- Intigriti May XSS Challenge winner & writeups

Responsible(ish) disclosure writeups

- 15 years later: Remote Code Execution in qmail (CVE-2005-1513) #RCE
- CVE-2020-11022/CVE-2020-11023: jQuery 3.5.0 Security Fix details & PoCs #Web
- Mattermost Enterprise Denial of Service #Web
- QNAP Pre-Auth Root RCE Affecting ~312K Devices on the Internet & Scanner #Web
- Analysis of CVE-2020-0605 – Code Execution using XPS Files in .NET #Deserialisation
- Docker Desktop for Windows PrivEsc (CVE-2020-11492) #Windows #PrivEsc
- Abusing WebRTC to Reveal Coarse Location Data in Signal #WebRTC
- Vulnerability in Google WordPress Plugin Grants Attacker Search Console Access #Web

Bug bounty writeups

- Stored XSS Leads to Plaintext Password Disclosure
- Parsing the DOM elements of Other pages via XSS: A Bug Bounty Story
- One Param => $10k & How to export parameters in Burp
- Easy bounties with subdomain discovery – Using Project Sonar for bug bounty (Bpost, $100)
- Multiple flaws leads to Account Takeover within an Application
- From XSS To CSRF | One-click Authorized Access To Account Takeover
- CVE-2020–1088 — Yet another arbitrary delete EoP (Microsoft)
- Disclosure of the name of a program that has a private part with an external link (HackerOne, $500)
- Chaining Bugs: Leakage of CSRF token which leads to Stored XSS and Account Takeover (xs1.tribalwars.cash) (InnoGames, $1,100)
- 404-response contains debug-information with all headers

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- CSTC, Modular HTTP Manipulator & Video tutorial: Cyber Security Transformation Chef, a Burp suite extension similar to CyberChef
- Shotlooter: A recon tool that finds sensitive data inside the screenshots uploaded to prnt.sc
- WEBSY & Introduction: Python tool for URL monitoring
- JWTweak: CLI tool that detects the algorithm of input JWT Token and provide options to generate the new JWT token based on the user selected algorithm
- Gitscraper: A tool which scrapes public github repositories for common naming conventions in variables, folders and files
- Authentication Token Obtain and Replace (ATOR), Introduction – Part 1 & Part 2: Burp extension for handling complex login sequences

More tools, if you have time

- WeirdAAL & Update info: AWS Attack Library
- CustomWordlistgenerator & Introduction: Python tool that takes a CMS repo/folder as input and generates a custom word-list based on its contents
- Safecopy: Burp Extension for copying requests safely when reporting vulnerabilities. It redacts headers like Cookie, Authorization & X-CSRF-Token
- H1 Report Finder: A burpsuite extension that helps security researchers find public security reports published on h1 based on the selected host
- localdataHog: String-based secret-searching tool (high entropy and regexes) based on truffleHog
- git-wild-hunt: A tool to hunt for credentials in github wild AKA git*hunt
- Decompiler: A decompiler extension for VS Code, that leverages Ghidra, IDA Pro & JadX/JD-CLI/dex2jar
- phpunit-brute: Tool to try multiple paths for PHPunit RCE CVE-2017-9841
- Powerob: An on-the-fly Powershell script obfuscator meant for red team engagements. Built out of necessity.
- Scout: A .NET assembly for performing recon against hosts on a network

Misc. pentest & bug bounty resources

- Q&A session with EdOverflow
- Bug bounty account take over check list

- Curated list of security tools for Hackers & Builders!

Challenges

- Documenting the impossible: Unexploitable XSS labs
- TerraGoat & Introduction: Vulnerable Terraform Infrastructure
- JWT lab, Source code & Walkthrough
- The d0nut 10k Challenge
- Can you #spotthebug in this code?

Articles

- NXNSAttack: upgrade resolvers to stop new kind of random subdomain attack
- Releasing the CAPTCHA Cracken & CAPTCHA22
- Weaponizing AWS ECS Task Definitions to Steal Credentials From Running Containers
- eBay port scans visitors' computers for remote access programs & Stealing Secrets from Developers using Websockets & Reddit discussion
- Abusing the osquery "curl" table for pivoting into cloud environments
- Using SharePoint as a Phishing Platform
- When Your Office Scanner Is Framed for Phishing
- Building a COM Server for Initial Execution & COMRunner

News

Bug bounty & Pentest news

- New Unc0ver jailbreak released, works on all recent iOS versions
- Notion is now free for personal use!
- Frida 12.9 Released
- Hacker Days: Kubernetes from a Attacker's Perspective: May 28
- Introduction to Bluetooth Low Energy Exploitation: May 28
- RSA Conference moves 2021 event from February to May
- [Survey] Better Bug Bounties

Reports

- Verizon's 2020 Data Breach Investigations Report & Daniel Miessler's Analysis of the 2020 Verizon Data Breach Report
- NTT's 2020 Global Threat Intelligence Report
- Chrome: 70% of all security bugs are memory safety issues

Vulnerabilities

- Smartphones, laptops, IoT devices vulnerable to new BIAS Bluetooth attack
- NXNSAttack technique can be abused for large-scale DDoS attacks
- Shielded web security flaws in QNAP storage devices finally released
- Signal patches (minor) approximate location disclosure flaw
- MyLittleAdmin has a big, unpatched security flaw
- Check Point released an open-source fix for common Linux memory corruption security hole
- Apple's MagicPairing for Bluetooth fails to enchant after mischief-making bugs found hiding in the stack

Breaches & Attacks

- Ragnar Locker ransomware deploys virtual machine to dodge security
- It wasn't just a few credit cards: Entire travel itineraries were stolen by hackers, Easyjet now tells victims
- Microsoft gives Office 365 admins the heads-up: Some internal queries over weekend might have returned results from completely different orgs
- Phishers are trying to bypass Office 365 MFA via rogue apps
- Houseparty denied it had been hacked... while miscreants were abusing its dot-com domain name infrastructure
- Hackers Say They Have Trump's 'Dirty Laundry' and Want $42 Million to Keep It Secret
- Hackers tried (and failed) to install ransomware using a zero-day in Sophos firewalls
- Beer rating app reveals homes and identities of spies and military bods, warns Bellingcat
- European supercomputers hacked in mysterious cyberattacks
- Mercedes-Benz onboard logic unit (OLU) source code leaks online

Other news

- To test its security mid-pandemic, GitLab tried phishing its own work-from-home staff. 1 in 5 fell for it

- Tech's Volkswagen moment? Trend Micro accused of cheating Microsoft driver QA by detecting test suite
- Microsoft: Here's why we love programming language Rust and kicked off Project Verona
- Alleged Hacker Behind Massive 'Collection 1' Data Dump Arrested
- NSO Group Impersonates Facebook Security Team to Spread Spyware — Report
- Attorney General: We didn't need Apple to crack terrorist's iPhones – tho we still want iGiant to do it in future
- Senate Votes to Allow FBI to Look at Your Web Browsing History Without a Warrant
- Winget: How to use Windows 10's new native Package Manager
- Windows Terminal 1.0
- Windows 10 Defender's hidden features revealed by this free tool
- How to enable the new Google Chrome 83 features now

Coronavirus

- Wuhan lab dossier debunked
- Apple and Google launch COVID-19 contact tracing API
- Dark web vendors feel the pinch as coronavirus lockdown restrictions impact underground operations
- Hackers preparing to launch ransomware attacks against hospitals arrested in Romania

Non technical

- I love to fail
- Bug Bounty Methodology...Just Have a Look.!
- It's Time to Get Back Into RSS
- Ethical dilemmas with responsible disclosure
- SAST vs DAST vs IAST
- In Flight Entertainment System Security

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 05/15/2020 to 05/22/2020.

Curated by Pentester Land & Sponsored by Intigriti

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com