Bug Bytes #211 – Hacking Casinos, Microsoft's Key Mishap, Read the Docs and ImageMagick Strikes Again

BY TRAVISINTIGRITI · SEPTEMBER 13, 2023 · LAST UPDATED ON APRIL 4, 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 September 5th to September 10th

Intigriti News

- We've got 2 spare tickets for @nullcon Goa 2023, courtesy of @redbull
- Our dev friend found one of his first coding projects on an old backup drive that he made back in 2007 for his first school project
- Top 4 tools to automate SQL Injection vulnerabilities!
- Let's see how we can solve the first JWT "expert" lab, focusing on algorithm confusion
- Some great insights from @VoysNL on why you might want to launch a bug bounty program, and how to make it a success!
- @odanorge has just launched their public bug bounty program with @intigriti, paying up to €4,000 for valid vulnerabilities!

From my notebook

1. Bug Bounty Stories (EP1): Hacking An Online Casino – Slightly different format of video, but a really interesting look into NahamSec's process
2. Results of Major Technical Investigations for Storm-0558 Key Acquisition – Oops from Microsoft
3. API Security Testing using AI in Postman – Really good guide on using Postman for API hacking, instead of or with Burp
4. Tricky Unauthenticated RCE on WordPress Media Library Assistant Plugin using a good old Imagick – Oh ImageMagick my old friend what you have you done this time
5. Episode 35: King of Collaboration: Douglas Day – ArchAngelDDay talks about how he finds bugs, his approach and auth testing

Videos 

- Learn Active Directory Kerberoasting
- How The Pirate Bay Became a Religion, Political Party, and (Almost) a Country Darknet Diaries Ep.92

Podcasts

- Risky Biz News: Microsoft explains how it lost its signing key
- UL NO. 397: Propaganda in a Box, Glacier-like Security, AGI by 2028?, Ancient Wisdom via AI, and Newsletter Differentiation
- Powerlifting and PowerShell: A Discussion with Jake Hildreth
- Risky Business #720 — How cloud identity provider federation features can get you mega-owned
- Deciphering Privacy in the Age of AI: An Expert Discussion
- SN 938: Apple Says No – Topics coming to Android, Apple security research, browser extension vulnerabilities
- Yuri Diogenes Discusses Building a Career in Cybersecurity
- EP137 Next 2023 Special: Conference Recap – AI, Cloud, Security, Magical Hallway Conversations
- 137: Predator

Tutorials

- Beginner
  - Unveiling the Web's Vulnerability: An Introduction to Cross-Site Scripting (XSS)

    - Unleashing Precision: Burp Suite's Intruder Tool in the World of Ethical Hacking
    - BurpSuite 101
    - How DNS Works—DNS Zone Transfer
    - 4-way handshake in wireless communication
- Intermediate
    - The Hidden SQL Injection Techniques That Google Doesn't Want You To Know
    - CVE-2023-38831 – WinRAR Zero-Day Vulnerability manually Exploit
    - A Comprehensive approach for testing for SQL Injection Vulnerabilities
    - Understanding SSTI and Building Payloads in Jinja2 Introduction
    - For Newbies: Simple Examples of LDAP Injection Vulnerabilities
    - Hacking a Windows Machine by Hiding a RAT Inside the File
    - Exploiting CORS misconfigurations
    - SAST & DevSecOps for Java
- Advanced
    - How to deploy & debug smart contracts with Foundry (Part 2)
    - Diagramming Smart Contract for Security Auditing | Sm4rty
    - Securing Microservices: Application Architecture for Distributed Systems
    - Recovering access to an AWS EC2 instance using SSM

- Security Research
    - bcrypt at 25: A retrospective on password security
    - Spoof iOS devices with Bluetooth pairing messages using Android
    - Orbeon Forms: The Final Form? On A Journey To RCE
    - BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild
    - Nagios Plugins: Hacking Monitored Servers with check_by_ssh and Argument Injection: CVE-2023-37154
    - Paranoids Vulnerability Research: Ivanti Issues Security Alert

    - Boot Unguarded: x86 Trust Anchor Downfalls to The Leaked OEM Internal Tools and Signing Keys
    - A tale about a Red Team exercise and the Forcepoint Endpoint One DLP client
    - Apache Superset Part II: RCE, Credential Harvesting and More
    - Main Analytical Frameworks for Cyber Threat Intelligence
    - eBPF Offensive Capabilities – Get Ready for Next-gen Malware – Sysdig
    - Android 14 blocks all modification of system certificates, even as root
    - Analyzing a Facebook Profile Stealer Written in Node js
    - When URL parsers disagree (CVE-2023-38633)
    - Uncovering Web Cache Deception: A Missed Vulnerability in the Most Unexpected Places
- Bugs
    - A casual hunt of the day : Open Redirect at one of the largest MNCs
    - Login Page Bypass With Google Hacking Database
    - Bypassed Input Escaping for XSS
    - How I placed into Apple Hall of Fame in 5 Minutes.
    - Finding Loose Comparison in the wild (Unga Bunga Bugs Part-1)
    - How I Find API disclosure $$$
    - Subdomain takeover via Frill.co
    - Information Disclosure exposes The Correct Answers through Debug in Quiz Scoring
    - Bug Bounty Chronicles: an SQL death spiral
    - Single XSS with Earn $600
    - Leaked Database and SMTP credentials through .env file
    - Wifi Soft Unibox Administration 3.0 Login Page Exploit
    - Unveiling RCE on Dutch Government Website
    - Bypass Mobile Phone verification using Mobile website
    - How I was able to find an information disclosure on the Google Tag manager
    - How I got $$$ from my First valid Bug
    - How I was able to find PHP info page on the website
    - My debut with a Critical Bug: How I found my first bug (API misconfiguration)
    - The Art of Brute force with Facebook (Oculus) White-Hat Security Team
    - Chaining low impact bugs leads to 0 click Mass ATO
    - Again? Subdomain takeover via ideanote.io
    - Story of Stored Blind XSS
    - Revealing a Security Flaw: How I Discovered a Data Leak.

    - Privilege Escalation to Super Admin
    - How I ethically hacked one of the domains of the United Kingdom
- CTF challenges
    - HTB: PikaTwoo
    - WordPress Infiltration Pen Test Lab (VM Included)
    - Lesson Learned writup || TryHackMe
    - Grep writeup | TryHackme
    - Blaster writup ~ TryHackMe

- Hakluke's Tool Stack
- DorXNG – Next Generation DorX. Built By Dorks, For Dorks
- Quick-Lookup-Ptrun – Quick Lookup Plugin For PowerToys Run (Wox)
- EmploLeaks – Finding Leaked Employees Info for the Win
- HTTP-Shell – MultiPlatform HTTP Reverse Shell
- securisec/chepy: Chepy is a python lib/cli equivalent of the awesome CyberChef tool.
- The Power of AXIOM Part 1
- Exploring Narrowlink: Your Swiss Army Knife for Secure Networking
- Enhancing Bug Bounty Workflow with Advanced Google Dorks
- Introduction to OpenVAS—A Vulnerability Scanner
- Tired of using many #Recon tools? I wrote a tool in rust that will help you do fuzzing, reverse dns lookup

- All my current bug bounty knowledge is gone. Here's how I get it back and make $100k in the first year:
- Hunting #opendir with sql files on FOFA Search Engine @fofabot
- Account Takeover Through Host Header Injection
- Admin Panel Takeover
- IDOR leads to Mass Account Takeover of Employees
- Account Takeover tip using password resets
- How to spot the CVE vulnerability in Ivanti MobileIron Sentry (CVE-2023-38035) that affects the MICS Admin Portal.