Bug Bytes #213 – Hacking a Prison, XSS on steroids, CAIDO free for students and Bogus CVEs

BY TRAVISINTIGRITI · OCTOBER 4, 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 25th to October 1st

Intigriti News

- Yahoo picks Intigriti to run crowdsourced bug bounty programme
- We're joining forces with TCM Security to educate the next generation of bug bounty talent
- Here are top 3 most popular tools for RCE vulnerabilities
- JWT algorithm confusion? What can we do when the server doesn't expose a public key

From my notebook

1. Bug Bounty Stories (EP2): Hacking a Prison – NahamSec shows us why reading the javascript is important
2. Bounty of an Insecure WebView (Part 1): XSS, but with Steroids – A fun XSS in a mobile apps WebView causes an interesting XSS vector
3. CAIDO launches a student plan! – If you're a student you can get CAIDO for free, simply email them proof of student status
4. The bogus CVE problem [LWN.net] – While the CVE system is crucial for tracking vulnerabilities, not every entry is submitted in good faith
5. Input Validation: Necessary but Not Sufficient; It Doesn't Target the Fundamental Issue – Input validation is an important method for stopping some vulnerabilities, but that doesn't mean it's akkways the right choice!

- How to become a CISO?
- Authentication Vulnerabilities – Lab #11 Password reset poisoning via middleware | Long Version
- Being careful with brute-forcing identifiers #bugbounty #bugbountytips #bugbountyhunter
- Learn to Code with AI
- $28K Apple Shortcuts IDOR
- The Truth Behind The SONY Hack
- ThemeBleed Exploit Analysis (CVE-2023-38146)
- The Penetration Test That Went Horribly Wrong Darknet Diaries Ep. 95: Jon & Brian's Big Adventure
- You don't always have to predict the identifier #bugbounty #bugbountytips #bugbountyhunter
- How AI and ML is changing cybersecurity?
- MGM and Caesars Hacked! Crypto Scam costs Mark Cuban Big Time, & more!
- Top hunters think about everything when submitting a report #bugbounty #bugbountytips
- Hackumentary Ep 1: Jonathan James – The boy who hacked Nasa
- Unveiling Vulnerabilities: Exploring Tech and Human Weaknesses within Organizations
- Charting Your Path in Cybersecurity: Navigating Certifications, Degrees, and Education
- Find and Exploit Server-Side Template Injection (SSTI)
- Do not forget about this attack scenario #bugbounty #bugbountytips #bugbountyhunter
- Start doing cloud pentesting in GCP?

- Mobile Hacking Maestro Sergey Toshin (Ep. 38)
- Jakoby's Journey
- Risky Biz News: More in-the-wild 0day for Firefox, Chrome
- Stealing your car's identity.
- 215 – DEF CON, HardwearIO, Broken Caching, and Dropping Headers

- EP140 System Hardening at Google Scale: New Challenges, New Solutions

- Beginner
  - Ways I followed to Bypass '403'—Your checklist
  - How to Discover API Subdomains? | API Hacking |
  - How to Setup crAPI in ubuntu server and make it network accessible
  - Input Sanitization Techniques for Secure Coding
  - Burpsuite vs Caido: Why You Should give Caido a try
  - IDOR. Autorize. Broken Access Control.
  - HTTP Security Headers
  - Race condition 101-Everything you need to know about race condition attacks
- Intermediate
  - Mass hunting for misconfigured S3 buckets
  - The Art of Monitoring Bug Bounty Programs
  - How To Hack 2FA/MFA—An Important Cybersecurity Topic
  - Hacking htmx applications
  - XML External Entity (XXE) Injection in Web App Penetration Testing | 2023
  - Path Traversal Vulnerabilities: A Beginner's Guide
  - Free awesome VPS for bug hunting process
  - AWS Cloud Security Checklist (Cloud Security)
- Advanced
  - DevSecOps—Docker Security (with Syft and Grype)
  - NucleiFuzzer: Automating XSS Detection for Unrivaled Security
  - Creating custom AXIOM modules
  - NoSQL injection

- Security Research
  - Screen Leakage
  - The development of multi ransomware killswitch!
  - Liferay Portal RCE | CVE-2020–7961
  - Chrome's Vulnerability: When a Single Click Exposes Your Deepest Secrets (CVE-2020–6547)
  - Details QA should share when reporting a bug for efficient resolution
  - Get persistent reverse shell from Android app without visible permissions to make device unusable
  - Getting RCE in Chrome with incorrect side effect in the JIT compiler
  - Survive Access Key Deletion with sts:GetFederationToken
  - Malicious npm Packages Strike Again: Exfiltrating Kubernetes Configurations and SSH Keys
  - Finding Hidden API Endpoints Using Path Prediction
  - Exploiting ASP.NET TemplateParser – Part I: Sitecore (CVE-2023-35813)
  - The De Vinci of DirtyPipe Local Privilege Escalation – CVE-2022-0847
  - CVE-2023-36664: Command injection with Ghostscript PoC + exploit
  - A Deep Dive into DNS Debugging
  - Analysis of CVE-2023-38831 Zero-Day vulnerability in WinRAR
- Bugs
  - RCE on Application's Tracking Admin Panel
  - Frontend Fumbles: The 250$ Curious Case of API Key Permissions.
  - IDOR and Mass Assignment attacks leads to Full Account Takeover of Internal Employees
  - You can add extra zeroes. XSS bypass on a private bug bounty program
  - Exploiting Keepass
  - How Could a Self-XSS end with $$$$
  - Backend takeover due to JS based authentication.
  - Decrypting Requests, Manipulating Responses to Gaining Super Admin Access
  - The Art of Identifying X$$ & WAF Bypass Fuzzing Technique
  - Easy Bugs Easy Bounty

    - Uncovering Critical Security Gaps: How I Gained Admin Privileges
    - How I exploited CVE-2023–36845 and got root access in one domain.
    - Response Manipulation to Account Takeover
    - Invisible Indirect Injection On ChatGPT-4
    - API Endpoints Manipulation for Fun & Profit
    - IDOR | My first P2 that Lead to Full PII Exposure
    - My Bug Bounty failures
    - Mixin Network's $20 Million Bug Bounty: A Crypto Tale of Redemption
- CTF challenges
    - CloudSEK—Nullcon Cyber Security CTF 2023
    - HTB Machine Stocker
    - 10.2 Lab: Basic SSRF against another back-end system | 2023
    - HTB: Format
    - Domain Detection, Tunneling Tactics, and Shellshock Dominance: An iCSI CTF Challenge.
    - HTB: Aero

- Exploring TLSX by Projectdiscovery: A Powerful Tool for Security Enthusiasts
- Injectus: Your Gateway to Open Redirection Testing
- SocketSleuth: Improving security testing for WebSocket applications
- Skyhook – A Round-Trip Obfuscated HTTP File Transfer Setup Built To Bypass IDS Detections
- Pinkerton – An JavaScript File Crawler And Secret Finder Developed In Python
- AtlasReaper – A Command-Line Tool For Reconnaissance And Targeted Write Operations On Confluence And Jira Instances
- Promptmap – Automatically Tests Prompt Injection Attacks On ChatGPT Instances
- CloudRecon – CloudRecon is a suite of tools for red teamers and bug hunters to find ephemeral and development assets in their campaigns and hunts.
- SSRFire – Automated SSRF Finder

- when you hunt and the program language is PHP try access to any .php endpoint and test parameter ‘id’ and ‘list[select]’ for sql injection vulnerability.
- CVE-2023-0126 Pre-authentication path traversal vulnerability in SMA1000
- Always try to understand and analyze every request you see in Burp History. Indeed, the API Calls
- When testing a target, forget the fact that others have also tested it. Assume it is new, and check for all vulnerabilities
- Database Credentials Disclosure via Enabled Laravel Debug Mode