Bug Bytes #27 – Secretz, Privilege Escalation on New Relic & How To Keep Your Bugs Organised

BY INTIGRITI · JULY 15, 2019 · LAST UPDATED ON JULY 31, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand.** Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

This issue covers the week from 05 to 12 of July.

Our favorite 5 hacking items

1. Tips of the week

> "– All you need to know to exit VIM without unplugging your laptop
> – 10 tips that are helpful if you are not finding vulns/bugs
> – Why http://1.0.0.1 is the same as http://1.1
> – How to use Tmux/Screen AFTER you've started Nmap"

These tweets are so good that I had to mention all four. They're about:

- How to exit VIM, and more importantly how to make `:!Q` (which isn't currently an option) quit it too
- Awesome advice to improve your environment and methodology, and start finding vulns/bugs
- Why some SSRF payloads include IP addresses like 1.1.1, and how routers know that it means 1.1.0.1 and not 1.1.1.0. I've been wondering about that and the answer was... RTFM!
- What to do when you're hours into an Nmap scan and you forgot to start it in a Tmux/Screen session (Genius!)

2. Writeup of the week

> "Privilege escalation via mass assignment on New Relic"

If testing for mass assignment isn't currently part of your methodology, this is an excellent opportunity to learn about it and start testing for it.
@albinowax was bug hunting on New Relic. He found that free accounts didn't have access to the API. But this restriction could be bypassed by intercepting a POST request to change your name and adding this parameter: *account[allow_api_access]=true*.
He also tells us how he guessed the parameter's name:

> "If you find a request updating/editing an object, be sure to run Param Miner on it – it might just find you a mass assignment vulnerability"

3. Webinar of the week

> "Securing Your Cloud Infrastructure | Security and Research Company (SECARMY)"

After last week's intro to cloud for pentesters and bug hunters, SECARMY returns with a sequel on common cloud security misconfigurations and their mitigations.
More specifically, this one is about SSRF and LFI on AWS, why they occur, how to detect them, how to leak AWS credentials and what companies can do to prevent it.

4. Tool of the week

> "Secretz"

A few weeks ago, @EdOverflow published the article "CI Knew There Would Be Bugs Here" — Exploring Continuous Integration Services as a Bug Bounty Hunter. He did the research with a few other hackers, and they developed a tool to automate fetching Travis CI build logs.
It allowed them to quickly look for sensitive information in CI logs and earn many bounties. It was awesome to read about that but they didn't release it because they didn't want to cause service disruptions to CI platforms.
I guess they've changed their minds because they've just released Secretz!
It minimizes the large attack surface of Travis CI by automatically fetching repos, builds, and logs for any given organization. So it's a really neat tool to add to your arsenal.

5. Non technical item of the week

> "How to better organize your notes while hunting for bugs"

Who doesn't like peeking at how other hackers organize their notes?
@GouveaHeitor shares here how he uses SwiftnessX to defines payloads, report templates and libraries / checklists. It's worth looking at his screenshots if you feel like your pentest/bug bounty notes could be better organized.

Other amazing things we stumbled upon this week

Videos

- Lets discuss SSRF/RCE.
- Wireshark Tips May 2019
- The Complete Beginner Network Penetration Testing Course for 2019 & Notes for Beginner Network Pentesting Course
- Information Gathering With Shodan
- Hacking with intruder
- Post Exploitation With Windows Credentials Editor (WCE) – Dump Windows Password Hashes

- Emirates NBD – Anti Phishing

Podcasts

- Security Now 722 – Gem Hack & Ghost Protocol
- Risky Business #547 — Zoom-gate, massive GDPR fines, ship hack warnings and more
- ThugCrowd S2:E6 – @hackgnar – BLECTF
- 7MS #371: Tales of Internal Pentest Pwnage – Part 4
- Darknet Diaries Ep 42: Mini-Stories: Vol 2
- Smashing Security 136: Oops, we created Iran's hacking exploit
- Security In Five Podcast – Episode 534 – Mozilla Is Tagged With 2019 Internet Villian, I Say Congrats
- Business Security Weekly #135 – Science, Ben Franklin, & Lessons
- Hack Naked News #226
- Paul's Security Weekly #611 – Porn Pirating, Zoom RCE, & Huawei
- Paul's Security Weekly #611 – Blue/Purple Teaming (defense)
- Application Security Weekly #68

Webinars & Webcasts

- An Intro to Application Whitelisting Bypasses

Conferences

- BSides Bristol 2019
- Introduction to Go

Slides only

- Android Apps – How easy is it to tear them apart and steal your data?
- TyphoonCon 2019 slides, especially:
  - NTLM Relay Risk Is Coming: A New Exploit Technique Makes It Reborn
  - Once Upon a Time in the West – A story on DNS Attacks
  - A Drone Tale, All Your Drones Are Belong To Us
- Effective Patch Analysis for Microsoft Updates

Tutorials

Medium to advanced

- How to write idempotent Bash scripts
- Abusing PHP query string parser to bypass IDS, IPS, and WAF
- IIS Application vs. Folder Detection During Blackbox Testing
- XSS Auditors – Abuses, Updates and Protection
- Mobile Hacking: Using Frida to Monitor Encryption
- Advanced Frida Witchcraft: Turning an Android Application into a Voodoo Doll
- Android 8.1 in qemu and Burp Suite SSL interception
- Hiding in the shadows at Members attribute
- Linux for Pentester: git Privilege Escalation, Pip Privilege Escalation & Sed Privilege Escalation
- Using macOS Internals for Post Exploitation

Beginners corner

- How to hack any Payment Gateway?
- Linux Fu: Named Pipe Dreams
- Introducing Rustbuster — A Comprehensive Web Fuzzer and Content Discovery Tool
- Collecting Contacts from zoominfo.com & Zoominfo-scraper
- Content Security Policy (CSP) explained including common bypasses
- What is a Man-in-the-Middle Attack and How To Avoid It?
- How you can transfer files with Whois command.
- Escaping restricted Linux shells like a boss

Writeups

Challenge writeups

- bnv – Google CTF 2019 Write-up (Video)
- CloudGoat Official Walkthrough Series: “rce_web_app”

Pentest writeups

- Path Traversal on multilingual feature

- Here's a quick #RedTeam (or rather #PenTest) walk-through of how I went from [Zero To Root] while testing an e-commerce website

Responsible(ish) disclosure writeups

- Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website! #Web
- Unsafe password reset in GLPI < 9.4.1 #Web #CodeReview
- Stored XSS in GLPI < 9.4.3 #Web #CodeReview
- Twitter Email Verification Bug let Hackers Impersonate Identities and Access Accounts on 3rd Party Services! #Web
- RCE Exploits of Redis Based on Master-Slave Replication #Web
- iOS URL Scheme Susceptible to Hijacking #Mobile
- Attacks on applications of k-anonymity for password retrieval: "Despite being promoted as protecting passwords, the model of k-anonymity used by Have I Been Pwned may allow a third-party server to learn user passwords. Affects password managers including 1Password and Bitwarden" #Web
- Second order SQL injection in ZoneMinder #Web
- Vulnerabilities in Nexus Repository left thousands of artifacts exposed #Web
- U-XSS in OperaMini for iOS Browser (0-Day) #Browser #Mobile
- Motorola – Directory Traversal Investigation #IoT
- Security Advisory: Targeting AD FS With External Brute-Force Attacks & TL;DR #ActiveDirectory

Bug bounty writeups

- Improper access control on VHX ($1,500)
- Business logic flaw on Upserve ($3,500)
- Blind SQL injection on Tube8 ($2,500)
- Forced browsing on HackerOne ($500)
- Privilege escalation on Maximum ($500)
- Jenkins RCE ($8,000)
- Open redirect / OAuth token theft / Account takeover on Airbnb
- Cleartext password in LocalStorage ($1,500)
- IDOR / Account takeover ($2,650)
- XSS on Google

- AWS misconfiguration

See more writeups on The list of bug bounty writeups.

Tools

- ScreenToGif: Allows you to record a selected area of your screen, edit and save it as a gif or video!. Useful for recording PoCs
- Qsreplace: A Go script to replace or append to query string values in URLs. Can be used in combination with waybackurls to generate URLs for fuzzing with a particular payload
- JWTrek: JWT Token C# Bruteforcer (HS256) (pure bruteforce, no wordlist yet)
- Android-App-Testing: Python3 scripts to help automate the installation of Burp Suite certificates on Android devices
- Venemy: OSINT tool for Venmo. It grabs profile information, friends lists & transactions
- BADministration & Introduction: Tool to leverage SolarWinds Orion servers from an offensive standpoint
- RedTeamCSharpScripts: C# Scripts for Red teaming
- Kali Linux Tools Interface: A graphical interface to use tools in Kali by the browser

Misc. pentest & bug bounty resources

- APIsecurity.io Issue 39: Vulnerable local Zoom webservers on 4+ mln Macs
- Infosec Income Questionnaire (Responses)
- Pepenote
- Useful-Python-Snippets
- Collection of CSP bypasses
- Bug bounty resources
- AWS Security Resources
- AWS AZURE Google Cloud Penetration Testing and Security
- Windows
- Null Pune (Discord channel)
- Red Team Phishing with Gophish.md
- Awesome Mainframe Hacking
- Awesome-Cellular-Hacking

Challenges

- WCTF 2019 & Solution (It's a new web exploitation technique dubbed the 'Antivirus Oracle')
- Secarmy CTF 2.0 Junior

Articles

- Hacking JavaScript with JavaScript – How to use parsers and other tools to analyze JavaScript
- Seriously, stop using RSA
- Security Testing of Thick Client Application
- Think Twice Before Adopting Security By Obscurity in Kotlin Android Apps
- Getting your head under the hood and out of the sand: Automotive security testing
- Cyber Kill Chain – Part 1
- Nuclear Meltdown with Critical ICS Vulnerabilities
- Abusing Common Cluster Configuration for Privileged Lateral Movement
- Executing Code Using Microsoft Teams Updater & Why popular apps like Slack & Discord can be used too

News

Bug bounty & Pentest news

- Coming soon on Burp Suite: Burp Repeater for Web sockets
- @Hacker0x01 is hiring Security Analyst for the Triage team in APAC & they're also hiring in EMEA & the USA
- SMB1 is disabled by default in Samba 4.11
- Chrome has started warning users about lookalike URLs

Reports

- Cybersecurity is the biggest threat to the world economy over the next decade, CEOs say
- 2018 Cyber Incident & Breach Trends Report

Vulnerabilities

- 'Zoom's performance has been fantastic... thanks to half their customers uninstalling it'
- Apple disables Walkie Talkie app due to vulnerability that could allow iPhone eavesdropping
- Bug in Anesthesia Respirators Allows Cyber-Tampering

- Interview of @logicbomb_1 by @HuffPostIndia over his recent finding in UPSRTC (the biggest fleet of buses in North India) exposing millions of user's PII data
- Two pentesters, one glitch: Firefox browser menaced by ancient file-snaffling bug, er, feature
- Hackers Hijacked VR Chatrooms to Manipulate Users' Reality
- Logitech Unifying Receivers Vulnerable to Key Injection Attacks
- GE Aviation server exposed in DNS misconfiguration

Breaches & Attacks

- Android malware silently infects 25m users in India
- Cyberattack lands ship in hot water
- Magecart crooks claim 17k victims with 'spray and pray' tactics
- Backdoor discovered in Ruby strong_password library

Malicious apps/sites

- Latest FinSpy Modules Lift Data from Secure Messaging Apps & The list of targetted apps
- Rogue Android apps ignore your permissions & Paper: 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System

Other news

- GDPR superpowers lead to whopper ICO fines for BA, Marriott: US $229.34 million million for British Airways & US $123 million for Marriott
- Facebook to be slapped with $5 billion fine for privacy lapses, say reports
- "Mozilla aren't villains after all" – ISPs back down after public outcry
- Google Home Silently Captures Recordings of Domestic Violence and More
- Top VPNs secretly owned by Chinese firms
- Metasploit Can Be Directly Used For Hardware Penetration Testing Now
- How to enable DNS-over-HTTPS (DoH) in Firefox

Non technical

- Remote-work resources
- Bug bounty : how to win the race against black-hat hackers ?
- Data Driven Bug Bounty

- Preserving Laptop Stickers on MacBooks
- How I got over my fear of public speaking
- Bug bounties and NDAs are an option, not the standard
- Types of Cybercrime and How to Protect Yourself Against Them
- Hacker vs Cracker: Main Differences Explained

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 07/05/2019 to 07/12/2019

Curated by Pentester Land & Sponsored by IntigritiDisclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.