Bug Bytes #185 – ChatGPT, ChatGPT and more ChatGPT

BY TRAVISINTIGRITI · DECEMBER 14, 2022 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-185-chatgpt-chatgpt-and-more-chatgpt

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 December 5th until December 11th.

Click here to subscribe

Intigriti News

- Vulnerable code snippet and the solution!
- November XSS challenge
- We packed our bags and headed to BlackHat EU in London

From my notebook

While ChatGPT released at the tail end of last week, we really saw the hacking community embrace it this week and start to experiment what can be done with the new chatbot. From its ability to generate code, to bypassing the security filters, so here are my top 5 of ChatGPT resources. If you want to play with it, if you haven't yet it's free you need an account and phone number, http://chat.openai.com.

1. Can AI create a flyhack in Minecraft? – LiveOverflow did a stream where he explored using ChatGPT to write a flyhack mod for Minecraft, this is a cut down video with the highlights, he experiments with creating a flyhack and bypassing the server's anti-cheat protection. He also argues with it which is actually very funny.

2. Exploring Prompt Injection Attacks – This post on NCC's blog looks at the ability to bypass content filters using a 'malicious' prompt, these prompts are often something like "ignore the above and...", and work on a variety of LLMs (large language models)

3. Temporary policy: ChatGPT is banned – StackOverflow has decided to ban the use of ChatGPT for answering code questions, this is primarily due to the bot's habit of being confidently incorrect as well as to reduce low effort contributions on the website.

4. ChatGPT bid for bogus bug bounty is thwarted – Sneaky bug hunters are trying to use ChatGPT to find security flaws, it did not go well! But as a positive at least the person triaging noticed they were arguing with a bot fairly quickly.

5. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It – This blog post from 2019 covers a short introduction to AI security bugs, if you're interested in learning more about AI security it's a fantastic place to start.

- HackTheBox UniCTF 2022 Talk – Variable is what you make of It
- run SHELLCODE within BASH!?!
- Phonebook.cz || Bugbounty Recon
- Google vs. ChatGPT for Hackers #shorts
- Hackers Exploit TikTok Trend to Spread Malware
- Linux Portbending Explained
- Setting up a new box for recon/hacking. Let's go!
- Interview with Guy Podjarny | Snyk, problems in cybersecurity,
- Ethical Hacking in 15 Hours – 2023 Edition – Learn to Hack! (Part 1)
- The Future Of Hacking #shorts
- HackTheBox – Outdated
- How to get a CVE | Methodology
- Infosec Jupyterthon 2022 Day 1
- Live Hacking On Indeed with Tess | Hacker2Hacker

- EP100 2022 Accelerate State of DevOps Report and Software Supply Chain Security
- NO. 360 | NEWS, ANALYSIS & DISCOVERY SERIES
- The Problem With Kernel-Mode Anti-Cheat Software [ML B-Side]
- 173 – Remotely Controlling Hyundai and a League of Legends XSS

- 301: AI chatbot or the start of Skynet? Eufy privacy, and hot desks
- 174 – A Huawei Hypervisor Vuln and More Memory Safety
- YOU DON'T ALWAYS NEED AWS EKS IN YOUR LIFE!

- A thread of courses and books for continued professional development
- AppSec interview tips by D0nut
- Overcoming bug bounty burnout by Rez0
- Full schedule for Nahamcon

- Set up Cloud Instances
- Intercepting HTTP traffic with OpenVPN on Android
- Bug Hunting 101—Credential Stuffing Vulnerabilities
- How you can find your first bug using google
- JavaScript – The language made for bugs
- Upgrading Your XSS Bugs from Medium to Critical: Techniques and Examples
- XSS Hunter Slack Alerts
- All about: Single-Sign On (SSO)
- Recon
- Mobile Bug Bounty Hunting? Enter BLE
- GraphQL Exploitation Techniques | Fintech Bug Bounty—Part 2

- [BAC/IDOR] How my father credit card help me to find this access control issue
- OTP Leaking Through Cookie Leads to Account Takeover
- NETGEAR Router Network Misconfiguration
- Coming across C++ BOF (Buffer Overflow) Vulnerabilities Within Libraries (part 2) EXTENSION
- How we breached ZDFheute live on television
- [WRITE-UP] Irremovable comments on the FB Lite app (Bounty: 500 USD) | by Shubham Bhamare
- [WRITE-UP] Irremovable Facebook group album photos and entire album under certain circumstances (Bounty: 1000 USD) | by Shubham Bhamare
- Facebook page admin disclosure by “Create doc” button (Bounty: 5000 USD)
- [WRITE-UP] Facebook page admin disclosure by “Message Seller” button (Bounty: 1500 USD)
- How to Hack Applications’ Logic
- Reflected XSS using Double Encoding
- SQL Injection Extracts Online Users status , completed registrations, net overall posts l Database
- Sensitive Information Disclosure in Mobile Application
- How I Found my First website Vulnerability
- P1 Bug Hunting—Account Takeover w/ 2FA Bypass
- Account takeover without user interaction via the mail server
- Hacking Government-Millions of Death-Certificate(EASY)
- A software bug captured Apple and other huge companies
- CORS Misconfig on Out of scope domain Bug Bounty Writeup (300 USD Reward)
- Bug Bounty Hunting 101—Remote Code Execution (RCE)
- Privilege Escalation to remove the owner from the organization
- Vertical Privilege Escalation: The user can takeover an admin account via response manipulation
- STRIPE Live Key Exposed:: Bounty: $1000
- Cross Origin Resource Sharing: Hacking Bank Accounts

- Scoring $$$ for a very simple bug : You don't always need proxy tools
- Automate Cross-Site Scripting (XSS) exploitation with unusal events and Burp Intruder
- Block 1M+ users from accessing their accounts by taking over third-party service
- How "I hacked the Dutch government and got the lousy t-shirt"
- Parameter Tampering Bug _ 3999 -> 3:
- Bug Writeup: RCE via SSTI on Spring Boot Error Page with Akamai WAF Bypass
- IDOR + PII Leakage
- Hacking into Wi-Fi Camera TP-Link Tapo C200 (CVE-2021–4045)
- The most underrated injection of all time—CYPHER INJECTION.

- Taking Over Databases using SQL Map—SQL Injection Attacks
- 10 Practical Recon & vulnerability Scanners for bug hunters (part one)
- Subdomain Enumeration...? DNS-Discovery
- Klyda – Highly Configurable Script For Dictionary/Spray Attacks Against Online Web Applications
- Frida-Mobile-Scripts – Collection of useful FRIDA Mobile Scripts
- Nuclei updates
- Using Recon-Ng for Recon for Bug Bounty

- Authentication bypass tips
- Bug bounty testing routine
- Replacing an ID in an API with -1

- RESPONSE MANIPULATION LED TO FULL ADMIN ACCESS
- Markdown injection
- Bookmarklet to remove all disabled properties on a webpage
- Apache Airflow auth bypass
- Front end disabled? Add it in anyway!

- HTB University CTF 2022—Cloud—Enchanted
- TryHackMe writeup: Bounty Hacker

- Supply Chain Attacks on the risk – Open Source Security
- My first experience in hosting a National Level Capture The Flag Competition
- The Difficulties That Bug Bounty Hunters Face
- One Million Vulnerabilities Have Been Resolved on Open Bug Bounty
- Orange Tsai and team wins pwn2own