Bug Bytes #80 – CI/DC kung fu, Path traversal via email & Pro DevTool tips

BY ANNA HAMMOND · JULY 22, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-80-ci-dc-kung-fu-path-traversal-via-email-pro-devtool-tips

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 10 to 17 of July.

Our favorite 5 hacking items

1. Videos of the week

Improve Your Hacking Skills Using Devtools | Bug Bounty Tips

Filedescriptor Talks About Learning Javascript for Hacking, Reconless, Hacking Twitter and More!

HUNTing with OptionalValue and hakluke

If you're short on time and want to learn something really useful, watch the first video. In literally 5 minutes, @filedescriptor shares amazing Devtools tips for bug hunters. And if you can't get enough of him, watch the @NahamSec interview (second video) where they discuss topics like recon, bug hunting methodology, learning JavaScript, etc.

The last video is an excellent introduction to the new HUNT Burp extension. A must watch if you want to learn what it is for and how to quickly start using it.

2. Writeup of the week

Write-up for a Path Traversal on Gravitee.io

Which impact level do you have in mind when you hear about HTML injection in emails?

If you're thinking low or medium impact, check out this creative writeup. @Fisjkars injected an image tag with a path traversal payload as the URL. Since the HTML code injected was rendered server-side, it became a path traversal bug with access to sensitive files. In other words, HTML injection + email = Path traversal.

3. Articles of the week

Abusing GitLab Runners

Shaking secrets out of CircleCI builds – insecure configuration and the threat of malicious pull requests & circleci-logs

© Intigriti

Both articles are about exploiting CI/DC tools for recon.

The first one shows how to use GitLab runner registration tokens you find to access the data of private Gitlab instances (even if you only have the token without context).

The second article extends past research on Travis-CI to CircleCI. It comes with a mini-CTF. Will you be able to find the flag before reading about the new technique?

4. Tool of the week

HeapProfiler Snapshot relative URL extractor

In the DevTools video mentioned above, @filedescriptor talked about using the Memory tab to extract API paths from heap snapshots. @smiegles took this idea and made it into a headless Node.js script that automates the process.

5. Resources of the week

OAuth 2.0 Playground & OAuth 2.0 Flow Simulator

If you find OAuth flows complicated to apprehend, these resources will be helpful. They are like demos that help see how different types of OAuth 2.0 and OpenID Connect flows work in practice.

The added value compared to just analyzing OAuth requests/responses on a bug bounty target, is that you'll find explanations on back channel (backend) requests that aren't visible in browsers.

Other amazing things we stumbled upon this week

Videos

- How easy is it to tweet as anyone? | Twitter Hacks & Bug Bounty
- How Pros Use CVEs to Find New Bugs (before anyone else! ft CVE-2020-5902)
- HACKING GraphQL FOR BEGINNERS + GIVEAWAY!
- Patreon CEO shares his most epic failures
- Did you know you can chain IDORs?
- Talon
- Interview With A Web Application Pentester – Tib3rius
- Real Bugs – API Information Disclosure
- Confused Deputy Problem Explained
- Exploit Development – Finding Zerodays With Github

Podcasts

- Security now – EARN IT is Still Evil, Google Tsunami

© Intigriti

- 7MS #423: Tales of Internal Pentest Pwnage – Part 18
- The InfoSec & OSINT Show 15 – Chris Dale & Breaking up Recon from the Pen Test
- SWN #48 – Wrap Up – F5-BIGIP RCE, Zoom 0-Day, & Apache Guacamole RCE

Webinars & Webcasts

- SANS@MIC- Git'ing Users for OSINT: Analysis of All GitHub Users
- Webcast: Securing Active Directory: Protecting AD Administration

Conferences

- Null Ahmedabad July 2020 Meetup (Kubernetes 101, Attacks on JWT, Intro to Metasploit & USB Forensics)

Slides & Workshop material

- SANS@MIC – The 14 Absolute Truths of Security

Tutorials

Medium to advanced

- How to prevent HTML email injection in Python web apps
- How to further automate your Flickr searches?
- DLL Proxy Loading Your Favourite C# Implant
- Advanced TTPs – DotNetToJScript (Part 1), Part 2 & Part 3
- A Developer's Introduction to Beacon Object Files
- Improving Packet Capture Performance – 1 of 3
- Using Visual Studio Code Extensions for Persistence
- Antimalware Scan Interface Provider for Persistence
- Bypassing LSA Protection (aka Protected Process Light) without Mimikatz on Windows 10

Beginners corner

- Under the hood: Hiding data in JPEG images
- WebView – Android's most convenient footgun
- Azure File Shares for Pentesters
- Keep your eyes open: How to avoid exposing your internal proxy
- How to Geolocate Mobile Phones (or not)

© Intigriti

- HTTP(s) C2 Pivoting

Writeups

Challenge writeups

- Marginwidth/marginheight – the unexpected cross-origin communication channel
- Gynvael Web Challenge #6

Pentest writeups

- Bypassing AWS WAF CRS with Cross-Site-Scripting (XSS) payload
- How I Bypassed Crowdstrike Restriction
- Android App Source code Extraction and Bypassing Root and SSL Pinning checks

Responsible(ish) disclosure writeups

- SIGRed – Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers #DNS #Windows
- Sophos XG – A Tale of the Unfortunate Re-engineering of an N-Day and the Lucky Find of a 0-Day #Web #CodeReview
- RCE in F5 Big-IP #RCE
- Tesco coupons easily faked to save £750 on Hotels.com bookings worldwide
- CVE-2020-13405: MicroWeber Unauthenticated User Database Disclosure #Web
- Threat modelling and IoT hubs #IoT

Bug bounty writeups

- How An API Misconfiguration Can Lead To Your Internal Company Data
- How I was able to change victim's password using IDN Homograph Attack ($600)
- Race Conditions – Exploring the Possibilities
- How we were able to delete Donald Trump posts on Facebook ? (Facebook, $10,000)
- The 3 Day Account Takeover
- Server Side Template injection to RCE (via CSRF token) (Video)
- Blind SSRF on https://labs.data.gov/dashboard/Campaign/json_status/ Endpoint (TTS Bug Bounty, $300)
- File writing by Directory traversal at actionpack-page_caching and RCE by it (Ruby on Rails)
- Account takeover intercepting magic link for Arrive app (Shopify, $500)

© Intigriti

- Ability to bruteforce mopub account's password due to lack of rate limitation protection using {ip rotation techniques} (Twitter, $420)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Mitmdump script to dump incoming HTTP requests to Slack
- PwnMachine & Intro: A self hosting solution based on docker aiming to provide an easy to use pwning station for bughunters
- getjswords.py: Simple Python tool for find a unique words in javascript files, help the bughunters to create a wordlist for the company (e.g for brute force the hidden params,..etc)
- Urlgrab: A golang utility to spider through a website searching for additional links
- fdnssearch: Swiftly search FDNS datasets from Rapid7 Open Data

More tools, if you have time

- Lazy: An example that shows how to create an axiom box that includes existing tools & resources
- Pscan: A parallel scanner that utilises axiom to spin up servers and parallel scan using masscan
- CodeArgos: Detect and watch for changes to Javascript files and scriptblocks of a target web app
- postMessageFinder: A tool that checks if a set of urls contains one or more postMessage functions or eventhandlers
- magiskfrida: Run frida-server on boot with Magisk
- reNgine: A python automated recon framework (with GUI)
- Bopscrk: Wordlists generation tool
- Convert Text to SQL Char
- SierraTwo: Simple reverse shell over Slack
- SuperTruder: An intruder custom that gave me bounties
- Netenum: A tool to passively discover active hosts on a network
- SqlClient & Intro: POC for .NET mssql client for accessing database data through beacon

Misc. pentest & bug bounty resources

- BugBug Bounty Roadmaps
- OAuth 2.0 Playground & OAuth 2.0 Flow Simulator
- Pentesting Git source repositories

© Intigriti

- S4P-DIR.txt
- Awesome AWS Security
- CTF-Katana: A listing of tools and commands that may help with CTF challenge
- Introduction to Reverse Engineering with Ghidra

Challenges

- DVTA 2.0: A Damn Vulnerable Thick Client App developed in C# .NET
- @terjanq's Harder XSS Challenge

Articles

- Escaping JavaScript sandboxes with parsing issues & Attacking and defending JavaScript sandboxes
- X Site eScape (Part I): Exploitation of and Old CoreFoundation Sandbox Bug
- That loyal MySQL is a rogue one: a tale of a (partially) failed idea
- Advanced VBA macros: bypassing olevba static analyses with 0 hits
- Copy pasting the copy-paste adversary for ｌｕｌｚ science.
- Testing Ripple20: A closer look and proof of concept script for CVE-2020-11898
- Requesting Azure AD Request Tokens on Azure-AD-joined Machines for Browser SSO

News

Bug bounty & Pentest news

- Launching Burp Suite's preconfigured browser (2020.7 release) (video)
- Burp Suite roadmap update: July 2020
- h@cktivitycon
- Your Mission, If You Choose to Accept It: LevelUp0x07
- Auth Bypass Bugs (on Google)

Reports

- Adventures of an SSH Honeypot
- Remote working during coronavirus pandemic leads to rise in cyber-attacks, say security professionals
- Over Half of Cyber Security Professionals Affected by Overwork or Burnout, CIISec Survey Finds

© Intigriti

Vulnerabilities

- Microsoft resolves 'wormable' DNS security vulnerability, PoC 1, PoC 2, Fake PoC & Webinar: What You Need to Know About the Windows DNS Vulnerability – CVE-2020-1350
- So kind of SAP NetWeaver to hand out admin accounts to anyone who can reach it. You'll want to patch this, CVE-2020-6287: Critical Vulnerability in SAP NetWeaver Application Server (AS) Java, PoC 1 & PoC 2
- The July 2020 Security Update Review
- This week of never-ending security updates continue. Now Apple emits dozens of fixes for iOS, macOS, etc
- Finally done with all those Patch Tuesday updates? Think again! Here's 33 Cisco bug fixes, with five criticals
- Fixing the Zoom 'Vanity Clause'
- Rust programming language: Crates package API tokens revoked over serious security flaw

Breaches & Attacks

- Twitter hack saga:
  - Twitter mass hacking: Bill Gates, Elon Musk, Jeff Bezos, Mike Bloomberg, Biden, Obama, more hijacked to peddle Bitcoin scam
  - Twitter says hackers downloaded the data of eight users in Wednesday's hack
  - Justin Sun is putting out a $1 million Bounty for the hackers
- Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the internet
- Russian hackers target COVID-19 vaccine research with custom malware
- Android chat app uses public code to spy, exposes user data
- Diebold Nixdorf warns of a new class of ATM 'black box' attacks across Europe

Other news

- EU-US Privacy Shield data-sharing framework declared invalid by ECJ: "The landmark decision means that companies seeking to transfer the personal data of EU-based customers to the US must instead sign legal contracts similar to those used by other countries."
- Inside America's Secretive $2 Billion Research Hub Collecting Fingerprints From Facebook, Hacking Smartwatches And Fighting Covid-19
- Iranian cyberspies leave training videos exposed online
- Abracadabra! – CryptBB demystifying the illusion of the private forum
- Report: CIA runs secret cyberwar with little oversight after Trump gave the OK, say US government officials
- EFF's new database reveals what tech local police are using to spy on you

© Intigriti

Non technical

- Bug Business #6 – Get to know Robin, Intigriti's Top Hacker in Q1
- Hacker Spotlight: Interview with rijalrojan
- Bugcrowd Spotlight: Maxim G
- Meet APAC Hacker @jin0ne: A Next Generation Cyber Defender
- Searching for the Ultimate Obstacle to Creativity
- Comparing 3 Great Web Security Books
- The Four Phases of Offensive Security Teams
- From N00b To OSCE In 18 Months

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 07/10/2020 to 07/17/2020.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

© Intigriti