Bug Bytes #195 – LastPass discovery, learning to code, and a complete guide to SSRF

BY TRAVISINTIGRITI · MARCH 8, 2023 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The second series is curated by InsiderPhD. Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the weeks from February 27th to March 5th

CLICK HERE TO SUBSCRIBE

Intigriti News

- Our latest code review challenge and the Solution
- Another Cheat engine video this time on multi-level pointers
- And another web3 security video

From my notebook

1. LastPass says employee's home computer was hacked and corporate vault taken
2. Live Recon: Interviewing a Hacker – @rez0
3. Web Cache Poisoning" which I utilized to deface/disable the target web application in the realtime
4. A New Vector For "Dirty" Arbitrary File Write to RCE
5. Code Literacy is a super power for hackers

Other Amazing Things

- Malicious XLS Analysis // CVE-2017-11882 Still Lives!
- The ChatGPT Scam

- Carving Exfiltrated Network Data from a Hack (Python & Scapy)
- Scanning UDP with nmap
- 10 Tips for DEF CON newbies!
- Is This Website LEAKING?
- Announcing HTB Seasons | Open Beta – Hackers Wrath (Ippsec's Thoughts on the New Hack The Box Seasons)
- Hacking APIs: Fuzzing 101
- Using GitHub to Look at Source for a CVE [HackTheBox – Forgot]
- NetworkChuck recommends other creators

- 191 – Param Pollution in Golang, OpenEMR, and CRLF Injection
- 291-Mobile App Security & Audio Transcription
- 192 – A GPU Bug and the World's Worst Fuzzer Findings
- Risky Biz News: White House unveils National Cybersecurity Strategy
- Episode 365 – "I am not your supplier" with Thomas Depierre
- Headless Browser SSRF & RebindMultiA Tool Release + Web3 Bug

- So you wanna do some azure recon
- STÖK shares a memory of fellow hackers and also here
- Every bug bounty hunter eventually comes to this realisation that he cannot do bugbountiee for his whole life. It's stressful, unstable and can't be relied upon when it comes to raising a family.
- InsiderPhD: The technology crystal ball
- John CENA

- Spaceraccoon discovered a buffer overflow in linear memory in one of its dependencies (libheif) used to convert HEIC image files (CVE-2023-0996). An interesting exploration of ASM.js (predecessor of webassembly).
- I am sitting in my underwear in the sun next to a pool hacking a website show me a more based career path
- 1 Click ATO success

- Wi-Fi Marauder with ESP32 and Flipper Zero
- Exploiting SQL Injection in Graphql | DVGA |
- Cross-Origin Resource Sharing (CORS) Testing Guide
- PortSwigger Os Command Injection Labs
- Directory Traversal, File Include, File Upload—Web For Pentester 1
- Bypass SSL Pinning on Flutter iOS App Using Frida and OpenVPN
- Exploring Web3 Security: A Step-by-Step Guide to Creating Proof of Concepts for Previous Findings
- Intro to Cloud Security | Tryhackme Writeup/Walkthrough | By Md Amiruddin
- The Wild World of Website Tech: HTTP Requests, TCP Connections, and Bug Bounties—Oh My!
- Deserilaization Disaster in PHP
- Exploring iOS Applications with Frida and Objection: Basic Commands for Pentesting
- DVGA walkthrough
- A Complete Guide To Server-Side Request Forgery (SSRF)

- How I found a Account Takeover in a big Ecommerce Website.

- How to do proper recon and find bugs
- IDOR Vulnerability at /myaccount/myorders/getShipmentAndItemData lets attacker view other user's...
- What is the Open Redirect vulnerability, find it, and protect against it
- Command Injection by Changing the Logo
- 500$ Bounty in just 5 minutes through Recon!!!!
- Unauthorized Access To Admin Panel via Swagger
- My Report on How I avoid That XSS out of Scope when I discovered XSS and How can I convert it to...
- 30-Minute Heist: How I Bagged a $1500 Bounty in Just few Minutes!
- How I was able to access 2 million user's data in the web3 domain(Another critical bug in crypto
- My first IDOR on hackerone
- Finally, that's Blind XSS
- The Story of My First Reflected XSS
- Email Verification Bypass Worth $$$
- How I Earned $$$ for Excessive Data Exposure Through Directory Traversal Leads to Product Price
- My Journey Finding HTML Injection Vulnerability in a popular British Accountancy platform
- Found a Juicy XSS Bug on a Website ...
- How I Was able to find 2 Stored XSS via SVG file Upload
- How an IDOR Can Wreak Havoc: Breaking through the front door!
- Reflected Cross Site Scripting(Browserless.io)
- Web Cache Deception Attack on a private bug bounty program
- Attacker Can Takeover Any Account Because of Misconfiguration of Invite Members (Bug-Bounty)
- SSRF That Allowed Us to Access Whole Infra Web Services and Many More
- Authentication Bypass and SQL Injection
- HOW I HACKED DIFFERENT IIT's IN INDIA
- Blind Server Side Request Forgery
- How I Earned $1800 for finding a (Business Logic) Account Takeover Vulnerability?
- Open Redirect on my.yotpo.com

- Subdomain takeover on open.itu.edu via Shopify
- My First Un-Expected $$$$ Digit Bounty for an Un-Expected Vulnerability
- SSRF vulnerabilities caused by SNI proxy misconfigurations
- OpenEMR 5.0.1.3—(Authenticated) Arbitrary File Actions
- How I Found My FIRST SQL Injection CVE-2023–23331

- RedTeam-Physical-Tools – Red Team Toolkit – A Curated List Of Tools That Are Commonly Used In The Field For Physical Security, Red Teaming, And Tactical Covert Entry
- DataSurgeon – Quickly Extracts IP's, Email Addresses, Hashes, Files, Credit Cards, Social Secuirty Numbers And More From Text
- Updates to waymore urless GAP xnLinkfinder
- Advice on tools from Jason Haddix
- rebindMultiA
- Nuclei filtering templates
- DigitalOcean Droplet Proxy for Burp Suite

- ChatGPT helps bug hunter with ADHD
- Create Your Own XSS Lab with ChatGPT
- JWT strikes again
- Pre-login XSS?
- Fuzzing insights

- IDOR through XML
- SQLMap tip using –random-agent, -level and –technique flag
- I reported a Stored XSS that allowed me to takeover their session and all i got was 931, I also reported a Open Redirect but a Stored One and I got 150
- More Recon tips