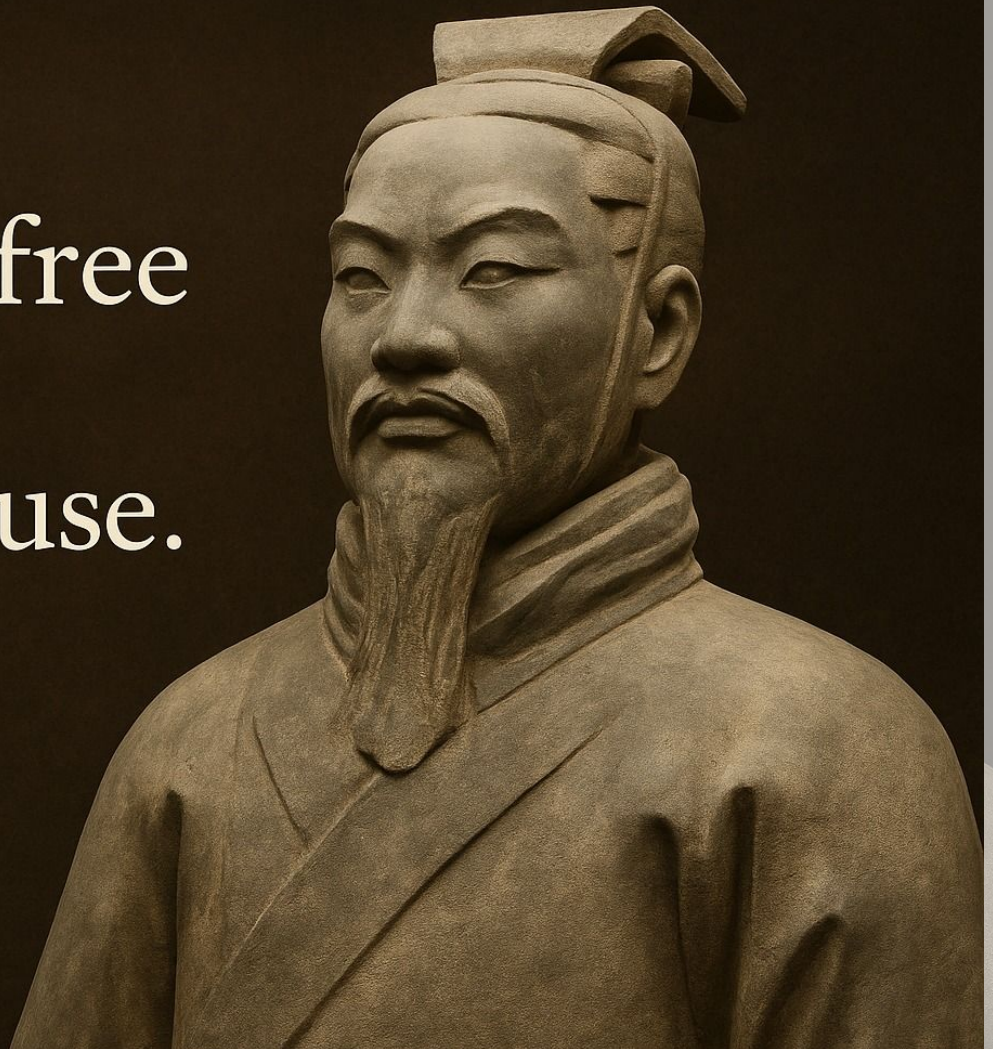
“

If there’s free compute, there’s abuse.

— Sun Tzu,
The Art of War
(500 BC)

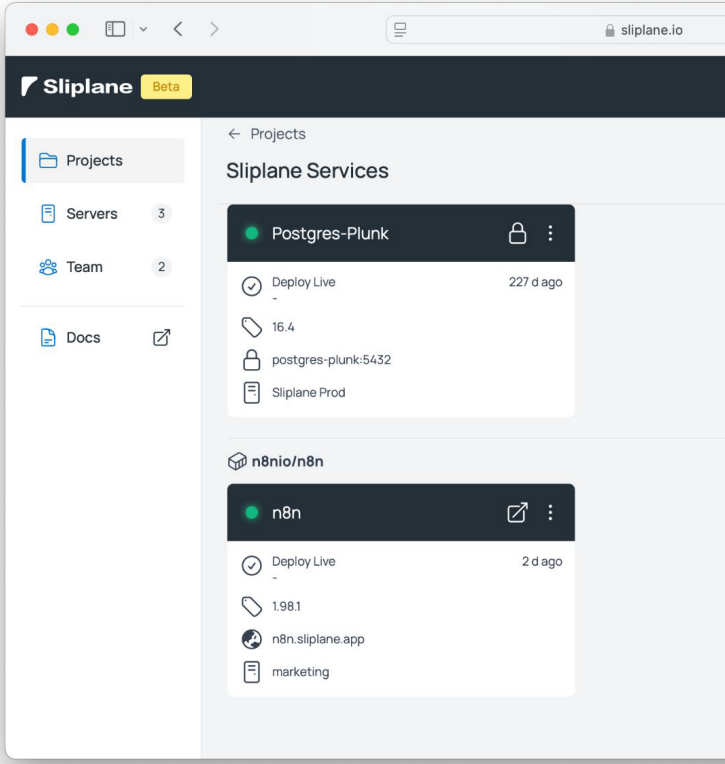


Background

Co-Founder @ sliplane.io

🇪🇺 Managed Container Hosting / PaaS

Connect Github Repository → We build and deploy your app to our infra



The Problem

Easy To Use Platform + Free Trial => ABUSE

40 Abuse Cases in May

Typical Abuse Scenarios

Crypto Mining

DDoS

Netscans

Illegal VPN

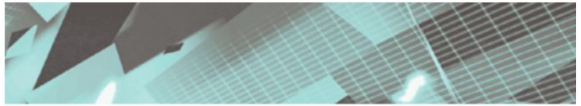
=> Easy to catch at runtime

Phishing

Spambots

file:///Users/jonasscholz/Development/ai-hackathon/data/phishing/afd

ARMED FORCES DEVISION MAILING SYSTEM



Name:

Password:

Sign In

mail.afd.gov.bd

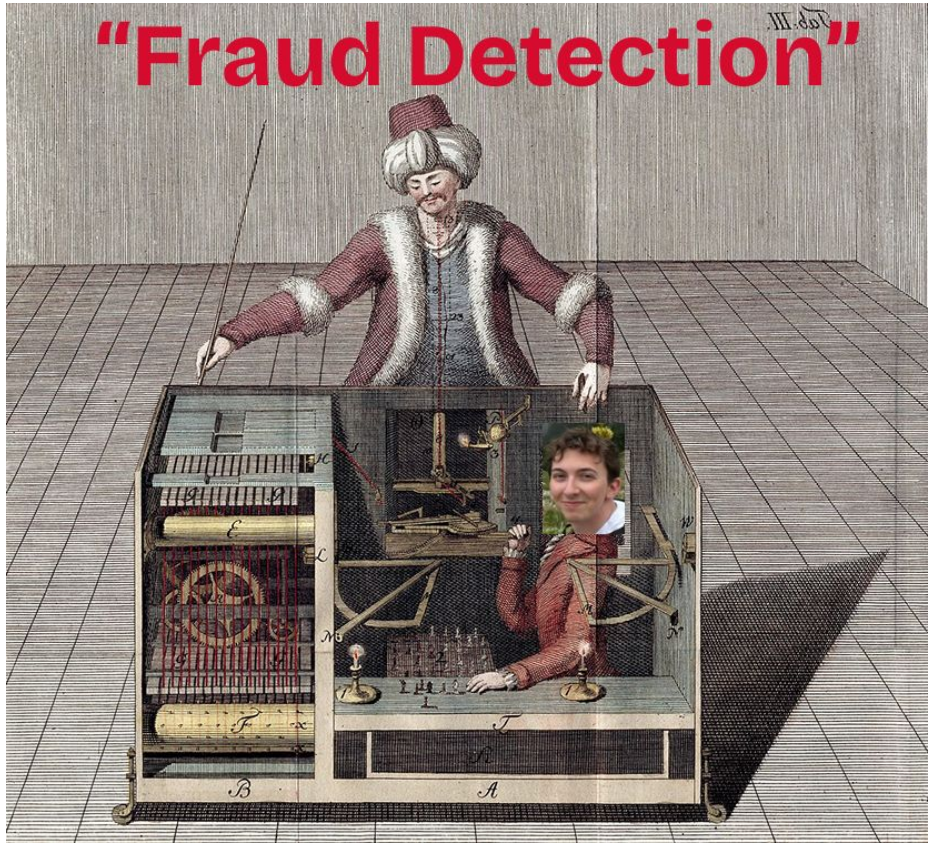
ARMED FORCES DIVISION
MAILING SYSTEM

Name:

Password:

Sign In

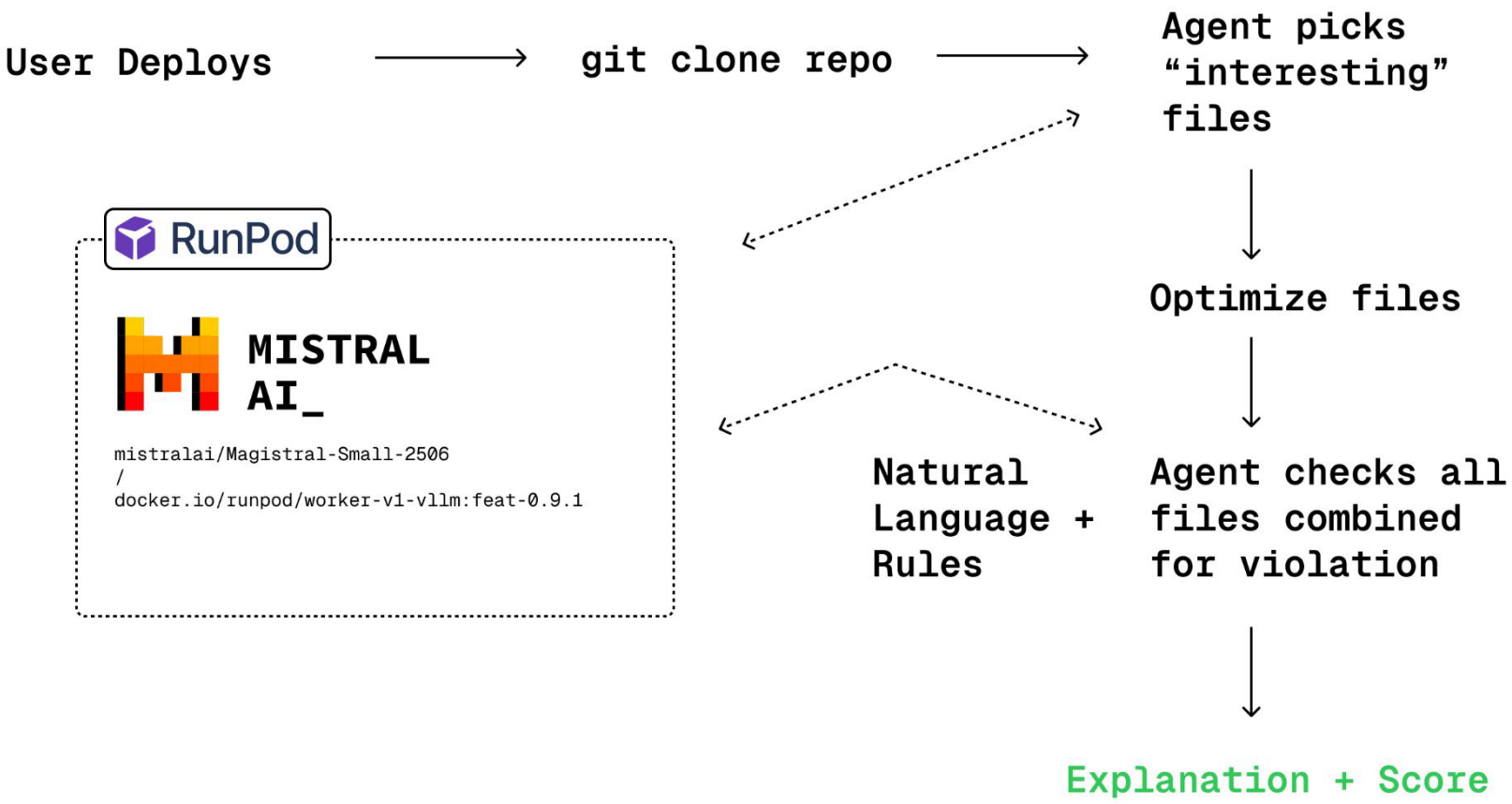
Current Solution



22:48 APP Captain Hook [SIGNUP 🚀] User 2001:f 8:5a99 has signed up

APP Captain Hook [ONBOARDING ✅] User (user_ic66wb0iemy6) completed onboarding

The New Solution


User Deploys
git clone repo
Agent picks "interesting" files
Optimize files
Agent checks all files combined for violation
Explanation + Score
Natural Language + Rules
RunPod
MISTRAL AI_
mistralai/Magistral-Small-2506
/
docker.io/runpod/worker-v1-vllm:feat-0.9.1

Problems 1K+ Terminal

zsh

```
├── server.js
├── Dockerfile
├── db.js
├── public
│   ├── index.html
│   ├── OM to coast guard.pdf
│   ├── login.html
│   ├── 3RD CISM WORLD MILITARY ARCHERY CHAMPIONSHIP BANGLADESH-2024 বাংলাদেশ পুরস্কার.pdf
│   ├── Invitation to Attend Red Flag ALASKA Executive Observer Pgme in USA.pdf
│   ├── files
│   │   ├── js.js
│   │   ├── favicon.jpeg
│   │   ├── customWMLoginImg5
│   │   ├── customWMLoginImg2
│   │   ├── 1495.gif
│   │   ├── styles.ce29b658bf35a0a571c5.css
│   │   └── img_avatar2.png
│   └── error.html
├── .gitignore
├── package-lock.json
├── package.json
├── views
│   ├── index.ejs
│   ├── error.ejs
│   ├── upload.ejs
│   ├── url.ejs
│   └── table.ejs
└── routes
    ├── index.js
    └── backend.js

Agent picked server.js
Added and optimized file
Agent picked db.js
Added and optimized file
Agent picked routes/index.js
Added and optimized file
Agent picked routes/backend.js
Added and optimized file
Agent picked public/login.html
Added and optimized file
Agent picked public/error.html
Added and optimized file
Agent picked views/index.ejs
Added and optimized file
Agent picked views/error.ejs
Added and optimized file
Agent picked public/files/js.js
Added and optimized file
--------------------------------
phishing afd
Raise a red flag for a codebase that is likely breaching your terms of service. The application appears to be a credentials harvester designed to phish sensitive login information from users, based on the follow
ing indicators:
 1. The form listed in `public/login.html` is designed to mimic a legitimate login page, as evidenced by the base64 encoded parameter and the HTML code. The page extract credentials and redirect the user to anot
her page or send them to a malicious server.
 2. There have Article successful form submissions to the `/submit` endpoint that likely save the credentials to the "usertable" according to the `index.js`, i.e. a potential exfiltration of sensitive data.
 3. The JavaScript in `public/files/js.js`, maintains more obfuscation and encoding functions (opaque functions) that seem to be designed to hide the data before sending it elsewhere.
 4. The application contains port scanning of a system (not in codebase but part of the hosting platform on which it runs) and other suspicious activities that a legitimate application wouldn't need. 5. The appl
ication is not something that the company should host as it may result in legal trouble. The combination of the harvesting nature of the site, the obfuscation methods used to hide its purpose, and the lack of a
legitimate use case indicate that this is a credentials harvesting tool for phishing. Given these indicators, this application should not be allowed to run on this platform, as it violates the terms of service r
egarding illegal activities such as phishing and is using the platform to harvest sensitive data and send to a questionable source without the knowledge or consent of the users.
--------------------------------
jonasscholz@Jonass-MacBook-Pro-2 ai-hackathon %
```

⌘K to generate a command