Bug Bytes #196 – Prompt Injection, Self Healing Code, Access Control and Hacker Motivation

BY TRAVISINTIGRITI · APRIL 19, 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 10th to April 16th

CLICK HERE TO SUBSCRIBE

Intigriti News

- Intigriti's March Challenge is over! Check out the winners

From my notebook

Another week another AI/LLM themed issue but as we move past the initial hype stage we're starting to see the cracks of LLMs particularly with the news that OpenAI started a bug bounty program, leading to some familiar faces already hitting the top 10 hackers on the program!

1. On self-healing code and the obvious issue – Gynvael shares some thoughts on asking code to fix their own bugs
2. Attacking LLM – Prompt Injection – LiveOverflow talks "prompt injection"
3. ReconAIzer: A powerful extension for Burp Suite that leverages OpenAI to help bug bounty hunters optimize their recon process. – A new Burp addon hopes to leverage GPT for recon tasks
4. Using AI to Develop Realistic Sock Puppet Accounts – Another use of AI in security
5. Google Tells AI Agents to Behave Like 'Believable Humans' to Create 'Artificial Society' – Finally do androids dream of electric sheep?

Other Amazing Things

- WHY YOU SUCK AT HACKING // How To Bug Bounty
- Python Script to Read Files on Encoding
- Wi-Fi Deauther || Attacks Demonstration
- PHP's Unsafe parse_url Function
- Cybersecurity Mental Health Statistics
- Episode 03 More Cloud Hacking Vulns
- Python Pwntools Hacking: ret2libc GOT & PLT
- Attacking Password Resets with Host Header Injection
- Is #cybersecurity #remotework a Thing? (Spoiler Yes)
- Learn to Hack Web Apps – Live | #APIs #BOLA #brokenAuth
- Cybersecurity Labs (FOR FREE) – Linux Backdoor Analysis
- TryHackMe – Attacktive Directory (Medium) – Live Walkthrough
- Most ChatGPT Extensions Are Just Malware
- My Hacking Setup and How to Use It (Firefox/Burp Community)
- What is Server-Side Request Forgery (SSRF)?
- How to Hack MFA
- WAF bypass and vulnerability chain exploiting parser differentials | Waffle-y Order @ HackTheBox
- [0x0d] Reversing Shorts :: Real-World Tutorials
- 3 Types of Bug Bounty Automation! (Automation Series)

- Episode 15: The Israeli Million-Dollar Hacker
- Inside the history of a child hacker.
- Episode 370 – Open Source is bigger than you can imagine
- 203 – Pentaho Pre-Auth RCE and Theft by CAN Injection
- EP116 SBOMs: A Step Towards a More Secure Software Supply Chain

- Episode 14: Mobile Hacking Dynamic Analysis w/ Frida + Random Hacker Stuff

- #NahamCon2023 | June 15-17: Opening Keynote by @emgeekboy and @codecancare CTF by @_JohnHammond/@JustHackingCo Hosted by @ippsec and @Alh4zr3d Workshops by @Jhaddix, @Agarri_FR, @0xTib3rius
- The most interesting piece of the ChatGPT plugin leak was the plugin that @openai was using to assess the security of the other plugins. Here's how it works.
- The DoD experienced its largest leak in 10 years.
- Struggle with mental health? Work in cyber? You're not alone.
- Newbie pentesters, remember: Don't get discouraged by failure. Embrace it, learn from it, and grow stronger. We all started somewhere, and perseverance is key to success.
- Just listen to how well @stokfredrik manages to capture the essence of how cool bug bounties are.
- I once sought guidance from the PortSwigger team on minimising memory usage when developing Sharpener which is a Java extension for Burp Suite

- HackTheBox – Encoding
- [HTB] Session Security
- What is a reentrancy attack?
- 5 common Vulnerabilities in smart contracts
- Unravelling the Secrets of Reverse Engineering: Practical Applications for In-Depth Analysis
- Hack Internal Service Desks
- NahamStore—TryHackMe Room
- Mastering Server-side Request Forgery (SSRF): Exploitation Techniques and Practical Labs

- AppSec Tales XIII | SQLI
- Information Disclosure and Bug Bounty Basics
- Introduction to OSINT
- JWT [JSON WEB TOKENS] [ALGORITHM CONFUSION ATTACK] (0x03)
- Attacking Kubernetes—Part 1
- Evading Attribution & Moving Laterally on AWS
- Advanced Web Application Security: Exploiting SSTI Vulnerabilities

- Shell in the Ghost: Ghostscript CVE-2023-28879 writeup
- Java Exploitation Restrictions in Modern JDK Times
- The Uninvited Guest: IDORs, Garage Doors, and Stolen Secrets
- Rule Writing for CodeQL and Semgrep
- How I found P2 bug in 5 mins
- Rukovoditel 3.3.1—Remote Code Execution (RCE)
- The Danger of Automatic Login: Bypassing MFA
- Bypassing the 2FA /MFA—An Easy win
- Rate Limit Bypass By Parameter Tampering | Easy Win
- How exploitable sensitive information in API is able to destruct business in disruption era / How exploitable sensitive information in API is able to destruct business in disruption era
- Bugbounty Write-up: IDOR Vulnerability in User Deletion Process
- From Django Debug Mode to PII Data Leak of more than 500+ Employees due Broken Access Control
- IDOR on Resend SMS Verification
- Account Takeover By OTP Brute force

- CVE-2023–29218:Twitter Recommendation Algorithm Vulnerability
- A successful prototype pollution chained to a DOM XSS
- How I found a Confluence Cloud misconfiguration affecting hundreds of companies: My first writeup!
- Revealing a Logic Flaw in an E-commerce Website
- SecurePwn Part 1: Bypassing SecurePoint UTM's Authentication (aka CVE-2023-22620) to take over the device

- Auto-GPT is an experimental open-source application showcasing the capabilities of the GPT-4 language model. This program, driven by GPT-4, chains together LLM "thoughts", to autonomously achieve whatever goal you set.
- Websites for subdomain enumeration
- Fuzzing Made Easy: How to Use wfuzz for Efficient Web Application Testing?
- Awesome Hacker Search Engines: A curated list of awesome search engines useful during Penetration testing, Vulnerability assessments, Red/Blue Team operations, Bug Bounty and more
- Scriptkiddi3 – Streamline Your Recon And Vulnerability Detection Process With SCRIPTKIDDI3, A Recon And Initial Vulnerability Detection Tool Built Using Shell Script And Open Source Tools
- Nmap-API – Uses Python3.10, Debian, python-Nmap, And Flask Framework To Create A Nmap API That Can Do Scans With A Good Speed Online And Is Easy To Deploy
- debugHunter – Discover Hidden Debugging Parameters And Uncover Web Application Secrets
- QuadraInspect – Android Framework That Integrates AndroPass, APKUtil, And MobFS, Providing A Powerful Tool For Analyzing The Security Of Android Applications
- Certwatcher – Tool For Capture And Tracking Certificate Transparency Logs, Using YAML Templates Based DSL
- OpenAI (LLM) Integration is coming to @pdnuclei using DSL that can be used in the template input/output context.
- Scoper: Burp Suite extension that allows users to easily add web addresses to the Burp Suite scope.
- Puredns: Fast domain resolver and subdomain bruteforcing with accurate wildcard filtering

- Fuzzing Smart Contracts Yields this Research Team $100K+ in Bounties
- The Best Vulnerability Disclosure Programs (Less Competitive Bounties)
- I faced an interesting scenario about browser behaviors after discovering an unexploitable Reflected XSS.
- 5 CSRF exploitation techniques
- You cannot perform any active requests to out-of-scope domains, but since with passive enumeration, you don't actually make any requests to the out-of-scope domain...