Bug Bytes #198 – Hackers go to RSA/BSides and CPanel gets pwned

BY TRAVISINTIGRITI · MAY 3, 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 April 24th to April 30th

CLICK HERE TO SUBSCRIBE

Intigriti News

- April Challenge results
- Understanding SSTI tweet thread!

From my notebook

It was RSA and BSides San Francisco this week, but that didn't stop some amazing research coming out of AssetNote, a fun LLM backdoor and hackers live in SF to chat about making content!

1. Ambushed by AngularJS: a hidden CSP bypass in Piwik PRO
2. Finding XSS in a million websites (cPanel CVE-2023-29489)
3. Deep Dive OSINT (Hacking, Shodan and more!)
4. Cybersecurity Content Creators | ITSPmagazine Event Coverage: RSAC 2023 Broadcast Alley
5. Accidental LLM Backdoor – Prompt Tricks

Other Amazing Things

- How to set up an Android Penetration Testing Lab from scratch
- [0b00] Reversing 101 :: Hacking Closed-Source Firmware

- How I Broke in to Cyber Security... And you can too!
- Snapchat paid a hacker $15,000! (shorts)
- A Conversation with Cybersecurity Community OG and EH-net Founder
- Web Challenges [Space Heroes CTF 2023]
- Top 3 Programming Languages for Cybersecurity in 2023
- CodeQL query to detect RCE via ZipSlip – $5,500 bounty from GitHub
- How to Not Suck at Hacking // How To Bug Bounty
- Hack The Box – Looking Glass (Easy) – Live Walkthrough
- What's the hardest part of writing a CodeQL query? (shorts)
- Writing a CodeQL query – the sink (shorts)
- What is CodeQL bug bounty program? (shorts)
- How To Test Your Security with Atomic Red Team
- Want to become a Bug Bounty Hunter? (shorts)
- Level Up Your CTF Skills INSTANTLY!
- Twitter OSINT ft. OSINTFramework
- Five resources to learn hacking, pentesting or get started (shorts)
- Episode 05 Cloud Hacking GCP V 01 v2 BLURRED V2
- Hack The Box – Sanitize (Easy) – Live Walkthrough
- Leaking Secret Data with a Heap Overflow – "Leek" Pwn Challenge
- HTB Stories 0x13: Tales, Tendencies, and PoCs with Mubix
- Hack The Box – Baby Waffles (Easy) – Live Walkthrough

- 295-Breach Data Collection Revisited
- Is the industry ready for AI?
- 206 – A Ghostscript RCE and a Windows Registry Bug

- The CEO who also ran IT, Strava strife, and TikTok tall tales
- Risky Business #703 — Russia whines about its tech dependence on China
- SN 920: An End-to-End Encryption Proposal – Wipe those routers, Lockdown Mode, ChatGPT black market
- 205 – SecurePoint UTM, Chfn, and Docker Named Pipe Vulns
- EP118 RSA 2023 – How to Protect Your Organization from Cyberattacks in a Time of Political Turmoil

- Should you learn to code before you learn to hack?
- OpenAI's new "Code Interpreter" gives every user a sandboxed k8s container which analyzes and executes arbitrary python code.
- CodeQL is a unique bug bounty program that rewards you for writing a scanner query to detect a CVE that is currently undetected.
- "The Bug Hunter's Methodology Live"
- I think bug bounty platforms will see a huge decrease of excellent hackers in the next years.
- This is the second time that I have requested a CVE from @MITREcorp where they have not filled out the details of the CVE before assigning it to us, even though all details were provided in the initial request. Is there a better way to claim CVEs these days?

- Vulnerability Capstone—TryHackme Room Simple Writeup | 2023
- HTTP parameter pollution : Bug bounties [Server-Side ; Client-Side]
- How To find Subdomain Takeover
- Secure Your Docker Compose Web App: A Comprehensive Guide for Penetration Testers
- Understanding the Shell Shock Vulnerability: A Comprehensive Guide | 2023

- SSRF in vAPI
- Complete Bug Bounty Recon Fundamentals.
- All in One Guide to Burp Suite: Hands-On
- (Reverse) shell to your Azure VM as 'Local System' user or 'root' user
- MY Methodology for Cross Site Scripting (XSS)
- File Inclusion—TryHackMe Simple Write up | 2023
- Python Penetration Testing: Connecting multiple SQL Databases to gather Juicy data

- Bug Bounty Writeup: Stored XSS Vulnerability WAF Bypass
- Authentication Bypass Email and Number Verify
- How I Chained an Information Disclosure Bug with SQL Injection
- Netflix—Bypassing Multi-Factor Authentication (MFA)
- How improper OTP implementation could lead to Account Take Over (Part1)
- How I was Able To Find Reflected XSS ?
- "Exception in thread "main" java.lang.NoClassDefFoundError:
- Bypass OTP Lead to Account Takeover on pashouses.id
- Client Side Desync Attack (CL.0 Request Smuggling)—Bounty of $150
- Researching Polymorphic Images for XSS on Google Scholar
- API Misconfiguration – Algolia API Key
- Azure security—Internal recon leveraging lack of access control
- Azure Privilege Escalation Via Service Principal
- Break the Logic: Playing with product ratings on a shopping site(600$)
- Abusing Javascript:history.back() as an open redirect
- Git Arbitrary Configuration Injection (CVE-2023-29007)

- CVE-2023-1767 – Stored XSS on Snyk Advisor service can allow full fabrication of npm packages health score

- GitHarvest3r—Simple CVE github exploit gathering tool written in python.
- Take screenshots of domain list while doing recon.
- hardCIDR – Linux Bash Script To Discover The Netblocks, Or Ranges, Owned By The Target Organization
- REcollapse Is A Helper Tool For Black-Box Regex Fuzzing To Bypass Validations And Discover Normalizations In Web Applications
- Sh4D0Wup – Signing-key Abuse And Update Exploitation Framework
- FirebaseExploiter – Vulnerability Discovery Tool That Discovers Firebase Database Which Are Open And Can Be Exploitable
- Bearer – Code Security Scanning Tool (SAST) That Discover, Filter And Prioritize Security Risks And Vulnerabilities Leading To Sensitive Data Exposures (PII, PHI, PD)
- PhoneSploit-Pro – An All-In-One Hacking Tool To Remotely Exploit Android Devices Using ADB And Metasploit-Framework To Get A Meterpreter Session
- httpx now supports screenshots using -screenshot
- Dorky – a new tool to quickly do keyword searches over Gitlab and Github for OSINT & bug bounty recon
- Just updated the legacy IIS Short File Name scanner (to v2023.3) to address an issue that it could miss some rare vulnerable servers due to an intrusive RegEx responsible to clean dynamic contents.

- reset password attack checklist, IDOR Checklist and adminpanal Bypass checklist

- found this Stanford course for web security; with exam papers, assignments, labs & everything
- One way to save and display ffuf results as a nice table using the Linux command "column"
- And these 0s can come in handy! Here is just one example of some bypasses for PHP's gethostbyname() https://onlinephp.io/c/f9855 This was a bypass in @WordPress which led to SSRF because of https://developer.wordpress.org/reference/functions/wp_http_validate_url/... (reported 5 years ago!)
- Need to bypass the JWT signature? Kid param injection + directory traversal = signature bypass