Bug Bytes #203 – CVSS 4.0, MOVEIt and How CI/CD Pipelines Go Wrong

BY TRAVISINTIGRITI · JUNE 14, 2023 · LAST UPDATED ON APRIL 1, 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 May 29th to June 11th

Click here to subscribe

Intigriti News

- 4 Tools to help you automate JWT Attacks
- Let's take a look at why this XSS won't execute, Another day, another XSS payload that won't execute
- Why might we want a rooted device when testing an Android app?

From my notebook

No real theme this week, here's some of the most interesting stuff I read!

1. Authentication Bypass Using Root Array – This is a deep dive into a #bugbountytips tweet diving in to the how and why of this authentication issue
2. CSP Bypass Unveiled: The Hidden Threat of Bookmarklets – I LOVE bookmarklets they're a combination of javascript and a bookmark to make dynamic bookmarks, anyway here's bookmarklet malware
3. Hacking AI: System Takeover in MLflow Strikes Again (And Again) – Good write up of an AI security bug!
4. Common Vulnerability Scoring System – CVSS has been updated to version 4, here are the changes
5. Casey Ellis: Pioneering The Bug Bounty Platform To Empower Ethical Hackers – Great podcast episode on the history of bug bounty hunting and a reminder of how dire disclosure used to be!
6. Patch Diffing Progress MOVEIt Transfer RCE (CVE-2023-34362) – OKAY extra bonus for this week, analysing the patch notes to reverse engineer the MoveIt bug

Videos 

- He Hacked His Own Company and Failed Miserably
- Reading 700 QRs with Python [Quilt – Hacky Easter 2023]
- Who should consider a career as a full-time bug bounty hunter? (shorts)
- OWASP API Top 10 Updates (shorts)
- The most common mistake of beginner security researchers? (shorts)
- How Can CI/CD Go Horribly Wrong?
- What does Shubs pay attention to when recruiting security researchers? (shorts)
- Sensitive Information Disclosure || Bug Bounty
- This Bookmark Hacks Discord Mods
- How to Become an Ethical Hacker 2023 V 03
- Next Level API Hacking with Kiterunner
- HackTheBox – TwoMillion
- Exploring the HackTheBox TwoMillion PHP Application
- Learn Bug Bounty Hunting with These Resources!
- Getting Offensive w/Phillip Wylie
- Blind SQL Injection Made Easy
- Hacking With ChatGPT by Mike Takahashi
- Trying to Find a Bug in WordPress
- How I broke into physical pentesting and my advice.

Podcasts

- NO. 384 — World AI Coin, Russian Power Attacks, Guidance AI Workflow...
- Risky Business #709 — Cl0p goes berserk with MOVEit 0day
- 134: Deviant
- Episode 378 – Naming things is harder than security
- EP124 Safe Browsing: Lessons from How Google Secures Five Billion Devices at Low False Positive Rates
- Episode 21: Chill Chat with Legendary DoD Hacker Corben Leo
- Hacker, Researcher, Educator, Entrepreneur, a Glimpse into The World of Vivek Ramachandran
- Dan Tentler on How the Old Ways Still Work

- Ever wonder why some people succeed while others don't?
- Hackers: Where do you get most of your tips + tricks from?
- Super excited to be accepted to teach at @DEFCON again this year! I'll be presenting my class "Hacking Organizations: Phishing Not Required" a course designed for red teamers, WebApp pentesters, or bug bounty hunters!
- Still struggling over that first bug hurdle? I got you let's hack an APIs together at NahamCon
- NahamCon2023 CTF registration is open now!
- I'm really excited and honored to be able to share my research around Unicode , ansi escape sequences and terminal command injections at Blackhat USA in August!

- Beginner
  - Ödül Avcılığı—Subdomain Keşfi (Turkish)
  - Ödül Avcılığı—File Upload XSS (Turkish)
  - Bug Bounty Recon (Part-2), Bug Bounty Recon (Part-3)

- Bug Bounty Bonanza: A Beginner's Guide
- How to write a Detailed Vulnerability Report
- A Beginner's Guide to Installing and Using the GF Tool
- Bug Bounty and Burp Suite for beginners
- Discover Sensitive Information on GitHub
- POST
- Mastering Subdomain Enumeration

- Intermediate
  - The differences between the same-site and the same-origin
  - Discover Sensitive Information on GitHub (Indonesian)
  - Hacking CSRF: Bypassing of CSRF token
  - Hacking Web Apps: Understanding Cross-Site Request Forgery (CSRF) Vulnerabilities
  - SQL injection with INSERT statement
  - How to Detect and Mitigate SSRF Vulnerabilities in the Early Coding Cycle: A Comprehensive Guide
  - Getting around x-requested-with header for CSRF
  - Understanding and Mitigating XXE Vulnerabilities via File Uploads
  - Uncovering the Secrets : The Potential of Web Archive in Bug Bounty Programs
  - How to use Maltego while doing bug bounty research?
  - Understanding Path Traversal Vulnerabilities and Their Exploitation

- Advanced
  - "Insights from Android VAPT"
  - Web3 Security Distilled
  - Build Centralized Security Workflows in Github: A tale of Reusable Workflows
  - Exploring a Lesser-Known Blockchain Vulnerability: The Vector Attack | Karthikeyan Nagaraj
  - Unveiling a Lesser-Known Blockchain Vulnerability: The Blockchain Time Warp Attack
  - Understanding a Lesser-Known Blockchain Vulnerability: Timestamp Manipulation

- Security Research
  - Pydio Cells: Unauthorised Role Assignments
  - Exploring Android Heap allocations in jemalloc 'new'
  - A deep-dive on Pluck CMS vulnerability CVE-2023-25828
  - chonked pt.1: MiniDLNA 1.3.2 HTTP Chunk Parsing Heap Overflow – Root Cause Analysis
  - Regular JSON
  - Avoiding the Apocalypse: A Guide to Finding Zombie APIs
  - RCE via LDAP truncation on hg.mozilla.org :: 0day.clickStoring Passwords – A Journey of Common Pitfalls
  - Bypassing CSP via DOM clobbering
- Bugs
  - Compromising Honda's power equipment / marine / lawn & garden dealer eCommerce platform through a vulnerable password reset API
  - XSS in Email Login Fields($$$)
  - BLH VULNERABILITY
  - HTML Injection in Craft-Cms Application
  - XSS in GMAIL Dynamic email (AMP for Email)
  - My First Bug: A Unique $500 XSS.
  - CVE-2021–44521: Apache Cassandra Remote Code Execution from vsociety
  - XSS Unleashed: Bypassing Filters with XLink Namespace
  - How I find valuable exploit in local bank website
  - Path traversal to RCE—Openfire—CVE-2023–32315
  - How I was able to get account takeover via IDOR form JWT
  - Turning a 50$ Tab-Nabbing vulnerability into a 1000$ Account takeover
  - How i Exploits bugs in web & Cross platform
  - Strategy v2 Burn Bug Post Mortem
  - XSS with 403 WAF Bypass for "(" and (document.cookie)
  - How Hackers can exploit Caching x Race-Conditions for followers count manipulation on Twitter
  - Weird Improper Access Control Bug of $$$
  - Simple Bugs—Buying Everything for Free!!!
  - Multiple CVEs affecting Pydio Cells 4.2.0
  - Rate Limit Bypass Leads to 0 Click ATO
  - How I Found Price Manipulation of Products Vulnerability
  - [TR] Bulduğum Price Manipulation of Products zafiyeti (Turkish)

    - A Story of API Key Leak in Page Source, Exploitation, Duplicate and Bounty.
    - AWS Chain Attack- Thousands of Vulnerable EKS Clusters
    - Breaking TikTok: Our Journey to Finding an Account Takeover Vulnerability
    - How a misconfigured Lotus Domino Server can lead to Disclosure of PII Data of Employees
    - IDor Bug Bounty
    - Unauthorized access to the Projects | Bug Bounty
    - Story Behind Open-Redirection worth $$$
    - Critical Finding on TP-Link service or how I got 0$
    - Automated Monitoring + Time = Bug, the bug on HackerOne Target (8×8)
- CTF challenges
    - HTB: Soccer
    - PicoCTF: Crack 'GDB Test Drive' Challenge In Practice
    - HTB: TwoMillion
    - Lack of Rate Limiting in vAPI
    - Vulnerable WordPress (Free Lab)
    - Broken Authentication in vAPI
    - TryHackMe | Valley Writeup
    - AllSafe (Intentionally Vulnerable Android Application)- Part 2
    - XSS Intigriti challenge
    - HTB: Bagel

- Burp-Dom-Scanner – Burp Suite's Extension To Scan And Crawl Single Page Applications
- LinkedInDumper – Tool To Dump Company Employees From LinkedIn API
- XSS-Exploitation-Tool – An XSS Exploitation Tool
- Complete Bug Bounty Tools List
- CloudBrute – Awesome cloud enumerator

- XSSwagger – A simple Swagger-ui scanner that can detect old versions vulnerable to various XSS attacks
- jsfinder – Fetches JavaScript files quickly and comprehensively from a defined list of URLs or domains

- Find creds on a red team campaign? Want to do more with them?
- Bug bounty hunters: want a #bugbountytip on finding the right public programs to participate in?
- Thousands of government websites are still vulnerable to CVE-2023-25157
- @gregxsunday is really doing it right. The dude puts out these really sick case studies and data-backed research methods on the regular.
- If you're only using Nuclei for HTTP requests, you're missing out!
- If you are a beginner in bug bounty I recommend don't ever buy any courses, nor look for mentors
- Reflected XSS Bug
- Here Is a weird CSR leads to XSS
- JSend – Burpsuite Community extension to fetch endpoints from all URL's from Proxy

- 60K+ Android Apps Have Delivered Adware Undetected for Months
- Service Rents Email Addresses for Account Signups
- The Growing Cyber Threats of Generative AI: Who's Accountable?