Bug Bytes #200 – AI Red Teaming, Firmware and Reverse Engineering, Prompt Injection Defence

BY TRAVISINTIGRITI · MAY 17, 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 8th to May 14th

Click here to subscribe

Intigriti News

- Familiar huh? Let us show you how you can exploit this XSS case
- If you want to master SSTI exploitation, open this thread!
- The intigriti YouTube channel has officially passed the 15k milestone!
- We've got a few insecure file upload videos for ya'll this week, covering practical labs from @WebSecAcademy
- Public program alert! 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

From my notebook

1. I MADE $100,000 IN TWO MONTHS!
2. 1 tip to improve your pentesting & bug bounty hunting
3. My Internship Journey
4. AI Village at DEF CON announces largest-ever public Generative AI Red Team
5. Issue 219: Money Lover app exposes user data, most web API flaws missed by standard testing

Videos 

- Hacking Complex Passwords with Rules & Munging
- Facebook's TOP1 bounty hunter doesn't bother reporting $4,000-$5,00 (shorts)
- Hack The Box – Gunship ("Very Easy") – Live Walkthrough
- What is Clickjacking?
- Browser in the browser attack (shorts)
- Must-Follow Cybersecurity Content Creators (shorts)
- Getting Started in Firmware Analysis & IoT Reverse Engineering
- Securing AI – Prompt Injection Defense
- Magecart Hackers Perfect Fake Checkout Pages
- Hide a Hacker's Reverse Shell in ONE Command
- FIVE Practical AI Uses for Cybersecurity
- Prerequisites || Penetration Testing Bootcamp

Podcasts

- Wireless Hacking with Hardware from the SME Kody Kinzie!
- The REAL Value of Cyber Threat Intel (And How To Get It)
- 296-The Argument for a Stock Browser
- The Right Amount of Trauma
- Episode 18: Audit Code, Earn Bounties
- 210 – TPMs and Baseband Bugs

- SN 922: Detecting Unwanted Location Trackers – Google Passkeys, Chrome lock icon, AI news sites, Vint Cerf
- 209 – Bad Ordering, Free OpenAI Credits, and Goodbye Passwords?
- What if AI could rebuild the middle class?
- EP120 Building Secure Cloud and Building Security Products: Finding the Balance
- Risky Biz News: DEFCON attendees will target AI models
- Episode 374 – The event we called left-pad, Episode 77 remaster part 1

- I did a few hours of bug bounty for a few nights last week to get a feel.
- Never get too proud to go back to the basics and LEARN like a beginner again.
- Me and my projects since GPT3 is accessible.
- Secret Tip – Keep checking your notes
- "We take our security very seriously."
- I'm really baffled how y'all find SQL injections so effortlessly. All you SQLi experts, I'll be in your DM's today.

- Beginner
  - Master the Art of Linux Firewall: Practical Guide to Iptables
  - The Secrets Behind EC2 Takeovers
  - Bug Bounty: Automate Blind SQLi
  - Search for sensitive data using theHarvester and h8mail tools
  - Kickstart Your Bug Bounty Hunting Journey
  - Cross-Origin Resource Sharing (CORS).

    - The Insider's Guide to Detecting and Preventing XSS Attacks: Tips and Tricks for Web Developers
    - What is path travelsal vulnerability?
    - How to not get paid for your submission.
    - Bug Bounty Mistakes I Made, So that You Can Avoid
- Intermediate
    - Handlebars Templating: Security Best Practices
    - SSRF: What is forgery, and what is exploitable information
    - How I Cracked CEH Within 6 Months Only With Free Resources.
    - Journey of a Script writer (Tool developer)
    - What is a zero-day (0-day) exploit? Real-life examples
    - What is insecure deserialization
    - Bypass Rate Limit Request (fuzzing/etc...) With TOR
    - Understanding LDAP Injection: Crafting Payloads and Mitigation Strategies
    - Bypassing Protocol Concatenation in SSRF: Strategies for Testing Vulnerable Applications
    - Populating Burp Suite's Sitemap using SpiderSuite crawler
- Advanced
    - Understanding HQL Injection and How to Prevent It
    - Exploring Algorithm Confusion Attacks on JWT: Exploiting ECDSA
    - The Security Researcher's Guide to Reporting Vulnerabilities to Vendors
    - A guide to writing network templates with Nuclei!

- Security Research
    - Bypass IIS Authorisation with this One Weird Trick – Three RCEs and Two Auth Bypasses in Sitecore 9.3
    - CVE-2022–26180:qdPM 9.2 CSRF Vulnerability in index.php/myAccount/update URI
    - Breaking Down Barriers : CVE-2023–2227
    - The printer goes brrrrr, again!

    - Prompt injection explained, with video, slides, and a transcript
    - Testing Zero Touch Production Platforms and Safe Proxies · Doyensec's Blog
    - Attacking APIs by tainting data in weird places
- Bugs
    - Unveiling the Untold Secrets: Unearthing the Holy Grail of Bug Bounties—How I Hacked EC2
    - Bypass SMS Authentication To Account Takeover (Indonesian)
    - SQLi Using Google Dorks
    - /Metrics Open Directory Bounty : 50$~200$
    - Discovering a Hidden Security Loophole: Rent luxury Cars for a Single Dollar
    - One Bug at a Time: My First Paid Bug ($1,000 IDOR)
    - Hyperlink Injection Earned Me $200 within 10 minutes
    - Automating XSS Detection: How My Setup Earned Me a Few Spots in various Hall of Fames
    - RCE due to Dependency Confusion—$5000 bounty!
    - Discovery of an XSS on Opera
    - How I bypassed the registration validation and logged-in with the company email
    - Hacking Chess.com: My Journey to Unlock Premium Bots on the Android App
    - My First Bug: Accessing Admin Page via Blind XSS $1000
    - Account Takeover via Signup Feature
    - Full Account takeover (even for admins)
    - Admin Account Takeover worth $5,657
- CTF challenges
    - Bypass JWT Authentication | Access Admin Panel
    - Network Services 2—Enumerating and Exploiting More Common Network Services & Misconfigurations
    - HTB: Interface
    - OverTheWire Bandit: Solving Level 0
    - TryHackMe—Res Room Simple Writeup
    - Skynet—TryHackMe Room Simple Writeup
    - PicoCTF asm3 challenge: Master the Art of Reverse Engineering—StackZero
    - AI Hacking Games (Jailbreak CTFs)

- Indicator-Intelligence – Finds Related Domains And IPv4 Addresses To Do Threat Intelligence After Indicator-Intelligence Collects Static Files
- SpiderSuite – Advance Web Spider/Crawler For Cyber Security Professionals
- Domain-Protect – OWASP Domain Protect – Prevent Subdomain Takeover
- Lfi-Space – LFI Scan Tool
- DNSRecon – DNS Enumeration Script
- PwnFox – A Firefox/Burp Suite extension that provide usefull tools for your security audit.
- gitGraber – monitor GitHub to search and find sensitive data in real time for different online services such as: Google, Amazon (AWS), Paypal, Github, Mailgun, Facebook, Twitter, Heroku, Stripe, Twilio...

- Want to succeed in bug bounties? Follow these 10 tips!
- View the recon data for every amass scan that you've ever done by using the db subcommand
- Trouble figuring out which ASN belongs to a company?
- XSS WAF Bypass using location concatenation
- Add "ui_config.properties" and "http://config.properties" files to your wordlist, these files contain juicy info like secret tokens and passwords
- Reflected XSS via Google Dorking
- Want to start bug bounties but don't know where to begin?
- If something is suspicious but SQLMap "thinks" it might/might not be vulnerable, manually confirm/deny before leaving.

- Found an interesting #XSS where I inject the payload within the image file name and got the alert!.
- Image upload path tip

- Capture The Bug's Ethical Hacker: Valligayatri Rachakonda
- AI Is About to Be Everywhere: Where Will Regulators Be?
- WordPress Plug-in Used in 1M+ Websites Patched to Close Critical Bug