Bug Bytes #35 – DerbyCon Roundup, From Zero To Admin & Same-Origin Summarised

BY INTIGRITI · SEPTEMBER 10, 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 30 of August to 06 of September.

Intigriti news

- Can you social engineer our receptionist?
- Check out our new sponsored video from **PwnFunction** ft. **LiveOverflow**: Paste-Tastic! ft. LiveOverflow – Google CTF 2019 Write-up

Our favorite 5 hacking items

1. Conference of the week

> "DerbyCon 9, especially:
> – To CORS! The cause of, and solution to, your SPA problems! & CORS Exploitation Framework (CEF)
> – REST in Peace: Abusing GraphQL to Attack Underlying Infrastructure
> – Assumed Breach: A Better Model for Penetration Testing
> – Kerberoasting Revisited
> – Old Tools, New Tricks: Hacking WebSockets
> – Full Steam Ahead: Serverless Hacking 101
> – Red Team Methodology: A Naked Look
> – API Keys, Now What?Taking the Pen Test Into the Amazon Cloud
> – Red Team Level over 9000! Fusing the powah of .NET with a scripting language of your choosing: introducing BYOI (Bring Your own Interpreter) payloads"

DerbyCon 9 had so many good talks! I'm particularly interested in the ones on CORS, Kerberoasting, WebSOckets, GraphQL, Serverless, API security & red teaming, but many other topics were discussed. Too bad, this was the last DerbyCon conference!

2. Writeup of the week

> "Add new user with Admin permission and takeover the organization"

This is the writeup a privilege escalation on a private program. Starting with a limited user account and no API documentation, the author was looking for admin endpoints.
He tried common ones like */api/v2/member/*, */api/v2/members/*, */api/v2/users/*, */api/v2/user/*... And noticed that existing and non-existing endpoints returned different HTTP codes.
api/v2/user returned a 405 (the method is not allowed). Changing the method from GET to POST, and

adding all parameters reported missing by the server, he was able to construct a valid POST request and create a new user. But the reset password functionality didn't work for that user until he passed the right value (found by bruteforce) to a specific parameter during user creation.
Then he was able to create an admin user by adding "role"="admin" to the request.
This whole process isn't complicated but I love how the author relies on parameters guessing and bruteforce, and also chains multiple actions to find hidden functionality and overcome any obstacle faced.

3. Article of the week

> "Same-Origin Policy: From birth until today"

The Same Origin Policy is an essential concept for Web app testers. This article presents the results of research on SOP and CORS on different browsers, as well as 2 CSRF bugs and how CSRF and SOP are related.
The author's conclusion: "do not use IE or Edge"... They violate the SOP standard, which makes them more vulnerable.

4. Tool of the week

> "gitGraber"

This is a great tool for Github recon. I've never seen one like it for two reasons: it does live monitoring with Slack notifications, and it searches all Github not only organization repositories. So even if a developer has a profile that is not explicitly linked to your target organization, gitGrabber will still search for secrets in this repository.
The syntax is basically *gitGraber.py -k KEYWORDSFILE -q QUERY,* where QUERY can be your target organization (e.g. yahoo) and KEYWORDSFILE is a file containing keywords like access_key, password, auth...
The tool looks for sensitive data for several online services (Google, Amazon, Paypal, Github, Mailgun, Stripe...) based on regexes and notifies you when potentially sensitive information is found.

5. Videos of the week

> "TomNomNom answers questions for 4 hours straight
> 8/25/2019 – Live Bug Bounty Recon Session w/ @FransRosen"

This livestreaming trend by bug hunters is getting crazy! I find it harder and harder to keep up with the pace. But these two videos are on the top of my list of things to watch this week.
@tomnomnom answers questions for more than 4 hours. They touch on everything from his peanut butter preferences to why he doesn't do bug bounty full-time, burnout, VIM, getting into bug bounty, etc.
The stream by @NahamSec covers topics like asset discovery and API fuzzing, and a ~1 hour interview with @fransrosen. I'm a big fan of his, so it's awesome to hear about his recon approach, research he's working on, why he doesn't automate everything, etc.

Other amazing things we stumbled upon this week

Videos

- Solving challenges from Hacker101 (GraphQL) and Bug Bounty Notes (SSRF) – Every Tuesday!
- TomNomNom answers questions for 4 hours straight
- 8/25/2019 – Live Bug Bounty Recon Session w/ @FransRosen
- Bugcrowd University @ CSUF – Crash Course on Penetration Testing
- Web App Testing: Episode 4 – XXE, Input Validation, Broken Access Control, and More XSS
- hacker:HUNTER
- How They Got Hacked Episode 25

Podcasts

- Security Now 730 – The Ransomware Epidemic
- 7MS #380: Tales of Internal Network Pentest Pwnage – Part 8
- Darknet Diaries EP 46: XBox Underground (Part 2)
- Risky Business #554 — Is there an iOS exploit glut?
- Hack Naked News #232
- Security In Five Episode 574 – How Did The CEO Of Twitter Get His Account Hacked

Webinars & Webcasts

- Seth & Ken's Excellent Adventures in Secure Code Review
- Don't Open These– The Five Most Dangerous File Types (Free registration required)

Slides only

- Malicious JS code

Tutorials

Medium to advanced

- Kubernetes Pentest Methodology Part 2
- PowerShell Productivity Hacks: How I use Get-Command

- Bypass GuardDuty PenTest Alerts
- Raspberry Pi Remote Access: Stealthy Approach to Internal Network Penetration Testing
- PowerShell, Azure, and Password Hashes in 4 steps
- Weak DPAPI encryption at rest in NordVPN
- Microsoft Exchange – Domain Escalation
- Microsoft Exchange – Password Spraying

Beginners corner

- Asset Enumeration: Expanding a Target's Attack Surface
- Use Sqlmap to find XSS vulnerabilities!
- Data Extraction to Command Execution CSV Injection
- (RCE) as root on Marathon-Mesos instance

Writeups

Challenge writeups

- Intigriti challenge writeups by the winner, @ride_faster & @Fady_Othman

Pentest writeups

- RCE using Path Traversal
- Bypassing Citrix , Firewall Restrictions & DLP to exfiltrate data using Grammarly
- From thick client exploitation to becoming Kubernetes cluster Admin — The story of a fun bug we found and it's exploitation

Responsible(ish) disclosure writeups

- Multiple WordPress Plugins SQL Injection Vulnerabilities #CodeReview #Web
- Bitbucket 6.1.1 Path Traversal to RCE #CodeReview #Web
- Virtual Media Vulnerability in BMC Opens Servers to Remote Attack #USB
- CVE-2019–11380 | How I was able to access complete storage of ES-FileExplorer End user #Android
- Microsoft Edge – Universal XSS #BrowserExploitation

Bug bounty writeups

- Stored XSS on GitLab ($4,500)

- Stored XSS via email on GitLab ($750)
- Information disclosure on GitLab ($750)
- IDOR on HackerOne
- Information disclosure on HackerOne ($500)
- Email verification bypass on GitLab ($3,000)
- Password reset flaw
- Information disclosure via GraphQl
- Information disclosure on HackerOne ($500)
- RCE on Facebook ($1000)
- Information disclosure via JSONP exploitation
- XSS on Google

Tools

If you don't have time

- TorIpRotate: Simple burp extension for routing traffic over tor. It instruments tor to switch to a new circuit after every N requests.

More tools, if you have time

- Requests-Racer & Introduction: A Python Library for Exploiting Concurrency-Related Vulnerabilities in Web Applications
- massNS: A tool that turns the authoritative nameservers of DNS providers to resolvers and resolves the target domain list
- Encoderama: String or worldlist encoder for use in fuzzing or web application testing
- Liffier: Tired of manually add dot-dot-slash to your possible path traversal? this short snippet will increment ../ on the URL
- C3 & Introduction: Custom Command and Control (C3). A framework for rapid prototyping of custom C2 channels, while still providing integration with existing offensive toolkits
- SharPersist & Introduction: Windows Persistence Toolkit in C#
- ActiveReign: A Network Enumeration and Attack Toolset. Similar to CrackMapExec with less functionalities but with a few modifications that might be handy
- Httptools: A python package that lets you to capture, repeat and live intercept HTTP requests with scripting capabilities, built on top of mitmproxy

Misc. pentest & bug bounty resources

- /dev/random – One Liner For Installing Burp Certificate Into Android Nougat and Later
- Breaking Into Information Security A Modern Guide
- Notes about attacking Jenkins servers
- AllThingsSSRF
- Learn Powershell Series

Challenges

- GTH CTF challenge: XSS, IDOR, injection, content discovery, enumeration, bruteforce...

Articles

- Attacking SSL VPN – Part 3: The Golden Pulse Secure SSL VPN RCE Chain, with Twitter as Case Study!
- Red Teamer's Guide to Pulse Secure SSL VPN
- Analyzing a Creative Attack Chain Used to Compromise a Web Application
- Security analysis of \ element
- Goodbye XSS Auditor
- A Closer Look at Recent HTTP/2 Vulnerabilities Affecting K8s and Other Implementations
- Gaining Persistency on Vulnerable Lambdas
- Stealthier persistence using new services purposely vulnerable to path interception
- Thoughts on the Capital One Security Breach
- Adventures in the Wonderful World of AMSI

News

Bug bounty & Pentest news

- @daeken's Bounty Progress – September 2019
- Kali Linux 2019.3 Release
- Initial Metasploit Exploit Module for BlueKeep (CVE-2019-0708)
- Next Gen Pen Test – The Researcher's Role
- Android exploits are now worth more than iOS exploits for the first time

Reports

- 2019 Insider Threat Report

Vulnerabilities

- Critical Exim TLS Flaw Lets Attackers Remotely Execute Commands as Root
- How MuleSoft patched a critical security flaw and avoided a disaster
- Cyber Experts Warn Of Vulnerabilities Facing 2020 Election Machines
- 600,000 GPS trackers for people and pets are using 123456 as a password
- Blindly accepting network update texts could have pwned your mobe, say researchers
- Zero-day disclosed in Android OS

Breaches & Attacks

- A huge database of Facebook users' phone numbers found online
- Fraudsters deepfake CEO's voice to trick manager into transferring $243,000
- Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran
- Data of 90K Mastercard Priceless Specials Members Shared Online
- Thousands of IoT Devices Bricked By Silex Malware
- This Crime Fighting App Is Leaking Criminals', Citizens and Even Police's Info
- iPhone attack may have targeted Android and Windows too

Malicious apps/sites

Other news

- How to keep spam from invading your Google Calendar
- Apple's $1 million bug bounty makes a lot more sense after that iOS hacking spree
- Astaroth Trojan Uses Cloudflare Workers to Bypass AV Software
- China's new face-swapping app Zao gets whiplash-fast privacy backlash –Apple disputes Google's accuracy on recent iOS hacks, and they may be right

Non technical

- Wrapping or modifying?
- Can we have a word about CVs?
- Day-1 Skills That Cybersecurity Hiring Managers Are Looking For

- How to build an internal red team?
- The Definition of a Green Team

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 08/30/2019 to 09/06/2019

*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.