Bug Bytes #207 - IIS, LLMs and iOS

BY TRAVISINTIGRITI · JULY 12, 2023 · LAST UPDATED ON JUNE 13, 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 week from July 3rd – July 9th

Intigriti News

- 4 reasons why you are not finding bugs
- What's the best security blog post you've read recently
- What was a unique high-severity vulnerability you found recently?
- Another week, another potentially dangerous JWT header

From my notebook

1. How to Write Great Bug Bounty Reports
2. 303-iOS Privacy & Security
3. Hunting for Bitwarden master passwords stored in memory | Red Maple Technologies
4. Beyond Microsoft IIS Short File Name Disclosure
5. OWASP Top 10 for Large Language Model Applications

- Free VPN Is Really DDoS Botnet in Disguise
- TryHackMe! Finding Computer Artifacts with osquery
- LiveOverflowGeneric HTML Sanitizer Bypass Investigation
- How Hackers Write Malware & Evade Antivirus (Nim)

- Top resources I used to learn Penetration Testing
- Demystifying Cybersecurity CTF's – LIVE "You Hack Too" Tutorial
- Day 7 – Internet Protocol Version 7
- How to Trick Hackers & Web Crawlers with Spidertrap
- Proving Grounds – MoneyBox (Easy) – Live Walkthrough
- Hands-on guide to CORS
- Day 8 – Two-Factor Authentication
- HackTheBox – Inject
- Hacker Interview: Ryan Montgomery AKA 0day
- Portswigger Web Academy – OS Command Injection – Lab Walkthroughs

- Episode 382 – Red Hat, you were the chosen one!
- EP128 Building Enterprise Threat Intelligence: The Who, What, Where, and Why
- 135: The D.R. Incident
- The Art of Red Teaming with Shani Peled
- Risky Biz News: $922 million worth of crypto stolen in H1 2023
- Indicators to insider threats.
- Episode 26: Client-side Quirks & Browser Hacks
- Danny 'Rand0h' Akacki discusses his love for streaming and community
- Ankita Dhakar: Revolutionizing Bug Bounty Platforms with AI Integration
- Episode 383 – Is open source dying?
- Risky Biz News: Mastodon plugs a horror-show bug

- I'm excited to announce the release of my IIS short filename discovery tool, shortscan. It only took 4 years, but better late than never right? Have fun!
- so clean, so smooth, no weird UI issues, easy to navigate and best of all, it just simply works out of the box and does exactly what you need it to do
- Join me on YouTube for an incredible Bug Bounty recon adventure
- The hardest part of being self employed for me is taking time off. Not that I always work, but having some days/weeks off without feeling guilty are rare.
- Threader accounts to follow!

- Beginner
  - Bypassing Door Password
  - What is IDOR and Why Should You Care About It?
  - My Top fav Google Dorks for web security testing
  - Learning SQLi
  - Chat GPT For Bug Bounty: Recon, Generate wordlist, Nuclei Template, Convert p3 or p4 in P2 or P1
  - How to Write A Bug Bounty Report Like a Pro!
  - HTB Network Enumeration with Nmap Walkthrough
  - Privileges Escalation Techniques (Basic to Advanced) in Linux
  - Getting Started with Azure DevOps CI/CD for Microsoft Sentinel
  - The Ultimate Guide to HACK S3 Buckets: Data Leaks and Discovery Techniques
- Intermediate
  - Sql injection using Parameters (P-DB-b-1)
  - How to find open ElasticSearch databases using Shodan
  - How to Install OpenVAS

- An In-Depth Look at PEN-300 and OSEP: Succeeding in the Offensive Security Path
- Art of hacking LLM apps
- IDN Homograph Attack and Response Manipulation – The Rarest Case
- Web3 Security Roadmap, How to become a Smart contract auditor
- Bug Bounty Hunter—Let's look at the CSTI attack method from every angle
- Mastering Google Dorking: Expanding Scope, Reconnaissance, and Resources – RiSec
- Evading Web Application Firewalls (WAFs)
- WebSocket protocol
- Testing for SSRF Vulnerabilities

- Advanced
  - Extending Burp Suite for fun and profit – The Montoya way – Part 1 – hn security
  - What is Force sending ether in smart contracts security?!
  - Game Hacking 101: Unleashing the Power of Memory Manipulation
  - Cracking PicoCTF Challenge: GDB Baby Step 1—StackZero
  - Unravelling PicoCTF: The GDB Baby Step 2 Challenge
  - GDB Baby Step 3: Unraveling Debugging Secrets—StackZero
  - Demystifying PyInstaller—A Journey into Decompiling Python Executables
  - Unveiling the Power of Binary Exploitation: Mastering Stack-Based Overflow Techniques
  - Code for reading Windows serialized certificates
  - Backdooring ClickOnce .NET for Initial Access: A Practical Example

- Security Research
  - How I Hacked CASIO F-91W digital watch
  - Technical Details of CVE-2023-30990 – Unauthenticated RCE in IBM i DDM Service
  - Desuperpacking Meta Superpacked APKs
  - Vulnerability Detection Using Attack Surface Management: Criminal IP ASM Use Case (1)
  - ServiceNow Insecure Access Control To Full Admin Takeover
  - Hunting for Nginx Alias Traversals in the wild

    - How to exploit an API using prototype pollution
    - Clop Ransomware and MoveIT CVE: Ransomware: History, Timeline, And Adversary Simulation – FourCore
    - Actively Exploited Industrial Control Systems Hardware – SolarView Series – Blog – VulnCheck
    - StackRot (CVE-2023-3269): Linux kernel privilege escalation vulnerability
    - Cloud Defense in Depth: Lessons from the Kinsing Malware – Sysdig
    - Hijacking S3 Buckets: New Attack Technique
    - Laurence Tratt: Two Stories for "What is CHERI?"
    - Flutter Restrictions Bypass
    - Windows Installer arbitrary content manipulation Elevation of Privilege (CVE-2020-0911)
    - The five-day job: A BlackByte ransomware intrusion case study | Microsoft Security Blog
    - Introducing Slinky Cat – Living off the AD Land
    - [REL] A Journey Into Hacking Google Search Appliance
    - The JSON Data Downfall: Discussing the overlooked aspects of JSON Data Amplification Attacks
    - CVE-2022–1388 BIG-IP RCE Hunt
- Bugs
    - How I hacked CTX and PHPass Modules
    - Hacking Chat GPT and infecting a conversation history
    - Tales of XSS: Navigating Web Vulnerabilities
    - Account takeover through changing id in reset password
    - How I got Two RCE at EPAM-Bounty Program
    - Account takeover in Indian Govt.Education site
    - Stored-XSS led to Keylogger injection
    - How I broke into Kiosk machine to get admin access
    - IDOR To Delete Hall Of Fame Page.
    - A trivial OTP Bypass Based On Business Logic Abuse
    - Finding Critical bugs in Android application—(Part 1)
    - Unveiling a Unique Bug: The Quest for Website Vulnerabilities
    - How To Apply For The Medium.com Bug Bounty Program—You Might Win Even 1,000 Dollars Or More Even
    - Easy Stored XSS give me $$$
    - How I Found a Subdomain Takeover | Bug bounty
    - Story Of My First RCE
    - How BAC(Broken Access Control) got me a Pre Account Takeover

    - Account Takeover (ATO) via Manipulation of the Change Password Funcionality
    - How i got my First CVE (CVE-2022–48150) on Self XSS to Reflected XSS
    - How I found my first P1 vulnerability by bypassing Adobe dispatcher
    - Unveiling a Bug: Paying $1 and Receiving $100 (or Any Amount) in Return
    - Using Github for easy Zero Days
    - Found +15 XSS Via Citrix gateway latest CVE , Dup's of (CVE-2023–24488)
    - Automating XSS
    - Exploring the Sneaky World of Race Condition Vulnerabilities
    - Account takeover hidden in Javascript files.
    - Exploiting Non-Cloud SSRF for More Fun & Profit
    - Exploring Eclipse IDE Attack Vectors: Unveiling Google Cloud Tools Plugin Vulnerabilities
    - How to Steal Social Media Accounts Using a Captive Portal
    - Beware of fake npm packages
    - Taking Entire server control Part 2 of How I Earned $2500 in 5 Minutes
- CTF challenges
    - Pollute only after Cleaning! (0623 Intigriti Challenge)
    - Gallery—TryHackMe's Challenge Room Simple WriteUp
    - HTB: Inject
    - Exploiting SMB using CVE2017–0144/MS17–010 (Manually & Automated Method)
    - Exploiting Active Directory—(TryHackMe) THM Attacktive Directory Lab
    - VulnHub – Kioptrix: Level 3 (1.2) (#3)

- GitHub – Anof-cyber/Pentest-Mapper: A Burp Suite Extension for Application Penetration Testing to map flows and vulnerabilities
- GitHub – introvertmac/EasyScan: Light-weight web security scanner
- Evilgophish Evilginx 3.0.0 Update
- GitHub – AbstractClass/CloudPrivs: Determine privileges from cloud credentials via brute-force testing.

- Amazing Burp extension: Header Issue Reporter
- NucleiFuzzer = Nuclei + Paramspider
- Introducing httpXplorer: Simplifying httpX URL Management and Analysis
- JS-Scan A .js scanner, built in PHP, designed to scrape urls and other info.
- Certificate Search – Get informations about SSL certificates
- CloudJack – Route53/CloudFront Vulnerability assessment utility.
- Hey Bug Bounty folks, I am working on a rather simple dashboard for domain/subdomain storage. I called the project “vīlicus” and you can find it here

- SQL injection in one of the biggest shopping website in the world
- When hunting for (DOM-)XSS vulnerabilities, I usually keep a close eye on the JS console to spot any new messages & errors being logged when fiddling around with params.
- 5 tips for writing bug bounty report
- Top bb hunters stay at top because they never share their methodology, and if they do, it is always for a few people, never publicly
- 10 tips for crushing bug bounties
- Don’t remember that one command you ran a long time ago?
- Always check the URL,s from waybackurls, katana
- How did I test the IDOR vulnerability that leads to all user Data leakage?
- Display the server of each subdomain in a list with the httpx -server option