Bug Bytes #205 – Live Hacking, AI Hacking and Helicopter Hacking

BY TRAVISINTIGRITI · JUNE 28, 2023 · LAST UPDATED ON MARCH 27, 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 June 19th to June 25th

Click here to subscribe

Intigriti News

- June's challenge is over, here are the results! And the video explanation
- We had a blast in Varna for 1337UP0623 with €260k on the leaderboard! Congrats to all the award winners!
- Android hacking continues!

From my notebook

Lots of fun stuff in this weeks issue, with a bunch of specialist hacking resources, including stealing a helicopter??? But also Intel has applications open for it's Live Hacking Event for sponsored and non-sponsored hacking, so if you want to give live hacking a shot this is a great opportunity. Also Twitter broke something this week so limited tweets but hopefully there's enough other stuff to make up for it!

1. Episode 24: AI + Hacking with Daniel Miessler and Rez0 – Daniel and Rez are some of the biggest ambassadors for AI in red teaming/security/bug bounty, so it's always interesting to hear them talk about their passion!
2. How to Hack WordPress – WordPress is everywhere, this is a good summary of what to do when you see a WordPress website!
3. OAuth vs SAML – These shorts from Bug Bounty Reports Explained are a great way to get nuggets of hacking info, without committing to a longer video
4. GTA V in real life? Stealing a helicopter as part of a physical security test – Freakyclown talks through his career and it's kinda wild to be honest
5. Intel opens applications for fully-sponsored and self-sponsored invitations in this October LHE (closes on July 8th), more info – This LHE is open to all hackers, and there's plenty of time to sort out things like visas so it should be really accessible for folks who've never done a LHE!

Videos 

- Finding Exploits!
- Hacking with Google Dorking!
- picoCTF – Java Code Analysis!?! – Live Walkthrough
- Inside a Cybercrime Scam Operation
- Men's Mental Health Awareness
- Authentication bypass by copying a cookie from another app
- Hack All The Things: A Fireside Chat with NahamSec
- 15-Minute Security Flash | MOVEit Vulnerability
- Fake OnlyFans MALWARE: Remcos Infostealer VBScript Stager
- Hacking Google Cloud?
- Hacker101 CTF – Micro-CMS v1 (Easy) – Live Walkthrough
- Critical authentication mistake made by big companies
- A common password reset vulnerability
- Burp Suite || Penetration Testing Boot camp
- Hacker101 CTF – Micro-CMS v2 (Medium) – Live Walkthrough
- BreachForums Hacked Just Days After Launch
- Introduction [Revival of Code 2023 – Advent of Code 2016]
- Advantages of Modern Bug Bounty

Podcasts 

- 301-Self-Hosted 3: Calendars, Contacts, & Notes

- Talking Content Creation and Marketing with Zach Hill
- SN 928: The Massive MOVEit Maelstrom – Patch Tuesday, SpinRite 7.1, MOVEit
- NO. 387 — Modern Parenting and Narcissism?, New Russian Hacking Unit, McKinsey AI Predictions, and more...
- A Conversation with Red Team Expert Manit Sahib
- EP126 What is Policy as Code and How Can It Help You Secure Your Cloud Environment?

- Beginner
  - Recon like a Pro!
  - Testing and Bypassing Technique for IDOR
  - Welcome to the Bug Bounty Beginner's Roadmap: Your Ultimate Guide to Success!
  - Mitigate bot attacks by Rate limiting
  - Exploring WordPress Juicy Endpoints: A Guide for Bug Bounty Hunters
- Intermediate
  - Exploiting Exposed Tokens and API Keys: Edition 2023
  - How to find SQL Injection using a simple technique
  - How to Perform an Evil Twin Attack & Steal Wi-Fi Passwords
  - Bug Bounty Recon: Content Discovery (Efficiency pays $)
  - Hacking CSRF: Referer-Based CSRF Defense
  - Understanding Prototype Pollution and its Exploitation—Part 2
  - Genymotion—Proxying Android App Traffic Through Burp Suite in Windows
  - Securing Your Infra: Exploring Nuclei's Defense Arsenal
  - Exploiting XSS Through File Uploads: Unveiling Vulnerabilities Step by Step
- Advanced
  - CVE 2022–33082 Practical Exploitation
  - Exam Preparation Blog: Mastering EWPTX
  - Privileges Escalation Techniques (Basic to Advanced) in Linux
  - Enhancing WordPress Website Security: Automate Wpscan and Receive Instant Alerts
  - Recreating Cordova Mobile Apps to Bypass Security Implementations

- Attacking AWS | Common Cognito Misconfigurations

- Security Research
  - A brief summary about a SSTI to RCE in Bagisto
  - AWS WAF Clients Left Vulnerable to SQL Injection Due to Unorthodox MSSQL Design Choice – GoSecure
  - LibreOffice Arbitrary File Write (CVE-2023-1883)
  - OPC UA Deep Dive Series (Part 4): Targeting Core OPC UA Components
  - nOAuth: How Microsoft OAuth Misconfiguration Can Lead to Full Account Takeover
  - Leaking secrets through caching with Bunny CDN
  - chonked pt.2: exploiting cve-2023-33476 for remote code execution
  - FortiNAC – Just a few more RCEs
  - How we tried to book a train ticket and ended up with a databreach with 245,000 records
  - The Phantom Menace: Exposing hidden risks through ACLs in Active Directory (Part 1)
  - A “cewl” way for API discovery
  - Exploring Kubernetes runtime security with Falco and Datadog
  - “Registry Run Keys: The Secret Sauce of Persistent Malware!”
  - KeePassXC Vulnerability CVE-2023–35866
- Bugs
  - idor on samyad.tvu.ac.ir
  - How did I hacked the Dutch government and made it into the Hall of Fame?
  - How To Abuse A Password Manager
  - Introspection Query leaks Graphql schema
  - One mistake, Three bugs: Comprehensive android pentesting.
  - SQL Injection UNION Based Unknown Table X Multi-line Query Issue
  - Unveiling a Bug: Paying $1 and Receiving $100 (or Any Amount) in Return
  - How I found a SQL Injection bug in using my cellphone
  - Uncovering SSRF attack

    - The Unexpected “0” Master ID for Account Data Manipulation
    - Hacking CSRF: Bypass Same Site Cookie Restriction Part 1
    - The tiny miny XSS | A Hacker Story
    - How I Hacked 500+ Univeristies , Foundations, and 2 ‘million + users Acount By Gajendra Singh
    - How I hacked NASA and get 8 bugs ?
    - Unleashing the Power of Recon: How I Earned $2500 in 5 Minutes | CVE-2017–5638 | OGNL injection
    - SQL Injection in The HTTP Custom Header
    - Simple CORS misconfig leads to disclose the sensitive token worth of $$$
    - [Bugcrowd’s]P1 Using Default Credentials
    - How I chained Host header Injection to Password Reset Link Poisoning to XSS and Account Takeover.
    - Exploiting SQL Error SQLSTATE[42000] To Own MariaDB of A Large EU based Online Media
    - How I Hacked my college cloud Servers and Find DOS + ATO + Google Authentication + Priv Esc ??
    - How I was able to Buy Tickets for 1 Rupee!—Payment Price Tampering
    - How I Unveiled a Critical Vulnerability: Exposing All Buyers’ Invoices PII with a Single Trick
- CTF challenges
    - HTB: Stocker
    - Cracking PicoCTF: ‘Hurry Up! Wait!’ With Ghidra
    - NahamCon CTF 2023—OSINT Challenges Walkthrough
    - VulnHub—Kioptrix Level 1 (#1)
    - CORS vulnerability with basic origin reflection
    - Hack The Box: Angler (Mobile Challenge) Walkthrough
    - TryHackMe – SmagGrotto

- Callisto – Automated Binary Vulnerability Discovery Tool
- #OpenSourceDiscovery | Pradeep Sharma | Substack

- 50+ Tools with Bash Script = Bounties $$$ Money: Unleash the Power of magicRecon
- Discovering Login Panels and Detecting SQL Injection with Logsensor
- DarkBERT: A Language Model for the Dark Side of the Internet
- Forensia – Anti Forensics Tool For Red Teamers, Used For Erasing Footprints In The Post Exploitation Phase
- Scanner-and-Patcher – A Web Vulnerability Scanner And Patcher
- EndExt – Go Tool For Extracting All The Possible Endpoints From The JS Files
- csp-analyzer – Analyze Content-Security-Policy header of a given URL.
- JWT cracker – JWT brute force cracker written in C
- Cross-site scripting cheat sheet
- TomNomNom releases jsluice – extracts URLs, paths, secrets, and other interesting data from JavaScript source code

- All the updates from AWS re:inforce, Google Cloud Security Summit + fwd:Cloudsec
- GitHub Dataset Research Reveals Millions Potentially Vulnerable to RepoJacking
- New Zealand became the latest nation to start mandating VDPs for government agencies