Bug Bytes #201 – Path Traversal, Prompt Injection, and GitHub Actions

BY TRAVISINTIGRITI · MAY 23, 2023 · LAST UPDATED ON MARCH 6, 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 15th to May 21st

Click here to subscribe

Intigriti News

- Exploiting file upload vulnerabilities a thread and a video
- This months XSS challenge!
- We're happy to announce the @PersonioHR program is now open to the public! Personio is a leading HR software company revolutionizing the way businesses manage their workforce
- Stay up to date with the latest challenges and events by joining our discord community

From my notebook

1. Exposing iCloud user's Name, phone numbers, and email addresses
2. How to turn a write-based path traversal into a critical?
3. Bug Bounty Changed My Life!
4. the story of "i915" bug, ChromeOS + Intel bounty programs, and beyond : pi3 blog
5. From GitHub to Account Takeover: Misconfigured Actions Place GCP & AWS Accounts at Risk – Rezonate

- Intro to Linux and Pentesting with World of Haiku

- The BEST Notetaking Apps Ranked
- $100,000 in two months with #bugbounty! (shorts)
- Here's a quick look at a path to becoming a webapp pentester! (shorts)
- Twitter Hacker Faces 77 Years in Prison
- Why Don't People Want Security?
- SESSION HIJACKING
- Learn to Hack Live | Token analysis & CTF
- Creating a SSH Honeypot with Python
- Answering your questions!
- Revealing Secrets with Information Disclosure Bugs
- Escaping the grind and decompiling python 3.9 pyc files
- Bug Hunting 101: Everything You Need to Know
- ChatGPT Analyzes Fake ChatGPT Malware
- .ZIP Domains Are a Disaster (Hackers Love them)
- the BEST resources for finding a cybersecurity job
- 15 – Authorisation Bypass (low/med/high)
- Networking And Cryptography || Penetration Testing Bootcamp
- HackTheBox – Precious
- Exploring a Simple Ruby Web Application
- Information Gathering(Part-2) || Penetration Testing Boot camp
- Why You Shouldn't Be An Ethical Hacker Part 1 (shorts)
- Getting Started with GeoGuessr and OSINT | UMDCTF 2023 (OSINT)

- 212 – Attacking VirtualBox and Malicious Chess
- Data privacy in a consumers world

- Episode 19: Audit Code, Earn Bounties (Part 2) + Zip-Snip, Sitecore, and more!
- Risky Biz News: Google will delete inactive accounts
- 297-KYC, 2FA, macOS, & OSINT Updates

- Uncomfortable (unpopular?) opinion
- A $1,000,000 bounty?
- One of my first ever bug bounties was an XSS against a WordPress host. It wasn't anything super special but the process I used to find it is one that has yielded loads of bugs over the years.
- Celebrating One Year as a Full-Time Bug Bounty Hunter!
- send help
- I recently got a nice surprise from @IntelSecurity: a $10,000 #BugBounty for a bug they have found internally resulting from one of my report comments.
- Found an endpoint with `something.php?run=`, execute the encoded `%26echo%20`id`%24()%5C%20 ` in HTTP request, surprised to see when server returned ID.

- Beginner
  - How to get started as an API hacker
  - Easy ways to Exploit HTML Injection
  - automation Rxss
  - LDAP protocol basics and the LDAP Injection attack
  - DoS vs DDoS vs DRDDoS vs PoD attack
  - Unveiling the Hidden Dangers: Exploring WordPress Vulnerabilities
  - Understanding Insecure Direct Object References (IDOR)
  - Privileges Escalation Techniques (Basic to Advanced) for Windows

- Intermediate
  - Intro to IOT Hardware Hacking
  - What is Forward Proxy and Reverse Proxy
  - How to Learn Manual SQL Injection for OSCP(Step by Step)
  - Attacking Active Directory & Kerberoasting
  - Unveiling Smart Contract Vulnerabilities: Challenges and Best Practices for Bug Bounty Hunters
  - Insecure Deserialization: Unraveling the Hidden Vulnerabilities
  - Digging Deeper: Unearthing Business Logic Vulnerabilities in Advanced Web Applications
  - Client Side Template Injection (CSTI)
  - Lateral Movement : Navigating the Intricate Web of Network Protection
  - Automating Adversary Emulation for my Lab Using MITRE Caldera
- Advanced
  - Learn Buffer Overflow for OSCP- TryHackMe
  - Hacking embedded systems using the routersploit tool
  - How I Built My 4th Level Deeper Subdomain Enumeration VAPT Automation Script Tool
  - Exploiting IAM security Misconfigurations—Part 1
  - Advanced Bug Bounty Reporting: Mastering the Art of Persuasive Details
  - Combining Python + ChatGPT + Payload Processor (burp) for brute forcing OTP
  - Detecting & Bypassing Defensive Measures (Canary Token)
  - From Theory to Reality: Explaining the Best Prompt Injection Proof of Concept
  - Tips and tricks for Burp Suite Pro, ten years later

- Security Research
  - Triple Threat: Breaking Teltonika Routers Three Ways
  - “Malverposting”—With Over 500K Estimated Infections, Facebook Ads Fuel This Evolving Stealer...
  - Synacktiv Webflow Arbitrary Email Forgery

- redrays-io/SAP_Cloud_Connector_SSFS_Decryption: A PoC of decryption the SAP Cloud Connector SSFS
- PGP signatures on PyPI: worse than useless
- Exploit For CVE-2022–41544—RCE in Get-Simple by vsociety
- Testing a new encrypted messaging app's extraordinary claims

- Bugs
  - Malicious code in PDF Toolbox extension
  - Python Penetration Testing: Microsoft 365 Session ID Login
  - SQL injection on a hidden API endpoint
  - How I was able to use Premium Feature for Free
  - Free Wallet TopUps
  - Fuzzing ends with XSS
  - Cors Misconfiguration
  - Hardcore RCE via directory name for $3.000
  - Account Takeover using Inspect element
  - Easy CSRF bypass
  - how i accidentally discovering XSS
  - Blind OS Command Injection via Activation Request
  - Stored Iframe Injection & Permanent Open Redirection – Zero Day
  - How improper OTP implementation could lead to Account Take Over (Part 2)
  - Bypassing Rate Limit
  - Why You Should Always Check The Audit Log [Medium]—$500
  - How I got My First Bug on a public Bug bounty program??
  - Reflected Cross-Site Scripting Vulnerability in Ellucian Ethos Identity CAS Logout Page
  - How ChatGPT exposes conversations from other users without being considered a vulnerability
  - IDOR leading to Privilege Escalation!
  - AEM Bug in Adobe
  - Full website takeover
  - DOS via cache poisoning
  - Behind the Scenes: Discovering an OTP Leakage Bug in a Leading Broadband Service's Website
  - Path Traversal Vulnerability
  - My Second VDP Bug Went Critical: Grafana Admin Panel Bypass
  - .

    - Uploading the Webshell using filename of Content-Disposition Header Story!
    - Account Takeover + IDOR
- CTF challenges
    - TryHackMe—Steel Mountain Simple Writeup by Karthikeyan Nagaraj | Mr. Robot | 2023
    - HackTheBox WriteUp—Ghoul
    - Network Services—Enumerating and Exploiting variety of network services and misconfiguration & Network Services 2—Enumerating and Exploiting More Common Network Services & Misconfigurations
    - SQL Injection Vulnerability in GoLang Code #2
    - Crack the Code: A Guide to Defend the Web CTF Crypt Challenges 1–5
    - Beginner's Guide: Defending Web SQLi 1–2 CTF Challenges
    - OverTheWire Bandit: Solving Level 4—Dealing with Hidden Directories
    - HTB: Precious
    - Intro to Docker | Tryhackme Writeup/Walkthrough
    - How to Pass the APIsec University—API Penetration Testing Certificate

- PASTIS For The Win!
- ADCSKiller – An ADCS Exploitation Automation Tool
- C2 and the Docker Dance: Mythic 3.0's Marvelous Microservice Moves
- KeePass 2.X Master Password Dumper (CVE-2023-32784)
- WebPalm is a command-line tool that enables users to traverse a website and generate a tree of all its webpages and their links.
- KoodousFinder – A Simple Tool To Allows Users To Search For And Analyze Android Apps For Potential Security Threats And Vulnerabilities
- Bypass-403 – A Simple Script Just Made For Self Use For Bypassing 403
- nuclei-burp-plugin – A Burp Suite plugin intended to help with Nuclei template generation
- Nginxpwner – Simple tool to look for common Nginx misconfigurations and vulnerabilities

- SubDomainizer – A tool to find subdomains and interesting things hidden inside.

- Walking the Tightrope: Maximizing Information Gathering while Avoiding Detection for Red Teams – TrustedSec
- Here's a useful recon one-liner using 2 of my tools!
- How to use Amass to find ASNs and CIDRs and then enumerate subdomains with them!
- Extract all URL endpoints from an application and dump them to the command-line with hakrawler
- Consistency is key in bug hunting. Regular practice not only sharpens your skills but also keeps you updated on new vulnerabilities.
- One of the fundamentals you need to exploiting issues you find is trying to understand what you have from the data you observed
- Don't ever post this type of shit, but everyone always talking JS files or GitHub etc. There is always shit hanging around in the HTML, don't forget to check
- Oh wow! In @Burp_Suite you can scope your search to ONLY a specific host by right clicking -> engagement tools -> search. The more you know
- f you are using Powershell and are going to use ADS to inside the restricted /bin/ folder, remember to escape the $ sign: bin::`$INDEX_ALLOCATION

- Google releases .zip domain names, everyone has questions and concerns
- Montana becomes first U.S. state to ban TikTok