Bug Bytes #2

BY INTIGRITI · JANUARY 23, 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. You can sign up for the newsletter here.*

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week. This issue covers the week from 11 to 18 of January.
Big thanks to Intigriti for sponsoring this newsletter!

Our favorite 5 hacking items

1. Tool of the week

> "bugbounty.link"

This is a URL shortening service. What's great about it is that it supports any protocol (file, gopher, etc). So it can be useful to test for SSRF or open redirects, and bypassing filters on certain URI schemes.

2. Writeup of the week

> "Reverse engineering games for fun and SSRF – part 1 & Part 2"

This is a great writeup if you want to learn how to hack thick applications. @tampe125 shows how he:

- Hacked an unnamed gaming thick application
- Set it up to go through Burp Proxy as a transparent proxy (by using his local /etc/hosts files)
- Extracted juicy information from the game's logs
- Reverse engineered a custom protocol using the logs
- Identified an endpoint vulnerable to SSRF
- Edited WebSocket connections to exploit the SSRF

It was only possible to configure Burp as a transparent proxy because the app didn't use certificate pinning.

3. Non technical item of the week

> "Are you submitting bugs for free when others are being paid? Welcome to BugBounties!"

If you're interested in bug bounty, this is an absolute must read! @zseano, a confirmed and experienced bug hunter, is denouncing some bad practices from bug bounty platforms. For example, some companies have a **paying private program and a public one with the same scope but no rewards** (kudos and Hall of Fame only).
He surprisingly concludes by saying that "bugbounties are overhyped and not sustainable" and that you should only do bug bounty as a hobby, not full time. He himself counts on quitting full-time bug hunting this year.
Whether he has an **ulterior motive** or not, one thing most people would agree on is: don't work for free, your time is too precious.

4. Tips of the week

> **"Tip 1: Find yourself using the same non-default wordlists over and over again in Intruder? Add them into the default list! Intruder menu > Configure predefined payload lists**
> **Tip 2: Sending lots of requests in Repeater and looking for specific text in the response? Use the find bar but also click the "+" and select "auto-scroll to match when text changes" to jump straight to what you want!**
> **Tip 3: Hold Ctrl and click a column heading to copy the contents of an entire column to the clipboard (don't be put off by the lack UI acknowledgement)"**

I love these Burp tips by @yppip. They might help you save time and avoid doing repetitive actions like loading your payload files manually every time.
And if you want to see more tips of this kind, @Agarri_FR has ~100 pages of them: **video** & **slides**. They date back a little but a lot of them are still valid.

5. Resource of the week

> **"Resources-for-Beginner-Bug-Bounty-Hunters"**

This one is for you if you dream of becoming a pro pentester or bug hunter and have absolutely no idea where to start. It's a short list of resources sorted by different categories: web, networking and programming basics, XSS and labs.
These are not exhaustive resources that will make you bug hunter of the year.
These are not exhaustive resources, rather basics to master and get a solid foundation as a start.

Other amazing things we stumbled upon this week

Videos

- Using Burp Suite – Video #1
- #1: The use of Public Data Breach Dumps in Cyber Defense
- WEBCAST: Sacred Cash Cow Tipping 2019, Slides & audio/podcast version

Podcasts

- Getting Into Infosec: Marcus Carey – Childhood Builder/Breaker to Navy Cryptologist to Founder and Mentor: Covers acing interviews, negotiating salary, gaining new skills, learning faster, hacking back, finishing degrees faster, and other life hacks. Recommended if you want to get into infosec.
- Absolute AppSec Ep. #43 – Keith Hoodlet
- TrustedSec Podcast Episode 3.7 – Intelligence and an End to USB Espionage?
- Black Duck Eggs: Darknet Diaries
- Hackable? Presents: Keyless Entry

Conference slides

- APKID: PEID for Android Apps
- Let's pwn a chinese Web browser!
- Automated Security Analysis AWS Clouds
- Black Hat Python workshop for Disobey 2019
- Threat modelling (from the perspective of a penetration tester)

Tutorials

Medium to advanced

- Angular and AngularJS for Pentesters – Part 1
- Backdooring Websites with just 35 byte
- Acquiring Data with CSS Selectors and Javascript on Time Based Attacks
- Dump iOS apps in Javascript (Part I)
- Attacking Kubernetes through Kubelet
- Kubernetes: unauth kublet API 10250 basic code exec
- Kubernetes: unauth kublet API 10250 token theft & kubectl
- Kubernetes: Kube-Hunter 10255

Beginners corner

- Pentesting Android applications by reversing and finding attack surfaces
- Active Directory Penetration Testing
- Day 19: Getting Started with Frida Tools

- Day 14: WebPwn (Automate Web Hacking)- Part 1

Writeups

Challenge writeups

- Intigriti CTF writeups: for the version with the ZIP password & for the version without the ZIP password
- Red-Team: Java Deserialization — From Discovery to Reverse Shell on Limited Environments

Pentest & Responsible disclosure writeups

- Hacking Fortnite Accounts
- Report: We Tested 5 Popular Web Hosting Companies & All Were Easily Hacked
- Out of Commission: How the Oklahoma Department of Securities Leaked Millions of Files
- Exposed JIRA server leaks NASA staff and project data!
- Hacking Jenkins Part 1 – Play with Dynamic Routing
- When Previewing Becomes Dangerous
- Reverse engineering McDonald's app
- Vulnerability Deep Dive: TP-Link TL-R600VPN remote code execution vulnerabilities

Bug bounty writeups

- AMPScript injection on Uber ($23,000)
- LFI via MySQL client on private program
- Blind XSS on private program
- LFI & IDOR on AntiHack.me
- IDOR on HackerOne
- Open redirect on SEMrush ($100)
- AWS S3 information disclosure on RATELIMITED

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Pktrecon & Explanation: Internal network segment reconnaissance using packets captured from broadcast and service discovery protocol traffic

- Recursive-gobuster: A wrapper around gobuster that automatically scans newly discovered directories

More tools, if you have time

- Uncaptcha2: Defeat ReCaptcha with 91% accuracy by asking for the audio challenge, downloading the mp3, forwarding it to Google Speech2Text API and submiting the answer back…
- Resolve_domain_computers.py: Get /etc/hosts entries for computers in Active Directory. Useful for internal pentests when for whatever reason you can't configure your box to use their DNS server directly. It uses domain creds to grab a list of hostnames from a DC, resolve their IP addresses, and gives you /etc/hosts entries.
- AEM hacker toolset: Tools to identify vulnerable Adobe Experience Manager (AEM) webapps
- s3-monster.py: Script to download fomes from open S3 buckets
- IdentYwaf: Blind WAF identification tool
- Giggity: Wraps github api for openly available information about an organization, user, or repo
- H8mail: Email OSINT and password breach hunting. Use h8mail to find passwords through different breach and reconnaissance services, or the infamous Breached Compilation torrent
- Cardfinder.py: Day 17: Looking for Credit Cards in Files
- ad-quick-install: Scripts to quickly setup AD and populate it with unique users (useful for building a lab

Misc. pentest & bug bounty resources

- Penetration Testing Pasties
- Pentesting Cheatsheets
- APIsecurity.io – Issue 14: Hacked hot tubs, airlines, trading sites; JSON encoding best practices
- Databases.today: Useful for recon, looking for leaked credentials or creating your owned haveibeenpwned database
- Mental Health Hackers
- Awesome-golang-security
- Day 18: Essential CTF Tools
- OSINT Framework
- Bash scripting cheatsheet

Challenges

- The Nixu Challenge: Online recruitment challenge

- DVFaaS – Damn Vulnerable Functions as a Service: Intentionally Vulnerable Serverless Functions to understand the specifics of Serverless Security Vulnerabilities

Articles

- The curious case of the Raspberry Pi in the network closet
- Super-systemic IoT flaws
- A small sex toy with big problems
- IoT: OFF by default
- What is IoT and How Do We Secure it?
- EternalSilence: Why your router may be at risk from this NSA tool

News

Bug bounty news

- Announcing Bug Bounty for Open Source Software: EU FOSSA 2 Intigriti bug bounty programs have started

Breaches & Vulnerabilities

- Android file manager app exposing user data through open port
- .gov security falters during U.S. shutdown: More than 80 TLS certificates used by .gov websites have expired without being renewed because of the ongoing U.S. federal shutdown. So dozens of government websites either became insecure or inaccessible (due to HSTS being used).
- Major Security Breach Discovered Affecting Nearly Half of All Airline Travelers Worldwide
- Hackers infect e-commerce sites by compromising their advertising partner
- Exclusive: Hackers Take Control Of Giant Construction Cranes
- Largest collection ever of breached data found (Collection #1)

Malicious apps/sites

- Pre-Installed Android App Impacts Millions with Slew of Malicious Activity
- GoDaddy is sneakily injecting JavaScript into your website and how to stop it

> If you happen to be a customer in US (which I am not but the website is hosted in a US data centre) then you are automatically opted into this service and all your website's pages will have this JavaScript injected into them.

Other

- 2019 will be our last year having a DerbyCon
- Women's Immersion Academy 2019: Here's a scholarship to get #cybersecurity training and certifications!
- Security concerns grow as Windows 7 support deadline approaches
- USB-C Authentication sounds great, so why are people worried?
- Firefox to disable Flash by default: Adobe Flash Player will be disabled by default in Firefox 69. Adobe itself is killing off Flash in 2020.
- Tesla's software bug bounty is going to the big leagues with Pwn2Own: Tesla is giving away a Model 3 for its bug bounty during Pwn2Own

Non technical

- On Bounties and Boffins & Twitter discussion vs Bug bounty programs: Everything you thought you knew is wrong
- Why I Think the NSA is Releasing a Free Reverse Engineering Tool This Year at RSA
- Capture That Flag!

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 01/11/2019 to 01/18/2019.

Subscribe to the newsletter

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.