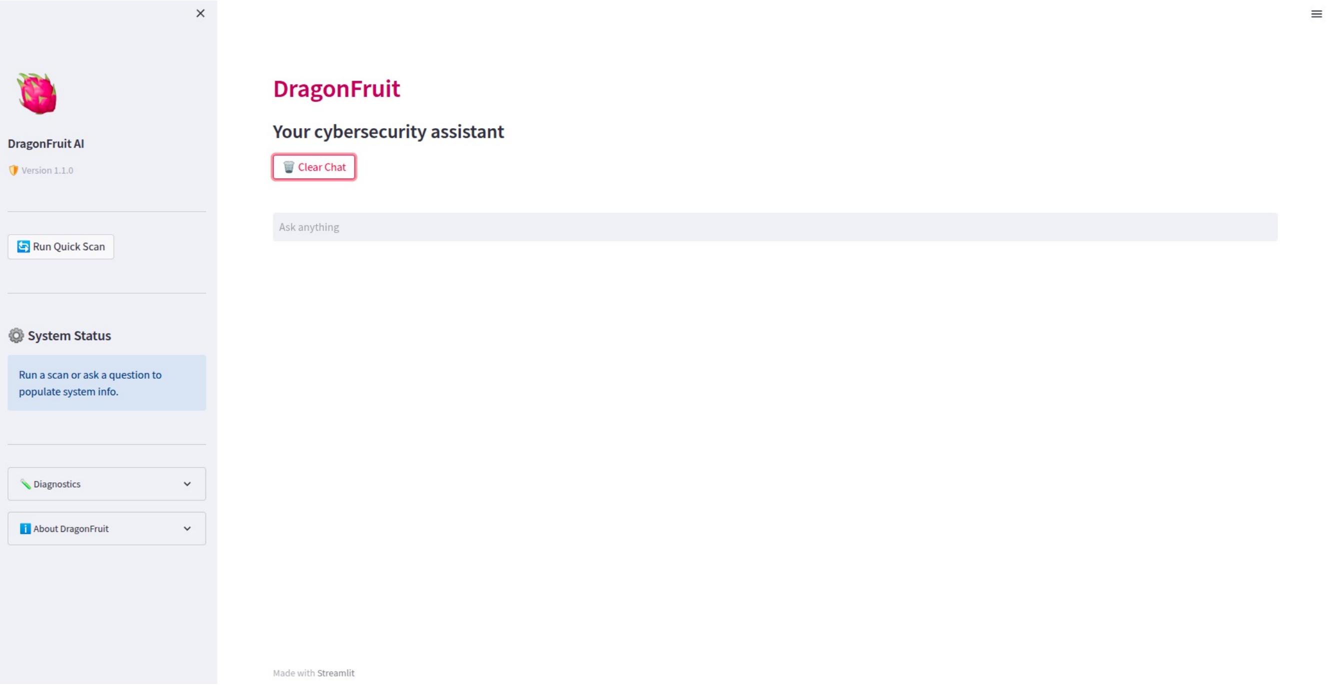
Application: DragonFruit

An Intelligent Cybersecurity Assistant

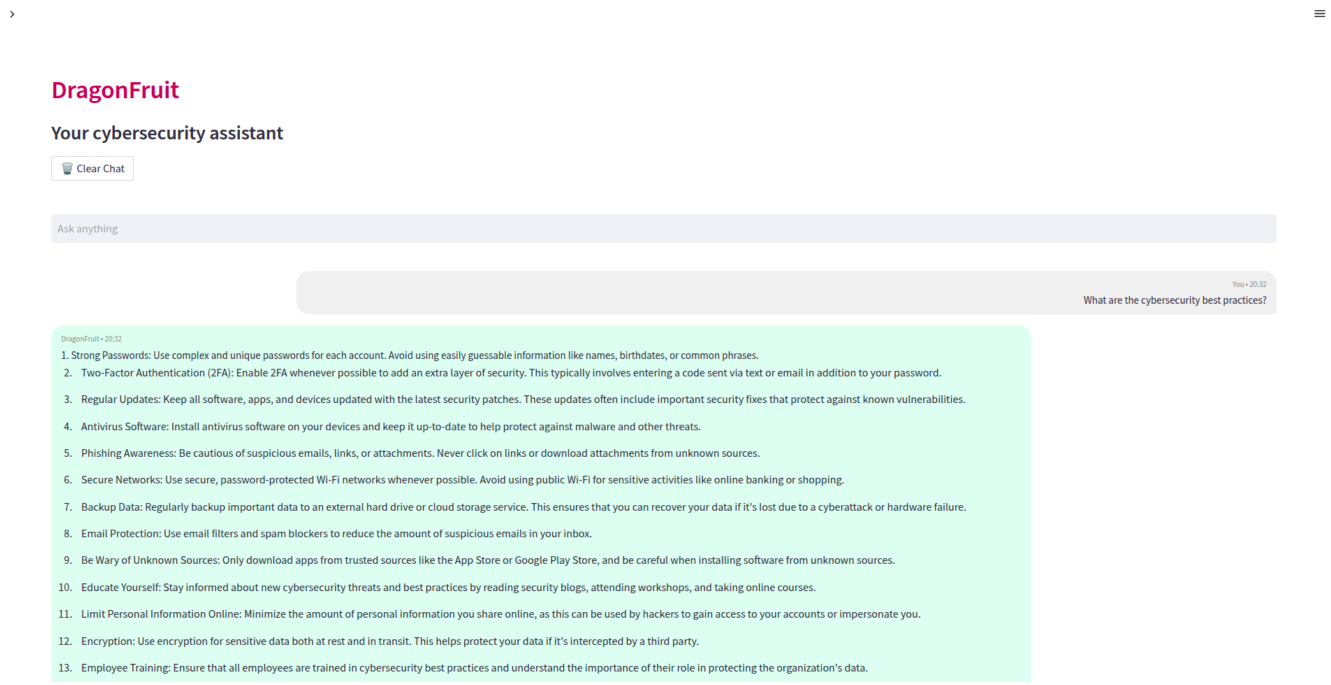
Use Cases

Use Case: UI Preview



Run a scan or ask a question to populate system info.

Use Case: AI response to a user query



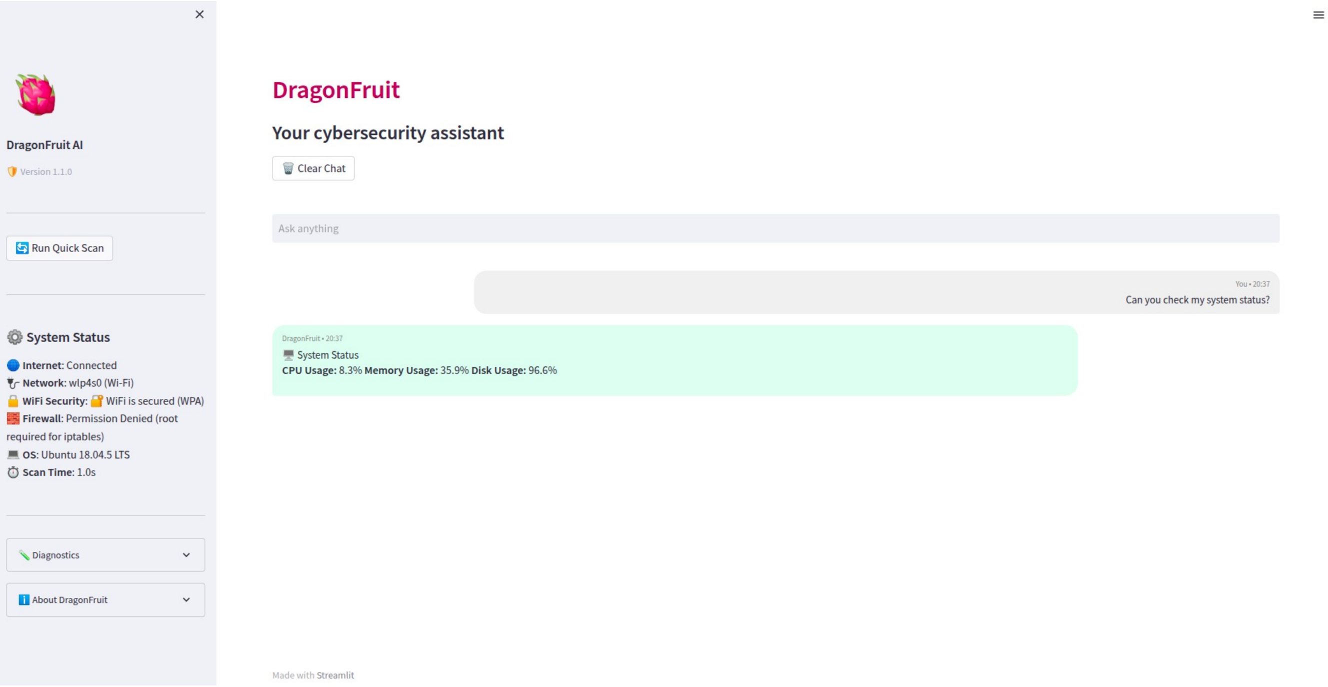
You • 20:32

What are the cybersecurity best practices?

DragonFruit • 20:32

1. Strong Passwords: Use complex and unique passwords for each account. Avoid using easily guessable information like names, birthdates, or common phrases.
2. Two-Factor Authentication (2FA): Enable 2FA whenever possible to add an extra layer of security. This typically involves entering a code sent via text or email in addition to your password.
3. Regular Updates: Keep all software, apps, and devices updated with the latest security patches. These updates often include important security fixes that protect against known vulnerabilities.
4. Antivirus Software: Install antivirus software on your devices and keep it up-to-date to help protect against malware and other threats.
5. Phishing Awareness: Be cautious of suspicious emails, links, or attachments. Never click on links or download attachments from unknown sources.
6. Secure Networks: Use secure, password-protected Wi-Fi networks whenever possible. Avoid using public Wi-Fi for sensitive activities like online banking or shopping.
7. Backup Data: Regularly backup important data to an external hard drive or cloud storage service. This ensures that you can recover your data if it's lost due to a cyberattack or hardware failure.
8. Email Protection: Use email filters and spam blockers to reduce the amount of suspicious emails in your inbox.
9. Be Wary of Unknown Sources: Only download apps from trusted sources like the App Store or Google Play Store, and be careful when installing software from unknown sources.
10. Educate Yourself: Stay informed about new cybersecurity threats and best practices by reading security blogs, attending workshops, and taking online courses.
11. Limit Personal Information Online: Minimize the amount of personal information you share online, as this can be used by hackers to gain access to your accounts or impersonate you.
12. Encryption: Use encryption for sensitive data both at rest and in transit. This helps protect your data if it's intercepted by a third party.
13. Employee Training: Ensure that all employees are trained in cybersecurity best practices and understand the importance of their role in protecting the organization's data.

Use Case: Rule based response as detected by NLP



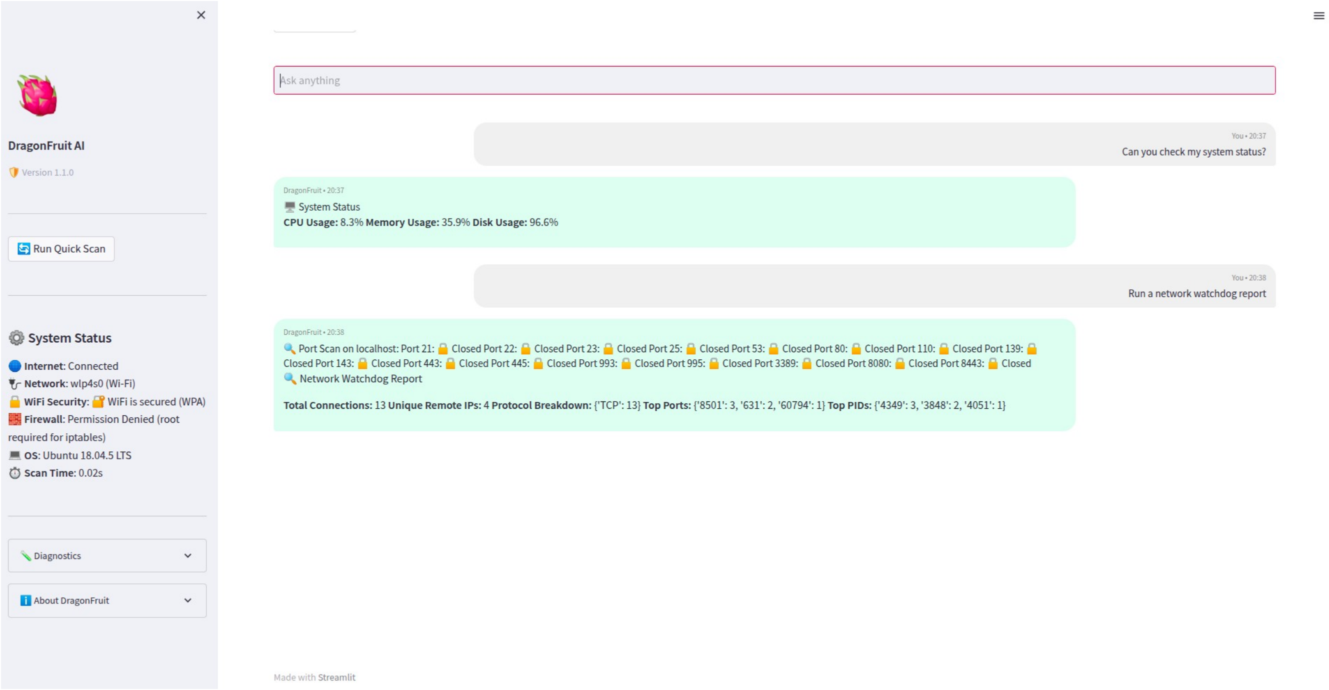
⚙️ System Status

🔵 **Internet:** Connected
🔌 **Network:** wlp4s0 (Wi-Fi)
🔒 **WiFi Security:** 🔐 WiFi is secured (WPA)
🧱 **Firewall:** Permission Denied (root required for iptables)
💻 **OS:** Ubuntu 18.04.5 LTS
⏱️ **Scan Time:** 1.0s

You • 20:37
Can you check my system status?

DragonFruit • 20:37
🖥️ System Status
CPU Usage: 8.3% **Memory Usage:** 35.9% **Disk Usage:** 96.6%

Use Case: Provides network watchdog report upon query



⚙️ System Status

🔵 **Internet:** Connected
🔌 **Network:** wlp4s0 (Wi-Fi)
🔒 **WiFi Security:** 🔐 WiFi is secured (WPA)
🧱 **Firewall:** Permission Denied (root required for iptables)
💻 **OS:** Ubuntu 18.04.5 LTS
⏱️ **Scan Time:** 0.02s

You • 20:37
Can you check my system status?

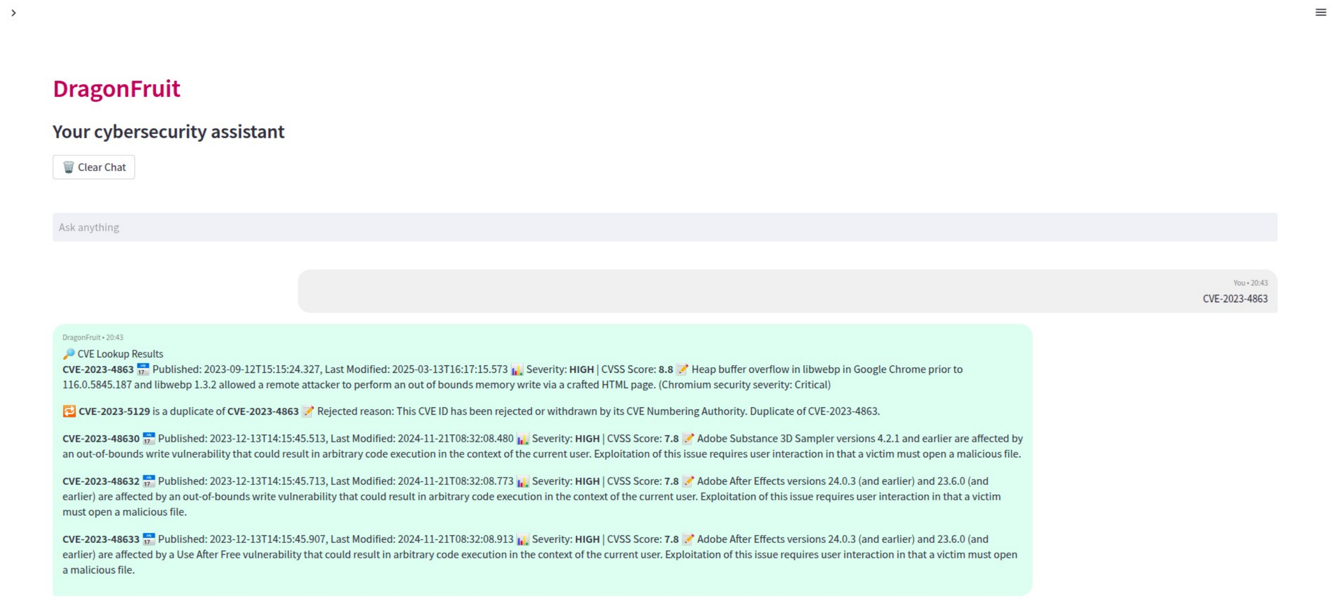
DragonFruit • 20:37
🖥️ System Status
CPU Usage: 8.3% **Memory Usage:** 35.9% **Disk Usage:** 96.6%

You • 20:38
Run a network watchdog report

DragonFruit • 20:38
🔍 Port Scan on localhost: Port 21: 🔒 Closed Port 22: 🔒 Closed Port 23: 🔒 Closed Port 25: 🔒 Closed Port 53: 🔒 Closed Port 80: 🔒 Closed Port 110: 🔒 Closed Port 139: 🔒 Closed Port 143: 🔒 Closed Port 443: 🔒 Closed Port 445: 🔒 Closed Port 993: 🔒 Closed Port 995: 🔒 Closed Port 3389: 🔒 Closed Port 8080: 🔒 Closed Port 8443: 🔒 Closed
🔍 Network Watchdog Report

Total Connections: 13 **Unique Remote IPs:** 4 **Protocol Breakdown:** {'TCP': 13} **Top Ports:** {'8501': 3, '631': 2, '60794': 1} **Top PIDs:** {'4349': 3, '3848': 2, '4051': 1}

Use Case: Performs CVE lookup by CVE ID



You • 20:43
CVE-2023-4863

DragonFruit • 20:43
🔎 CVE Lookup Results
CVE-2023-4863 📅 Published: 2023-09-12T15:15:24.327, Last Modified: 2025-03-13T16:17:15.573 📊 Severity: **HIGH** | CVSS Score: **8.8** 📝 Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

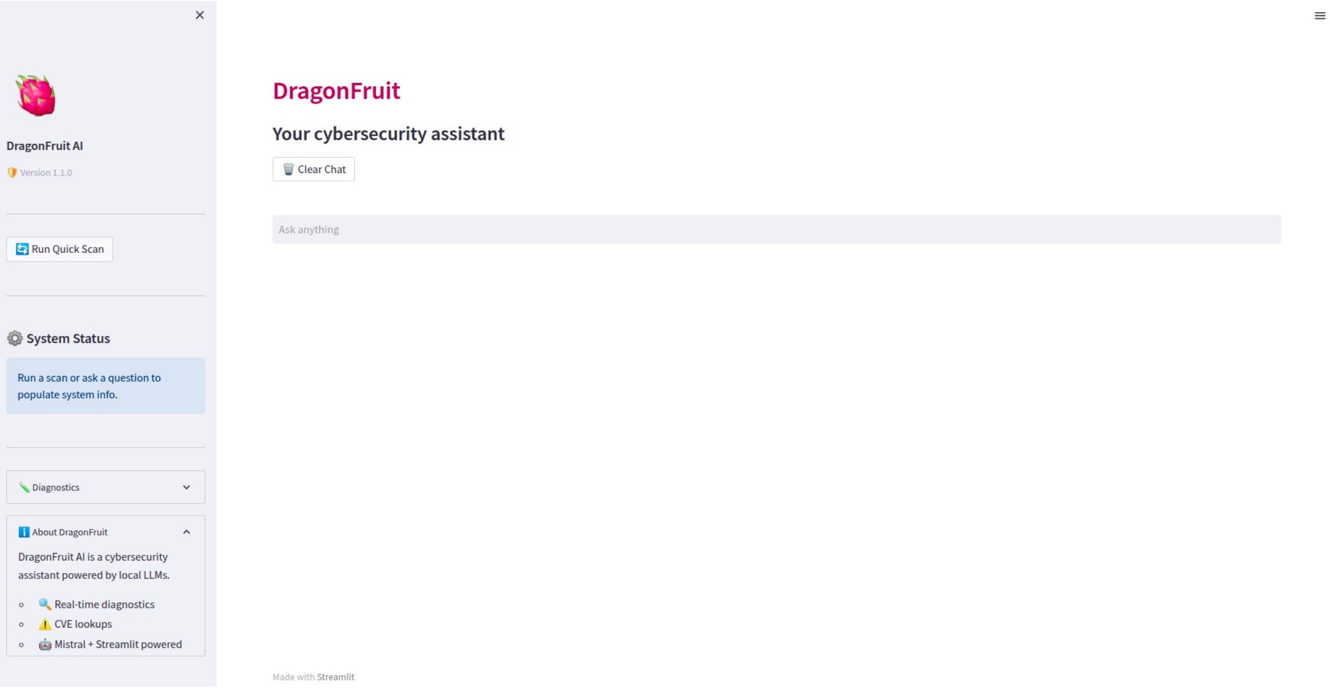
🔁 **CVE-2023-5129** is a duplicate of **CVE-2023-4863** 📝 Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. Duplicate of CVE-2023-4863.

CVE-2023-48630 📅 Published: 2023-12-13T14:15:45.513, Last Modified: 2024-11-21T08:32:08.480 📊 Severity: **HIGH** | CVSS Score: **7.8** 📝 Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE-2023-48632 📅 Published: 2023-12-13T14:15:45.713, Last Modified: 2024-11-21T08:32:08.773 📊 Severity: **HIGH** | CVSS Score: **7.8** 📝 Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE-2023-48633 📅 Published: 2023-12-13T14:15:45.907, Last Modified: 2024-11-21T08:32:08.913 📊 Severity: **HIGH** | CVSS Score: **7.8** 📝 Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

Use Case: About section



DragonFruit

Your cybersecurity assistant

Run a scan or ask a question to populate system info.

DragonFruit AI is a cybersecurity assistant powered by local LLMs.

- 🔍 Real-time diagnostics
- ⚠️ CVE lookups
- 🤖 Mistral + Streamlit powered