Bug Bytes #37 – How to find more IDORs, Race Condition to RCE & Tracy

BY INTIGRITI · SEPTEMBER 24, 2019 · LAST UPDATED ON MARCH 6, 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 13 to 20 of September.

Our favorite 5 hacking items

1. Tutorial of the week

> "How to find more IDORs"

This tutorial explains how to find IDORs that are less obvious than just incrementing an ID. The techniques mentioned can be very helpful especially in the context of bug bounty.
Some of them are testing encoded & hashed IDs, adding an ID to the request even if the app didn't ask for it, changing the request method, etc.
Also, IDOR and self-XSS combined can lead to stored XSS, increasing the impact of the IDOR.

2. Writeup of the week

> "Race Condition that could Result to RCE – (A story with an App that temporary stored an uploaded file within 2 seconds before moving it to Amazon S3)"

@YoKoAcc, @JRs_Faisal and Tomi teamed up and found a whole bunch of bugs on a private program. They share multiple writeups that each explains different bugs.
This one is interesting because of the weird race condition. Here are my main takeaways:
They couldn't find any flaws in the main file upload functionality. But the file edit functionality allowed them to change already uploaded files to any extension (including PHP!). Nice way to get unrestricted file upload...
So they could upload Web shells, but didn't get RCE because uploaded files were moved to AWS after 2 seconds! And here is the weird part: for some reason, the request that modified the uploaded file was vulnerable to a race condition. By sending multiple requests, the server returned the file's location (before it is moved to AWS). So in the short window where the file was still on the server, they got a reverse shell by requesting the file in a browser.
Not sure why this is happening, but it's interesting to see a race condition help get RCE via file upload!

3. Tool of the week

> "Tracy"

Most tools that help with XSS detection are limited because they rely on server response reflection. Tracy tries to go further by helping you identify sources of input and their corresponding outputs (or sinks). You can trace risky input throughout the DOM, even in apps that use a lot of JavaScript. This helps detect harder-to-find XSS types like DOM XSS.
The only other tool I've seen efficiently help with this was DOMinator Pro, but it was commercial and I can't find it online anymore. So it is awesome to have a free open source alternative!

4. Non technical item of the week

> "Problems I have faced in Bug Bounty"

I really enjoyed reading this article. After 2 months of bug hunting, @Unknownuser1806 shares 6 problems he faced and how he solved them.
They revolve around productivity and mental health. I feel that we can easily lose sight of these topics when we get engrossed in hacking. Burnout is never that far... So the refresher is great! It's also nice to see the specific tools a fellow bug hunter found helpful: Engross App, Habitica, Evernote/Diary, Morning habits, meditation & exercise.

5. Tips of the week

> "– If you can't access the admin panel, try discovering the javascript files for the admin section! E.g. if /admin/ is restricted try and see if /admin/js or similar exists and brute in front of there
> – While registering account there's no fields like address or about me, but they're exist on the page where you can edit your info after registering account. Try to add them while registering another account and paste payloads in values, this can bypass (XSS/injection) protection"

There's not much to comment here, the tips are self-explanatory.
I've never encountered these ideas before and think they're worth adding to any Web testing methodology!

Other amazing things we stumbled upon this week

Videos

- Web Hacking Pro Tips #18: @tomnomnom Tom Hudson
- Struggling with Hacker101's GraphQL CTF and solving an XSS challenge from Bug Bounty Notes!
- 09/01/2019 – Live Bug Bounty Recon Session on Yahoo (censys, altdns, amass) w/ @infosec_au
- Watchdogs 2 and hacking on Yahoo

Podcasts

- Ladybug podcast – What The Heck Is GraphQL?
- Influencing Bug Bounty Hackers with STÖK
- Security Now 732 – SIM Jacking

- Darknet Diaries EP 47: Project Raven
- 7MS #381: DIY $500 Pentesting Lab Deployment Tips
- Risky Business #556 — US Treasury targets DPRK crews, more details on Ukraine power hack
- Alissa Knight talks API security, formjacking and hacking
- PSW #620 – iOS, Equifax Is Back, & phpMyAdmin CSRF Zero-Day
- HNN #234

Webinars & Webcasts

- A day in the life of a penetration tester – Part 3 & Part 4

Conferences

- SEC-T – 0x0Compute, especially:
  - Chinese Police and CloudPets
  - Pwning AWS Cloud services

Slides only

- Continuous Integration Continuous Bounties
- Android Mobile App Pentesting
- Adversary Emulation using CALDERA
- Elbsides 2019 Bettercap Workshop
- OWASP Find Security Bugs

Tutorials

Medium to advanced

- Server Side Template Injection – on the example of Pebble
- Diving into unserialize()
- How to: Kerberoast like a boss
- Linux reverse shell without python
- Dynamic Instrumentation: Frida And r2frida For Noobs
- Metasploit Framework console on Docker. (with workspace)
- Microsoft Exchange – Privilege Escalation

- Container Runtime Security Bypasses on Falco

Beginners corner

- Hacking with AWS: incorporating leaky buckets into your OSINT workflow
- How to bypass Android certificate pinning and intercept SSL traffic
- 8 Vim Tricks That Will Take You From Beginner to Expert
- Psexec: The Ultimate Guide
- Explaining Server Side Template Injections
- Open redirect Vulnerability and How To Not Mess It Up!

Writeups

Challenge writeups

- DerbyCon 2019 CTF Write Up #Web
- DroidCon, SEC-T CTF 2019 #Android
- 44Con HackerOne CTF write up #Web

Pentest writeups

- More Than a Penetration Test (Microsoft Windows CVE-2019–1082)
- Recon To Network Takeover

Responsible(ish) disclosure writeups

- Security: HTTP Smuggling, Apache Traffic Server #Web
- HAProxy HTTP request smuggling #Web
- Security Vulnerabilities in Network Accessible Services #Web
- Azure AD privilege escalation – Taking over default application permissions as Application Admin #ActiveDirectory
- SSRF | Reading Local Files from DownNotifier server #Web
- D-Link DNS-320 ShareCenter <= 2.05.B10 – Unauthenticated Remote code execution #RCE #CodeReview

Bug bounty writeups

- Account takeover via Stored XSS & CSRF on Dolibarr
- DOM XSS on Shopify ($500)

- IDOR on GitLab ($1,000)
- Information disclosure via Github on Twitter ($280)
- Information disclosure on Zomato ($750)
- Web cache deception on OLX

Tools

If you don't have time

- Pixload: Image Payload Creating/Injecting tools
- Bass: A tool that combines valid DNS resolvers from various DNS Providers of your target and generates a maximum final list of DNS resolvers. Add anywhere from 100-4k resolvers to your 'resolver.txt' (TL;DR)
- Docem: Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)
- Curryfinger & Introduction: A Go tool for finding the server behind popular CDNs through SNI & Host header spoofing

More tools, if you have time

- Dupe Key Injector: A Burp Suite extension implementing Dupe Key Confusion, a new XML signature bypass technique presented at BSides/BlackHat/DEFCON 2019 "SSO Wars: The Token Menace" presentation
- G-Calendar-Audit: A Python script to check for public Google calendars
- Lockdoor Pentesting Framework: A Penetration Testing framework with Cyber Security Resources
- Dnmasscan: A script that can resolve an input file of domains & scan them with masscan
- EZDomain: Python script for subdomain, file, directory & S3 bucket bruteforce
- Dr Robot: A tool for Domain Reconnaissance and Enumeration
- Dolos Cloak: Automated 802.1x Bypass
- Cryptbreaker & Introduction: A cloud-backed password cracking and assessment tool

Misc. pentest & bug bounty resources

- 12 OSINT Resources For E-mail Addresses
- Zen Rails Security Checklist: Checklist of security precautions for Ruby on Rails applications
- Open Redirect Payload List
- Awesome Shodan Search Queries

- Ptest Method
- Bug bounty hunters starter notes

Challenges

- VyAPI & How to make the best of it
- Vulnerable single sign on & Install tip
- Kubernetes Local Security Testing Lab

Articles & Papers

- Automating Exploitation of a Pulse SSL VPN Arbitrary File Read Vulnerability & pwn-pulse.sh
- How to Get a Finger on the Pulse of Corporate Networks via the SSL VPN
- Deserialization Bugs in the Wild
- Leveraging Javascript Debuggers for compromise
- Reversing HackEx – An android game
- Patch Analysis: Examining a Missing Dot-Dot in Oracle WebLogic
- Affordable USB Attack Device: Part 1
- Abusing VPC Traffic Mirroring in AWS
- Defense Informs Offense Improves Defense — How to Compromise an Industrial Control Systems Network – and How to Defend it

News

Bug bounty & Pentest news

- 2019 CWE Top 25 Most Dangerous Software Errors: CWE Version 3.4 released
- Samba 4.11.0 released: SMB1 disabled by default, LanMan and plaintext authentication deprecated
- The ex-felon who has made $1 million as a hacker, legally
- LevelUp0x05 is coming live to you on Saturday, October 5!
- Web Security Academy Hall of fame

Reports

- Report: Use of AI surveillance is growing around the world

Vulnerabilities

- Security Analysis of LastPass credential leak — By bypassing do_popupregister()
- Patch now: Exploit released for WordPress plugin RCE bug
- Alarm over zero-day cross-site request forgery in phpMyAdmin

Breaches & Attacks

- Marketing Analytics Company Leaks Deep Profiles of Entire Ecuador Population
- Mattress Company Exposes 387k Customer Records Online
- Scanner or Scammer: Analysis of CamScanner Vulnerability
- Phishing Attack Targets The Guardian's Whistleblowing Site
- Clones of popular Ad blockers caught ad frauding millions of Chrome users
- Payment card thieves hack Click2Gov bill paying portals in 8 cities
- Researchers find 737 million medical images exposed on the internet
- New clues show how Russia's grid hackers aimed for physical destruction
- WannaCry – the worm that just won't die
- Exclusive: Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil

Malicious apps/sites

Other news

- Disqus & Kickstarter hacker warns against password reuse
- Air Force to offer up a satellite to hackers at Defcon 2020
- US files suit against Snowden to keep book profits out of his hands
- New Documents About Pentesters Jailed for Courthouse Break-In & This article does not paint Dallas County (Iowa not Texas) Sheriff Chad Leonard in a pretty light

Non technical

- Banks, Arbitrary Password Restrictions and Why They Don't Matter
- The Most Important Productivity Lesson I Ever Learned
- Unusual Journeys into Infosec Featuring Phillip Wylie

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 09/13/2019 to 09/20/2019.

Curated by Pentester Land & Sponsored by Intigriti

Disclaimer:The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.