Bug Bytes #7 – Abusing bounces, LazyRecon and LiveOverflow's definition of a vuln

BY INTIGRITI · FEBRUARY 26, 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 15 to 22 of February.

Our favorite 5 hacking items

1. Resource of the week

> "NetSPI SQL Injection Wiki"

This is a great wiki on SQL injection for both beginners and advanced testers.
I'm always talking abount maintaining a personal knowledge base. If you need inspiration, this is a perfect example of one which is very well organized and includes most things you need to learn or remember for testing SQL injections:

- Payloads for detection (by type of request)
- How to identify the Database Management System in use
- The different injection types and techniques including WAF evasion techniques
- Payloads for different attack queries (for information gathering, OS commands execution, privilege escalation, etc)

2. Writeup of the week

> "Abusing autoresponders and email bounces"

I think the best bugs are those found after researching a specific topic, finding a new type of bugs, then applying the finding to as many sites with a bug bounty program as possible.
This is a great strategy for finding a lot of valid bugs but it requires new thinking and discovering something that few people might have noticed. So it is nice to read about @securinti's thought process!
This article encompasses a lot of information like:

- How to find valid target email addresses without spamming them

- Examples of how to exploit them for many different attacks (blind XSS, arbitrary file upload, Ticket Trick, abusing printers…)
- How to abuse autoresponder and bounce emails to obtain sensitive information (like someone's real email address behind a generic one)
- Two examples of such bugs found on Google and Intigriti

Also, don't bother testing for the Intigriti bug on other bug bounty platforms, he already did.

3. Tool of the week

> **"LazyRecon by @CaptMeelo (not to be confused with @Nahamsec's LazyRecon script)"**

I love peeping into recon tools and seeing which tools, techniques or development practices they use that I don't.
LazyRecon is very similar to my own automated tool. It's written in Bash, is a wrapper around staple bug hunting tools (like Amass, Subfinder, Massdns, Masscan, Nmap, Aquatone, Dirsearch…) and is organized following a workflow including all the basic recon steps: subdomain enumeration, subdomain takeover, CORS configuration, IP discovery, port scanning, visual recon and content discovery.
I highly recommend reading through the tool's description (especially the "Notes" section) and the source code. It's good to use as is or as a basis for your own complete and customized recon tool.

4. Video of the week

> **"What is a Security Vulnerability?"**

@LiveOverflow is a genious! Seriously, reading the title of this video, I didn't understand what was there to discuss: a security vulnerability is any unexpected behaviour or flaw which can have a business impact, whether it is financial or brand image loss.
But this video is about 5 examples which makes you think:

- A CVE that isn't really a security vulnerability
- A security vulnerability in a smart contract, which isn't one according to the owner of the contract, but is a big issue for investors
- A no-vulnerability that some newbies mistake for one. But if the length of session cookies was shorter, it would actually become a vulnerability…
- Why there are proposals for removing XSS Auditor from browsers, and why an XSS should be reported even if it is stopped by it
- Whether to report a vulnerability that is not easily exploitable because of TLS

Sometimes, the line is blurry and it takes experience and intuition to decide whether a bug is a vulnerability or not. It makes sense.
I didn't realize this before hearing in it explained in these terms, but I use intuition too. Reading reports and experience that comes from discussions with clients and developers also help.

5. Tutorial of the week

> "AWS s3 Buckets Create"

This is a short to the point tutorial on how to create AWS s3 buckets. It's not groundbreaking but it's nice to have if you find a misconfigured subdomain pointing to an unclaimed bucket name.
Here's an example bug bounty writeup from the same author on exploiting such a misconfigured subdomain.

Other amazing things we stumbled upon this week

Videos

- Web Hacking Pro Tips #17 – @dawgyg Tommy DeVoss
- Extract endpoints with BurpBounty
- 10 Minute Tip: Finding Usernames Fast!
- 10 Minute Tip: Using EyeWitness to Surf Web Sites
- YAML: code execution using !!python/object
- OSINT : The Hack3rs Arsenal by Shreya Pohekar
- Path to OSCP Days 47 – 60 of 90

Podcasts

- Security Now 702 – Authenticity on the Internet
- Smashing Security 116: Stalking debtors, Facebook farce, and a cyber insurance snag
- Sophos Podcast Ep. 020 – Leaky containers, careless coders and risky USB cables
- Threatpost News Wrap Podcast For Feb. 22
- Hack Naked News #208 – Apple Sued, Lenovo X, & DNS
- Absolute AppSec Ep. #47 – Kevin Cody (on mobile app testing
- Darnet Diaries Ep. 32: The Carder
- Latest Hacking News Podcast #224 & #225

Conferences

- OWASP Meetup – SF February 2019
- Reviewing Modern JavaScript Applications & Slides

- Anatomy of Recent Security Breaches
- Abusing Insecure WCF Endpoints for PrivEsc and RCE
- Shitty First Draft – Lily Rogers

Slides only

- Bad API, hAPI Hackers!
- Host Header injection

Tutorials

Medium to advanced

- Undetectable Reverse shell with golang
- WPA-Enterprise: Learn how to steal WPA-Enterprise credentials. Most devices don't validate the authentication server certificate…
- Playing with Dirty Sock
- Multiple Vendor DNS Response Flooding Denial Of Service (CVE-2004–0789) | Clint Josy
- Reverse engineering of a mobile game, part 3: Now, it's obfuscated
- Azure AD Connect for Red Teamers
- "Relaying" Kerberos – Having fun with unconstrained delegation & Krbrelayx
- Day 50: Symbolic Link Attack, Overwrite Root Files with SUID/Root Invocation

Beginners corner

- Hacking 101: Basic network enumeration
- Wfuzz – Tips and Tricks for Bug Bounty
- Database Service Enumeration
- Pentest Lab Setup on Memcached & Penetration Testing on Memcached Server
- SQL Injection — Double Query Injection | Sudharshan Kumar
- Insecure Deserialization | Aditya Chaudhary
- Unvalidated Redirects and Forwards (Open Redirects) | Asfiya Shaikh
- Exploiting Put Method | Asfiya Shaikh
- Quick and Dirty BurpSuite Tutorial (2019 Update)

Writeups

Challenge writeups

- Analysis and Exploitation of Prototype Pollution attacks on NodeJs – Nullcon HackIM CTF web 500 writeup
- Hack The Box – Giddy

Pentest writeups

- Red Team Techniques: Gaining access on an external engagement through spear-phishing

Responsible disclosure writeups

- Hacking Jenkins Part 2 – Abusing Meta Programming for Unauthenticated RCE!, Exploitation tips, PoC 1 & PoC 2
- Exploiting Drupal8's REST RCE (SA-CORE-2019-003, CVE-2019-6340)
- Path Traversal & LFI leading to RCE on WordPress: uncovered for over 6 years!
- How I could have hacked lakhs of IRCTC accounts and get access to all your private info including easily cancelling booked tickets
- Medical Exploitation: You Are Now Diabetic
- Indane leaked Aadhaar numbers: 6,700,000 Aadhaar numbers
- CVE-2019-8389 – Arbitrary file read in Musicloud v1.6

Bug bounty writeups

- Information disclosure on Uber, Shopify & Netflix
- Logic flaw on PrivateInternetAccess VPN ($1000)
- Information disclosure on Uber ($5,000)
- DoS on Upwork ($400)
- SSRF in Slack ($1,000)
- DOM XSS on HackerOne ($500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Chomp Scan & Introduction
- Dirscraper: Tool to scrape directories from javascript files hosted on a website

- Get_schemas: Print out URL schemas from an Android app
- Simdjson: Parsing gigabytes of JSON per second & Pysimdjson: Python bindings for the simdjson project

More tools, if you have time

- Gorecon: All in one Reconnaissance Tool , a.k.a swiss knife for Reconnaissance , A tool that every pentester/bughunter might wanna consider into their arsenal
- Venom: A Multi-hop Proxy for Penetration Testers Written in Go
- RootHelper](https://github.com/NullArray/RootHelper): A Bash script that downloads and unzips scripts that will aid with privilege escalation on a Linux system. It automatically downloads and deploys enum & priv-esc tools
- Orc: Post-exploitation framework for Linux written in Bash
- Deckard: Performs static and dynamic analysis on APKs to extract Xposed hooks
- Jast: Just Another Screenshot Tool
- CVE-2019-5736-PoC: PoC for CVE-2019-5736, the recent runc (runtime for Docker and Kubernetes) container breakout bug

Misc. pentest & bug bounty resources

- Burp Suite Pro v2 FAQ
- JWT Handbook
- APIsecurity.io Issue 19: Half of Amazon's top-selling smart devices found vulnerable
- Markdown XSS Payloads
- Popular Tools for Brute-force Attacks [Updated for 2019]
- Can you hack your university?

Challenges

- Vulnado: Purposely vulnerable Java/Spring appo help lead secure coding workshops. Includes SQL injection, XSS, SSRF and RCE (plus reverse shell) all detailed for instruction in markdown so you don't even need a slide deck
- XSS challenge by @LooseSecurity
- RIPS Technologies new source code analysis challenge (spoilers in the Tweet's comments)
- Subdomain Takeover Lab: Website with more than 70 subdomains intentionally vulnerable to subdomain takeover (AWS/S3, Github Page, Heroku, Tumblr, Tilda...)

Articles

- Whitepaper: Security Cookies
- Why you should not use GraphQL schema generators
- Profiling a Website for Penetration Testing
- Tips on designing boot2root challenges
- Day 51: Understanding the OSI Model
- Exploring Commonly-Used Yet Vulnerable Components
- Day 49: Common C Code Vulnerabilities and Mitigations
- Can you really sniff out gas station card skimmers with your phone?
- Sinking a ship and hiding the evidence
- The Azure Security Model, Part 1 – Access Control Basics
- CSRF PoC for Jenkins Groovy console

News

Breaches & Vulnerabilities

- Password managers leaking data in memory, but you should still use one
- Healthcare hotline: Millions of medical advice calls exposed in Sweden: 2.7 million phone calls accessible without a password or any authentication
- Mega-crackers back with nearly 100 million new stolen data records
- Data Breach Bonanza: Dating Apps, Equifax, Mass Credential Dumps
- Drupal patches critical RCE bug in out-of-band update & Technical details

Other news

- New global standard aims to set a baseline for IoT security
- Virus attack! Hackers unleash social media worm after bug report ignored
- Will the EU's new copyright directive ruin the web?
- If you think your deleted Twitter DMs are sliding into the trash, you're wrong
- Design the next HackerOne T-Shirt
- Symantec's 2019 Internet Security Threat Report

- How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of: Story of Azimuth Security, an Australian startup dealing in exploit trade with democratic governments worldwide

- Edgescan's 2019 Vulnerability statistics report: Statistics on Web and network (infrastructure) security based on Edgescan data for 2018. E.g.: "The average time to fix a vulnerability discovered in the application layer is 77.5 days"

- You have around 20 minutes to contain a Russian APT attack: Crowdstrike report includes a ranking of threat groups based on their "breakout time" ("the window of time from when an adversary first compromises an endpoint machine, to when they begin moving laterally across your network"). The minimum is 20 minutes for russia!

Non technical

- [ITW] Daniel Kalinowski: "Participating in bug bounties improves your skills and increase the overall knowledge."

- Bounty Progress – January/February 2019

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 02/15/2019 to 02/22/2019.

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.