Bug Bytes #20 – Another LFI on Google, Turning your time into bugs by @Zseano & Live Hacking like a MVH by @fransrosen

BY INTIGRITI · MAY 28, 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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 17 to 24 of May.

Our favorite 5 hacking items

1. Article of the week

> "Turning your time into bugs — zseano's thoughts"

If you're into bug bounty, and want to get into the right mindset for success, then you need to read this and apply it.
The advice given is common sense, but sometimes what we need to hear is exactly that.
I love this piece, especially these two reminders: What you can try is limitless. And focus on specific goals to avoid burnout.

2. Writeup of the week

> "Another LFI on Google ($13,337)"

An LFI on a Google subdomain is an impressive finding. The most interesting parts of this writeup (the entire vulnerable paths) are sadly redacted, but here are 3 important lessons I got from it:

- Do file/directory bruteforce even on redirection pages
- Improving the wordlist & doing a second round can yield more new directories
- Persist if a bug is rejected. And follow your gut: if an endpoint looks interesting, keep digging

Also, it's good to know that @omespino used a combination of known wordlists (all.txt & SecLists) and custom ones (based on pattern matching and discovery).

3. Resource of the week

> "EdOverflow's newsletter"

A couple of weeks ago, when @EdOverflow announced he was starting a newsletter, I didn't know what it would be about. But I knew for sure that it would be good, as is everything shared by Ed.
Now after two issues, I urge you to subscribe if you haven't already. Each email is about a vulnerability class, with links to articles for digging deeper. This is a great opportunity to learn about lesser known

bugs and dedicate some quality time to research them.
I can't wait for more of these emails! Reading them is like the hacker version of reading a good magazine, sitting by the pool with mango juice and a good playlist. Fun times!

4. Tool of the week

> "TravisLeaks"

Remember this recent article by @EdOverflow on extracting sensitive information from Travis CI? It voluntarily didn't include the tools used to fetch build logs to avoid them causing any service disruptions. So if you've been wondering how to automate the techniques explained in the article, TravisLeaks will be very helpful. It has room for improvement but is a good start. Use it responsibly and customize it starting with the wordlist.

5. Slides of the week

> "Live Hacking like a MVH – A walkthrough on methodology and strategies to win big"

These are slides by @fransrosen on live hacking (i.e. bug bounty live events), touching on many different topics: technical advice, methodology, recon, the genesis of live events, reporting, what to focus on, examples of bugs...
To give you a taste, here's something to do when you're blocked while doing file/directory bruteforce: Use VPN with switchable IP.
Need I say more? Stop everything and go check it out!

6. Intigriti News

6.1 Write-up 5K XSS-Challenge

Did you win a Burp Pro License by solving our XSS Challenge? Read everything about the winner, our intended solution and the TWO (!) extra solutions found by our amazing community.

Read the solution here!

Other amazing things we stumbled upon this week

Videos

- Bug Bounty World Interviews Swaroop Yermalkar – Bug Bounty Talks
- Understanding Cross Site Request Forgery
- h1-65: First Live Hacking Event in Singapore with Dropbox
- May 2019 Pwn School – TinkerSec "Breach"
- Not Your Ordinary OSCP Review
- Zero to Hero: Episode 10 – MS17-010/EternalBlue, GPP/cPasswords, and Kerberoasting
- New Series: Getting Into Browser Exploitation – browser 0x00

Podcasts

- Smashing Security 129: Too Long; Didn't Listen
- Hackable? 25 – Phreaks and Geeks
- Risky Business #542 — Confusion reigns over Huawei ban
- Security Now 715 – CPU.fail
- 7MS #364: Tales of External Pentest Pwnage
- The Many Hats Club – Ep. 59, Veterans and hackers unite (with Cybermentor)
- Business Security Weekly #129 – Discovering Applications, Netsparker
- Secure Digital Life #111 – Mistakes In Your Career Search , RWU

Conferences

- NolaCon 2019, especially:
  - Let's Talk About WAF (Bypass) Baby
  - Baking Your Anomalous Cookies
  - Understanding XSS & Slides
  - One Random Insecure Wep Application Please (ORIWAP)
  - Automating Hashtopolis
- Security Fest 2019 Day 1 & Day 2, especially:
  - DOMXSS is not dead
  - Oh! Auth: Implementation pitfalls of OAuth 2.0 & the Auth Providers who have fell in it
  - Don't Sniff the MIME
- Votre vie privée contre des services ? (in French but here's how to get auto-generated English subtitles)
- Aggressive Autonomous Actions – Operating with Automation

Slides only

- Car infotainment hacking methodology and attack surface scenarios
- Hacking 101 – Hash cracking

Tutorials

Medium to advanced

- Self-hosted Burp collaborator for fun and profit

- New Generation Robots.txt: Apple App-Site-Association
- The signed JSON Web Token – A supposedly Secure Token and its Weak Spots
- Exploiting PHP Phar Deserialization Vulnerabilities – Part 1
- Azure Apps for Command and Control (or subdomain takeovers)
- 0x04 Calling iOS Native Functions from Python Using Frida and RPC

Beginners corner

- Back to Basics: DNS Enumeration
- Cybersecurity Fingerprinting Techniques and OS-Network Fingerprint Tools
- Hunting for Insecure Docker Registries
- Fantastic Vulnerabilities and Where To Find Them (Part 1)—Cross-site Scripting with Django form errors
- Types of SQL Injection (SQLi)
- A Kubernetes quick start for people who know just enough about Docker to get by
- Network Basics for Hackers: Domain Name Service (DNS) and BIND. Theory, Vulnerabilities and Implementation

Writeups

Responsible disclosure writeups

- Search Engine Abuse in Popular Social Networks
- The detailed analysis of WordPress 5.0 RCE
- Panic! at the Cisco :: Unauthenticated Remote Code Execution in Cisco Prime Infrastructure
- WD My Cloud RCE
- Pwning the Nokelock API
- Linux Privilege Escalation via LXD & Hijacked UNIX Socket Credentials
- Fun With Custom URI Schemes
- Slack Patches Download Hijack Vulnerability in Windows Desktop App

Bug bounty writeups

- Logic flaw on Facebook ($7,500)
- Authorization flaw on Shopify ($3,000)
- Race condition on HackerOne ($500)
- Logic flaw on HackerOne ($500)

- Authentication bypass on Revive Adserver #SourceCodeAnalysis
- LFI on Google ($3,134)
- XSS ($1,000)
- OpenID flaw
- Open redirect & Account takeover
- A different kind of CSRF on Slack

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Openinbrowser.py: Python script to open a list of URLs from a file in browser tabs, n tabs at a time
- Tt-ext – Taint Testing Tool: Chrome extension to aid in finding DOMXSS by simple taint analysis of string values
- To Fuzz a WebSocket: WebSocket Fuzzer in Python
- Pown-cdb: Automate common Chrome Debug Protocol tasks to help debug web applications from the command-line and actively monitor and intercept HTTP requests and responses. As @hakluke said, "like Burp proxy but CLI"

More tools, if you have time

- Subdomain Takeover.py & Usage: SubDomain TakeOver Scanner
- JS-Alpha: Funny project to create a converter that converts any javascript code to the code that contains only [a-z().] characters
- Vulnx: Cms And Vulnerabilites Detector And An Intelligent Auto Shell Injector
- Project Black: Pentest/BugBounty progress control with scanning modules
- XSSCon: XSS Scanner in Python
- Kaboom: Automatic pentest
- Censys.go & Usage example: Search censys from the CLI
- Trivy: A Simple and Comprehensive Vulnerability Scanner for Containers, Compatible with CI
- CVE-2019-0708 scanner & Metasploit module: Scanner PoC for CVE-2019-0708 RDP RCE vuln (BlueKeep)
- Pymetasploit3 & Tutorial: Metasploit automation library

Misc. pentest & bug bounty resources

- ZIP/RAR Wordlists
  - https://twitter.com/bit3c0de/status/1130728112147374080?s=20
- Aws-testing-notes: Notes as I learn basic AWS penetration testing
- Cracking resources for fun and profit
- Offensiveinterview: Interview questions to screen offensive (red team/pentest) candidates
- 60 Cybersecurity Interview Questions [2019 Update]
- What Every Security Leader Needs to Know Handbook
- Smart-Contract-Hacking

Challenges

- Intigriti XSS challenge 2: Challenge over but still available online if you want to play
- VulnCommerce
- Two Android challenges by @reyammer
- MySpace "Samy" Worm
- DVCW: Damn Vulnerable Crypto Wallet

Articles

- How I Eat For Free in NYC Using Python, Automation, Artificial Intelligence, and Instagram
- How to Upgrade Your XSS Bugs from Medium to Critical
- Permanent URL Hijack Through 301 HTTP Redirect Cache Poisoning
- Abusing jQuery for CSS powered timing attacks
- The Most Expensive Lesson Of My Life: Details of SIM port hack
- Analysis of a WordPress Remote Code Execution Attack
- No, 2FA Does Not Stop Credential Stuffing Attacks
- Failure Is Not the End – How to Provide Value to Your Customer Even When You Can't Own Their Network
- RDP Stands for "Really DO Patch!" – Understanding the Wormable RDP Vulnerability CVE-2019-0708

News

Bug bounty / Pentest news

- Bountybash: Live Hacking Hackathon on July 19-20,2019
- Kali Linux 2019.2 Release
- Register to Bugcrowd LevelUp 0x04: Free online conference on June 1-2

Reports

- Fortinet's Quarterly Threat Landscape Report
- Organizations dissatisfied with WAFs ineffective protection, time-consuming management, high cost
- GDPR report
- Hackers for hire – the good, the bad and the just-plain-scammers

Vulnerabilities

- Google Stored G Suite Passwords in Plaintext Since 2005
- Windows Zero-Day Drops on Twitter, Developer Promises 4 More

Breaches & Attacks

- Unistellar attackers already wiped over 12,000 MongoDB databases
- Millions of Instagram influencers had their private contact data scraped and exposed
- >20,000 Linksys routers leak historic record of every device ever connected

Malicious apps/sites

- A Huge Chinese Video App Is Charging People, Draining Their Batteries, And Exposing Data Without Their Knowledge
- Google uses Gmail to track a history of things you buy — and it's hard to delete

Other news

- Google launches Portals, a new web page navigation system for Chrome
- Nearly 20% of the 1000 Most Popular Docker Containers Have No Root Password
- Amnesty sues maker of Pegasus, the spyware let in by WhatsApp zero day
- Why You Should Never Use Airport USB Charging Stations
- Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers

- Faulty database script brings Salesforce to its knees: Faulty production script gave users access to all their company's Salesforce data.
- Equifax just became the first company to have its outlook downgraded for a cyber attack
- Huawei given stay of execution from US trade blacklist

Non technical

- Everything you wanted to know about the OSWE
- The Art of Threading – A Conversation with Tinker
- The Human Nature of Cybersecurity
- Grit is the Ultimate Privilege

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 05/17/2019 to 05/24/2019.

Subscribe to the newsletter here!

Disclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.Curated by Pentester Land & Sponsored by Intigriti