AI Security Intern - Offensive Security

Location: Bangalore, India

Company: CyberWarFare Labs

About Us:

CyberWarFare Labs is an Ed-Tech Cyber Security Focused Platform which is totally engrossed in solving the problem of Cybersecurity by providing real-time hands-on manner solutions to problems of B2C & B2B Audience.

Job Overview:

We are looking for a Security Intern to assist with cybersecurity research, offensive security testing, and AI security assessments. The role involves analyzing emerging threats, simulating attacks, and performing LLM red teaming, RAG security testing, and prompt injection/adversarial AI research in controlled lab environments.

Qualifications:

- Pursuing or recently completed B.S / B.E / B.Tech / BCA / M.Tech / MCA in Computer Science or related field.
- Hands-on exposure to Offensive Security (OS, Network, Web App, or Cloud Security).
- Programming knowledge in Python, Bash, C, or C++.
- Understanding of security principles and OS internals (Windows/Linux).
- Strong analytical and problem-solving skills.

Responsibilities:

- Conduct research in Offensive Security and AI Security.
- Simulate attacks and replicate TTPs in lab environments.
- Perform LLM red teaming, RAG testing, and prompt injection analysis.
- Build scripts/tools to simulate threat actor techniques.
- Document methodologies, findings, and research outcomes.
- Support red team operations and exploit research activities.

AI Security Intern - Offensive Security

Bonus: Personal blog, home lab setup, open-source contributions, or exposure to AI/LLM security.

Internship time period - 3 - 6 months
Internship type - Paid

After internship , Full time position will be offered based on performance