Project Title: BreachAware-LAW – A Legal Response Toolkit for Cybersecurity Breaches

# Abstract:

In the current digital era, organizations face increasing cyber threats such as ransomware, unauthorized access, and data leaks. However, the majority of cybersecurity response tools focus only on detection and recovery, often ignoring the legal obligations companies must fulfill post-breach.  
  
BreachAware-LAW is a Python-based, open-source toolkit built on Kali Linux that helps cybersecurity teams quickly map detected breaches to relevant legal and regulatory compliance obligations. The toolkit analyzes simulated or real breach logs, identifies the breach type, and provides a structured legal response plan by referring to laws such as the IT Act 2000, CERT-In 2022 Guidelines, GDPR, HIPAA, and India’s DPDP Act 2023.  
  
Additionally, it generates a PDF-based legal breach report that outlines the type of incident, affected data categories (PII, PHI, etc.), and the corresponding laws and required actions. This project bridges the gap between cyber incident response and legal compliance, which is crucial in today's regulatory-driven world.

# Key Features:

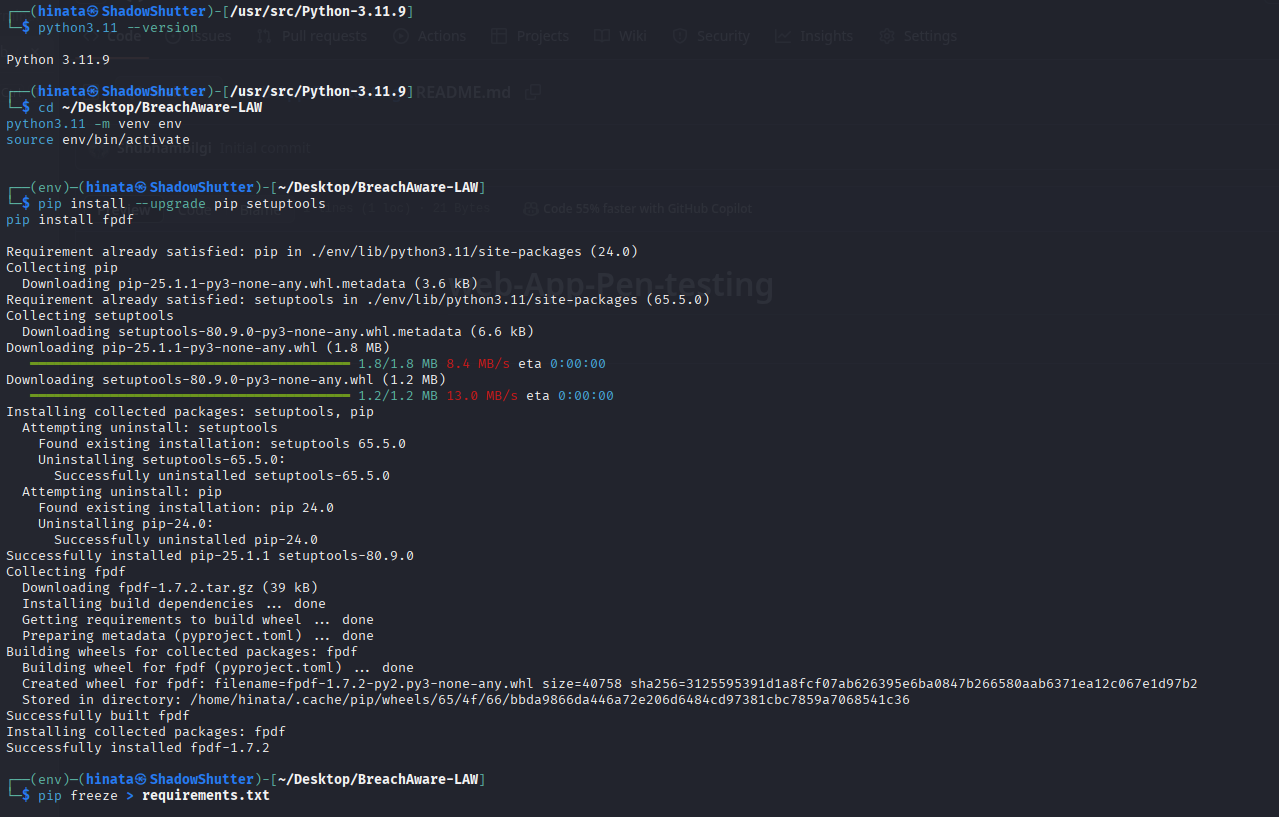
- Log-based breach identification  
- JSON-based legal rule mapping  
- PDF compliance report generation  
- Works completely offline on Kali Linux

# Keywords:

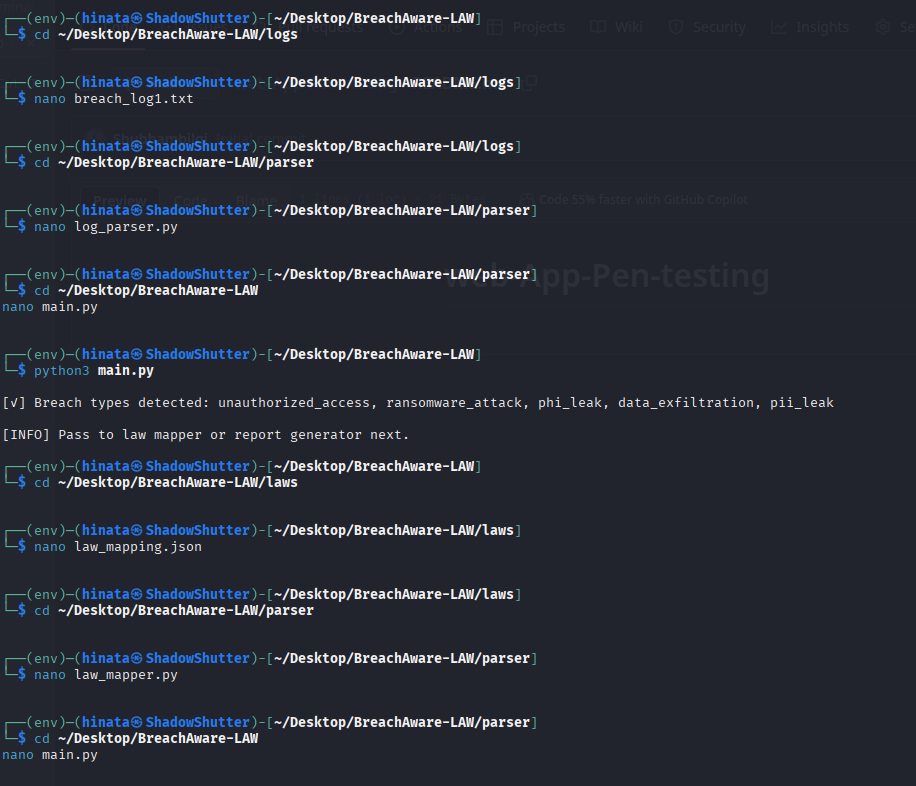
Cybersecurity, Legal Tech, Data Breach, GDPR, IT Act, CERT-In, Compliance Automation, Kali Linux

# Implementation Flow

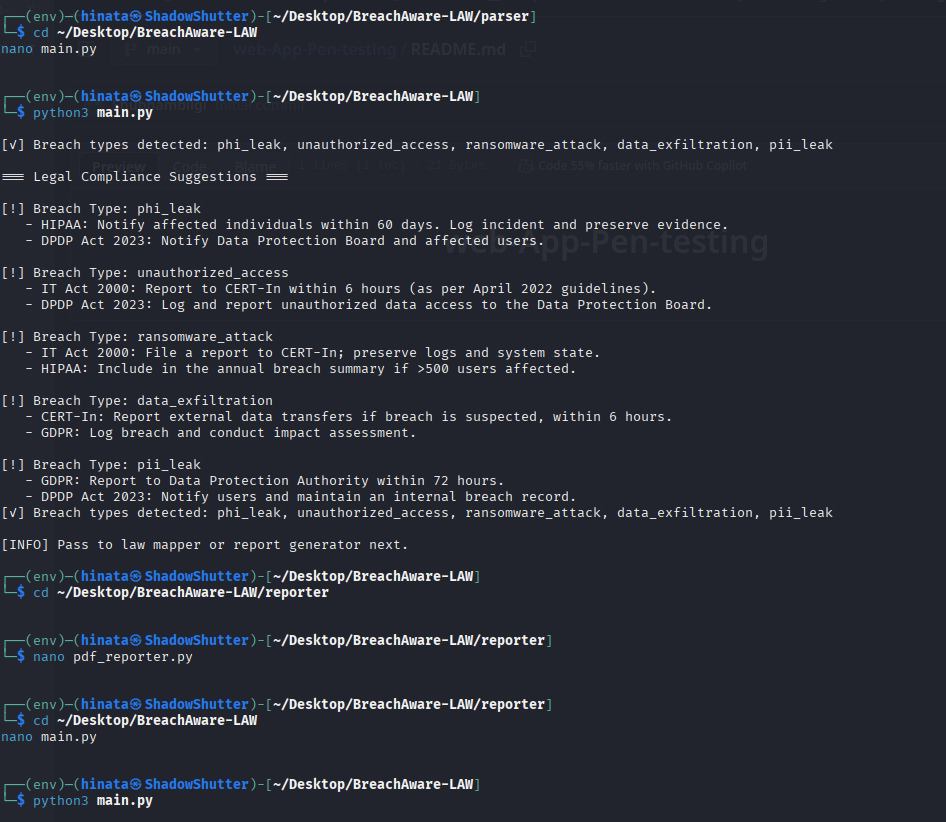
## Step 1: Parse Logs



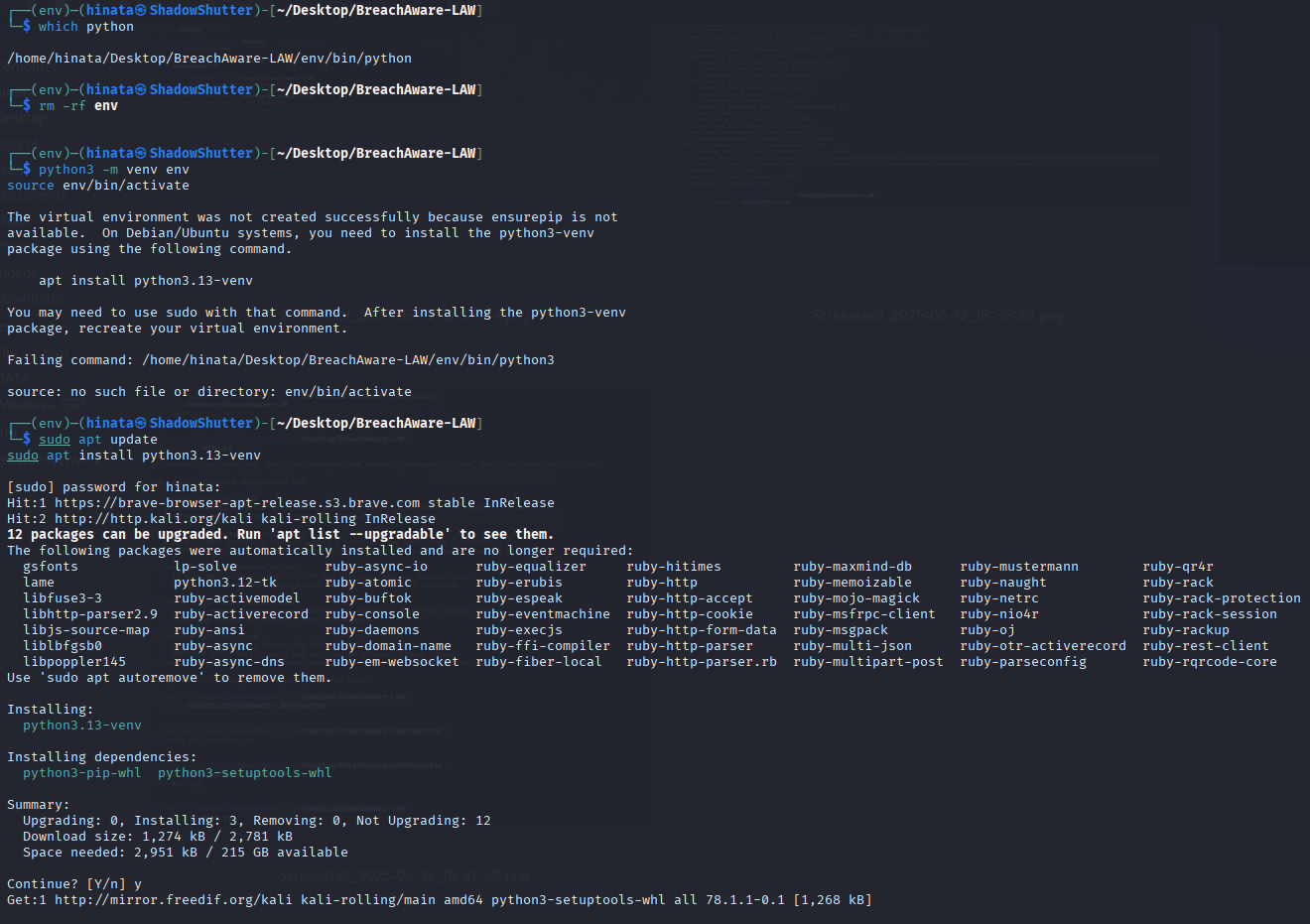
## Step 2: Legal Mapping



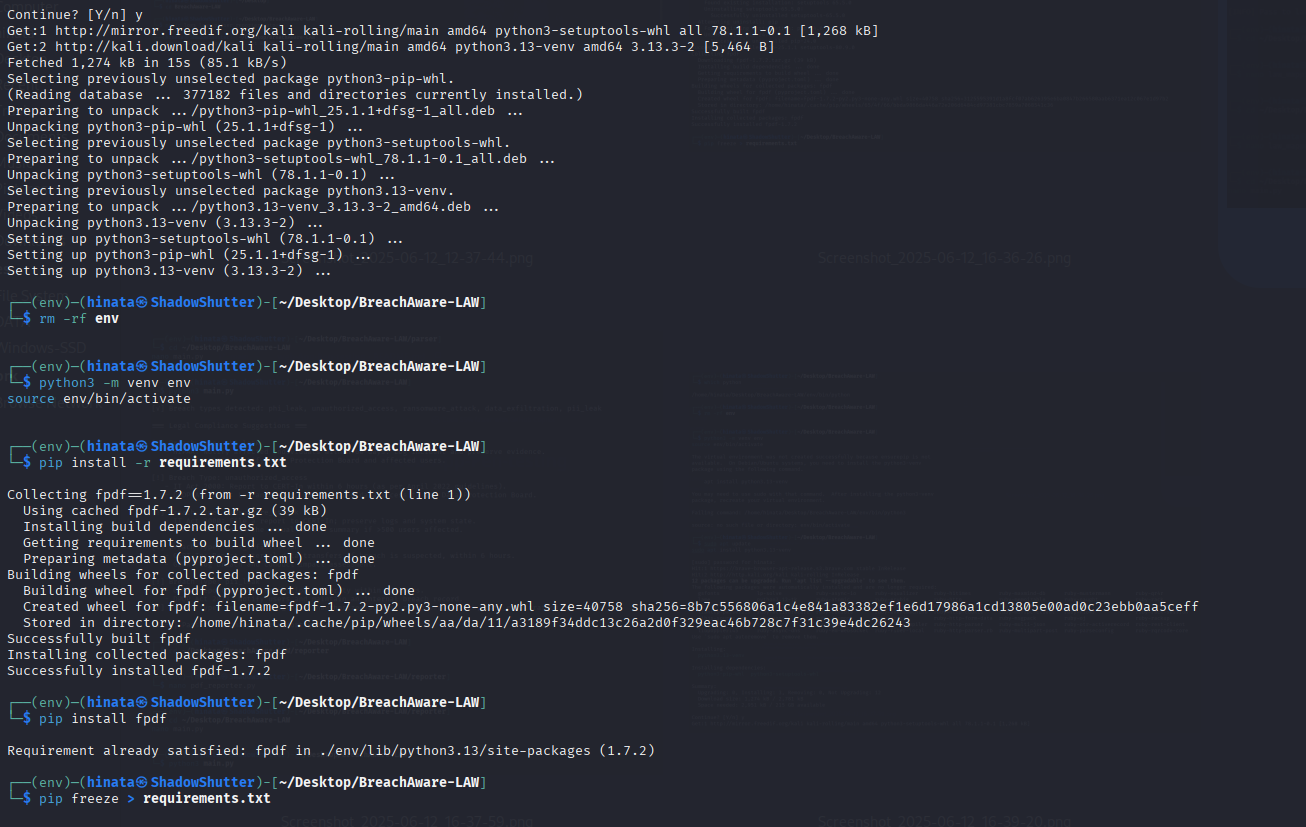
## Step 3: Report Generation



## PDF Output Preview



## Re-run and Final Compliance Suggestion



# Challenges Faced:

- Dependency issues with Python virtual environment on Kali Linux.  
- Required installing missing components like python3.13-venv manually.  
- Network errors while fetching packages from Kali repositories.

# Conclusion:

BreachAware-LAW effectively integrates breach detection with automated legal mapping and compliance reporting. It is especially useful for cybersecurity professionals and legal compliance teams working in data protection environments. The project highlights the importance of not only addressing technical vulnerabilities but also fulfilling mandatory legal requirements.