UNIVERSITY OF BAHRAIN
COLLEGE OF INFORMATION TECHNOLOGY
CYBERSECURITY SENIOR PROJECTS

Secure Natural Language to Bash Execution - ShellSentry

Aljazi Ali Almujaddam – 202202227 | Dana Hussain Alhayki – 20223431

Supervised By : Dr. Abdulla Khalifa Aldoseri

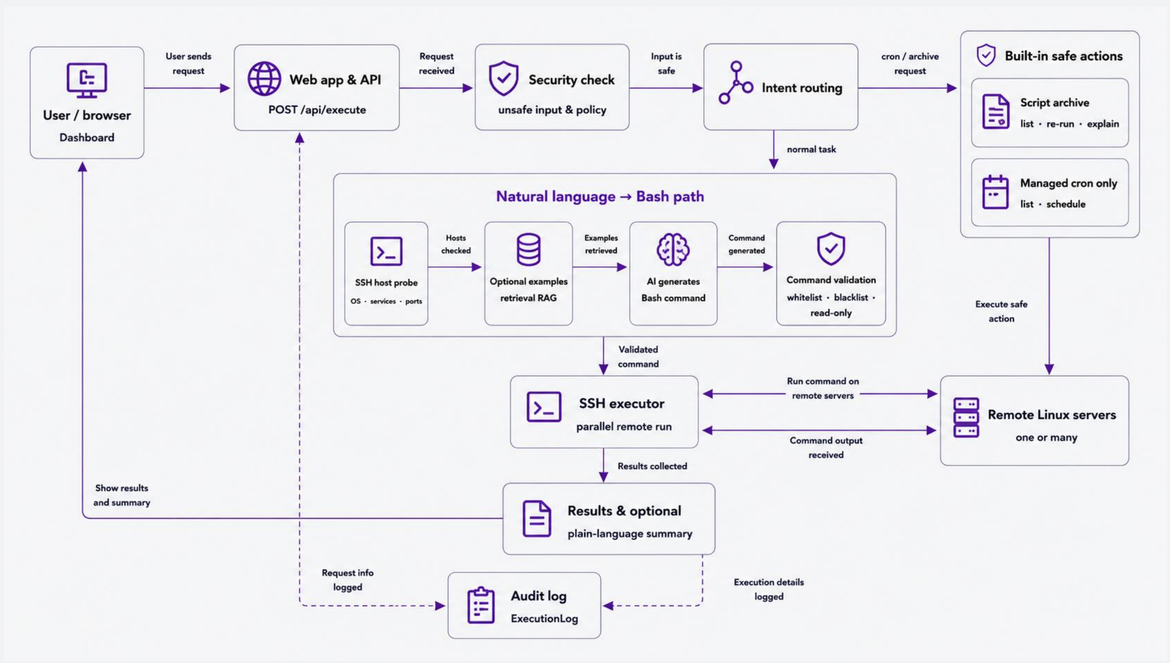
ABSTRACT

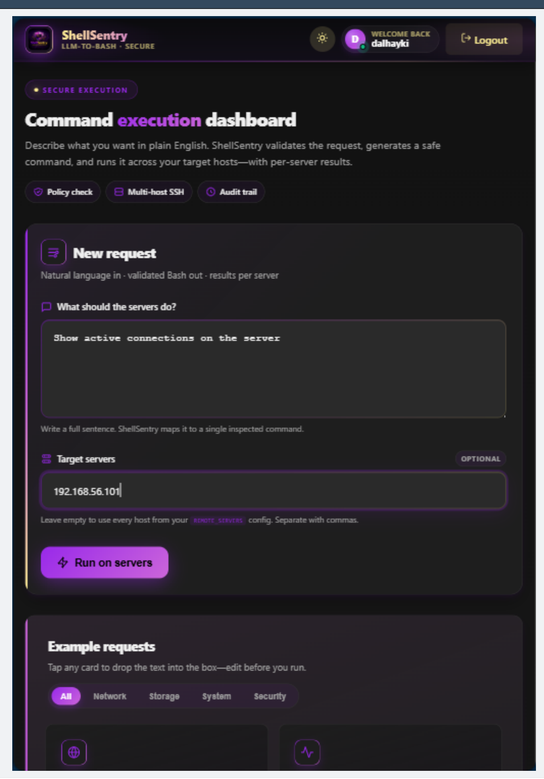
A secure, web-based prototype that takes admin requests in natural language to a validated bash command to execute on a remote Linux system. The project tackles the challenges of manual shell management and the execution of commands generated by AI, using a combination of authenticated access, retrieval-augmented generation (RAG), host-aware context collection, deterministic command validation, and SSH-based multi-server orchestration. Flask, Python, Paramiko, FAISS, and an OpenAI-compatible Large Language Model were used to implement the system. Functional, security, and performance testing are done in a controlled environment in the virtual lab. The results demonstrated successful authentication of execution, multi-host command orchestration, blocking of unsafe commands, and structured audit logging with a reliable report. ShellSentry showcases how AI-driven shell automation can become much more secure by implementing multiple-level validation, execution policies, and accountability.

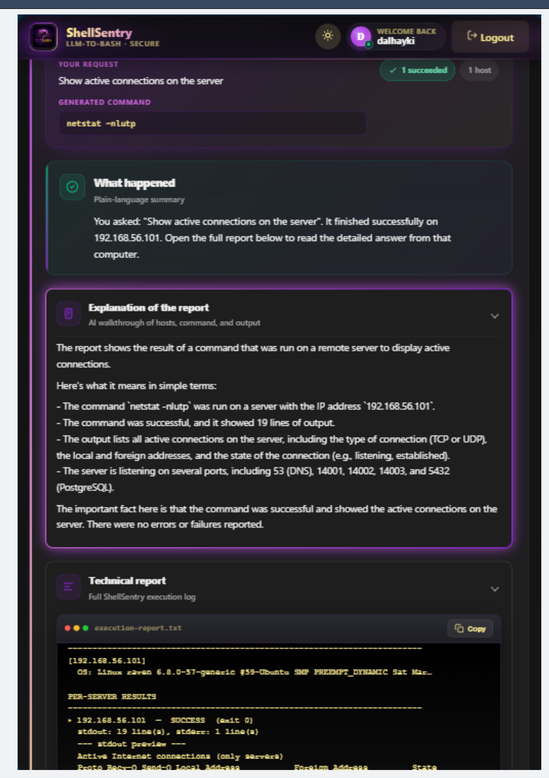
OBJECTIVES

- Develop a secure web-based system that converts natural-language requests into Bash commands.
- Enable authenticated remote execution across multiple Linux servers via SSH.
- Reduce unsafe AI-generated command risks through deterministic validation and security controls.
- Improve command accuracy using host-aware context and retrieval-augmented generation (RAG).
- Provide audit logging, script management, and explainable execution reporting.

METHODS/DIAGRAMS/FIGURES

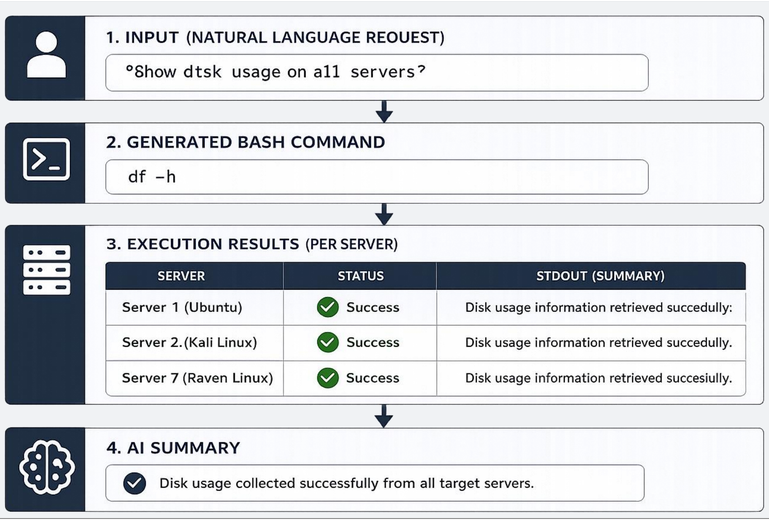






RESULTS

REAL RESULT WORKFLOW



CONCLUSION & FUTURE WORK

- **Conclusion**

Secure AI-assisted Linux administration prototype
Natural language to validate Bash execution
Multi-server SSH orchestration with audit logging.
Successfully blocked unsafe commands through layered security

- **Future Work**

Role-based access control (RBAC)
Human approval for sensitive commands
SIEM-integrated immutable audit logging
Production-ready deployment enhancements