EELU

الجامعة المصرية للتعلم الإلكتروني الأهلية

THE EGYPTIAN E-LEARNING UNIVERSITY

Vulnerability Scanner with AI

Supervised By:

Dr. Mohammed Zidan

Eng: Toka Ashraf

Faculty of Computers and information Technology

- **Project BY:**

- ❑ Eslam Mohammed Moawed Elabd
- ❑ Abdelrahman Ail Abdelhafeez Abdulbari
- ❑ Nourhan Mohammed Shaban Mohammed
- ❑ Alaa Elsayed Saber Eissa
- ❑ Walaa Ahmed Korani Mohamed
- ❑ Mohamed Yasser Hussein Abdelhamid
- ❑ Walaa Mostafa Ahmed Abdelaziz
- ❑ Mohamed Ahmed Ali

Introduction

Overview

Vulnerability scanners are essential cybersecurity tools that systematically identify and prioritize security weaknesses within digital systems, helping organizations proactively mitigate risks and enhance overall security posture.

Purpose

The vulnerability scanner app serves to actively seek out and assess security vulnerabilities within digital systems, with the overarching goal of fortifying defenses and preempting potential cyber threats. Through systematic identification and prioritization of risks, it aims to bolster security posture, ensuring compliance and safeguarding sensitive data from exploitation.

Problem Statement:

1. Cybersecurity challenges persist due to unpatched vulnerabilities.
2. Limited availability of unexpensive and accessible security tools.
3. Existing tools primarily focus on web scanners
4. Businesses and users face risks of website compromise and data theft.
5. Executable file malware remains a significant concern for antivirus solutions, leaving systems vulnerable to attacks.

Solution :

We Developed a tool (Unixty Vulnerability Scanner) it allow any user to

Website before use it and put his sensitive data in it .

The tool also has a Network scanner the user can scan any router or switch .

And an Antivirus based on Ai can detect the files.

The tool improve with a friendly User interface to make it easy to use By all users .

incorporating cybersecurity into software development processes

Related Work :

1. **Nessus**

A widely-used vulnerability scanner that can identify vulnerabilities, misconfigurations, and compliance issues in networks and web applications

2. **Acunetix**

A web vulnerability scanner designed to automatically identify security flaws in web application ,including SQL injection and XSS

3. **OWASP ZAP**

An open-source Security tool for finding vulnerabilities in web application during The development and testing phases.

Technical Architecture

System Components

1 Scanner Engines

- Web Scanner Engine
- Network Scanner Engine
- File Scanner Engine

2 Database

- Stores and manages vulnerabilities detected online, enabling efficient analysis and informed security decision-making.

3 User Interface

- Features a responsive design optimized for online access, prioritizing usability and accessibility for seamless interaction.

4 Reporting and Alerts

- Generates real-time reports and alerts for online scan findings, empowering stakeholders with actionable insights for effective risk mitigation.

Streamlined Vulnerability Scanning Workflow: From Setup to Results

1-Setup:

- **Authorized User Access**
- **Target Identification**

2-Execution:

- **Scan Initiation**
- **Scan Progress**
- **Real-time Monitoring**

3-Results

- **Comprehensive Reports**
- **Visual Representation**

Vulnerability Scanner Life Cycle

Vulnerability Identification

the process of recognizing weaknesses in software, networks, or systems.

Reporting and Mitigation

the generation of reports and the subsequent steps for addressing and resolving vulnerabilities.

Risk Assessment

Assess potential impacts and possibilities associated with identified vulnerabilities

Key Features :

Web Scanning:
The app meticulously inspects web applications for vulnerabilities such as SQL injection and XSS, offering actionable insights for enhanced security.

Network Scanning:
 the app conducts thorough port scans and vulnerability assessments, fortifying network defenses against potential cyber threats.

File Scanning: (Antivirus)
Powered by innovative AI technology, the app rigorously analyzes uploaded files for malware and integrity issues

Antivirus Based on AI

Overview:

Our Antivirus is Designed to Improve the traditional methods of detecting the malwares using the Machine learning.

The model aims to identify and classify malicious files with high accuracy by using 5 Algorithms it choose the higher accuracy is the Winner.

it uses previously trained machine learning models to analyze and classify new files as malicious or legitimate based on the patterns and features it has learned from the training data.

File Upload and Classification

1

File Upload

Users can easily upload executable files(.exe) for analysis through a user-friendly interface.

2

Feature Extraction

The system extracts important features from the uploaded file.
Features include file metadata, entropy values, section characteristics, and resource information.

3

Model Prediction

Extracted features are fed into a pre-trained machine learning model.
The model evaluates the features to classify the file as malicious or legitimate.

4

Result Return

The system provides users with the classification results to enable timely threat detection and mitigation.

Dataset:
Description : -

The dataset provided is a comprehensive collection of executable files and their respective features, specifically designed to train and evaluate machine learning models for antivirus and malware detection. This dataset includes detailed attributes extracted from executable files, which are critical for distinguishing between legitimate software and potentially harmful malware.

	Name	md5	Machine	\
0	memtest.exe	631ea355665f28d4707448e442fbf5b8	332	
1	ose.exe	9d10f99a6712e28f8acd5641e3a7ea6b	332	
2	setup.exe	4d92f518527353c0db88a70fddcfd390	332	

	SizeOfOptionalHeader	Characteristics	MajorLinkerVersion	\
0	224	258	9	
1	224	3330	9	
2	224	3330	9	

	MinorLinkerVersion	SizeOfCode	SizeOfInitializedData	\
0	0	361984	115712	
1	0	130560	19968	
2	0	517120	621568	

	SizeOfUninitializedData	...	ResourcesNb	ResourcesMeanEntropy	\
0	0	...	4	3.262823	
1	0	...	2	4.250461	
2	0	...	11	4.426324	

	ResourcesMinEntropy	ResourcesMaxEntropy	ResourcesMeanSize	\
0	2.568844	3.537939	8797.000000	
1	3.420744	5.080177	837.000000	
2	2.846449	5.271813	31102.272727	

	ResourcesMinSize	ResourcesMaxSize	LoadConfigurationSize	\
0	216	18032	0	
1	518	1156	72	
2	104	270376	72	

	VersionInformationSize	legitimate
0	16	1
1	18	1
2	18	1

The Dataset: Why chosen it ?

Rich Feature Set	The dataset includes a wide variety of features extracted from executable files
Size	With over 138,000 samples, the dataset is large enough to train and validate complex models effectively.
Real-world Relevance:	The features are directly related to the structure and content of executable files, making the model's predictions highly relevant to real-world antivirus applications.

Algorithms:

- Decision Trees
- Random Forests
- Gradient Boosting
- Gaussian Naive Bayes
- AdaBoost

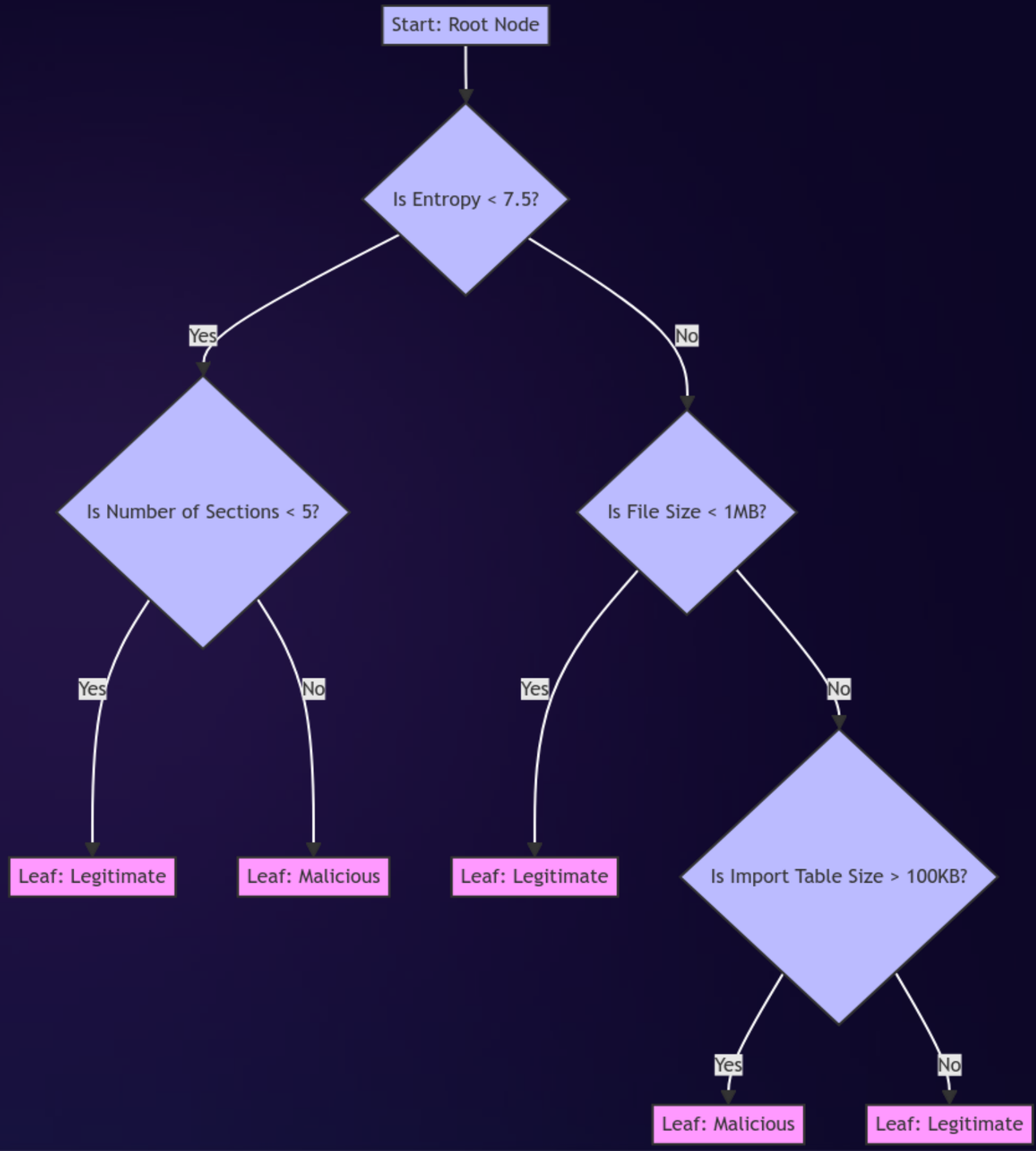
Decision tree Algorithm

lgorithm

Description:

Decision trees are a type of machine learning algorithm used for classification and regression tasks. They work by splitting the dataset into subsets based on feature values, creating a tree-like structure of decisions that lead to a final prediction.

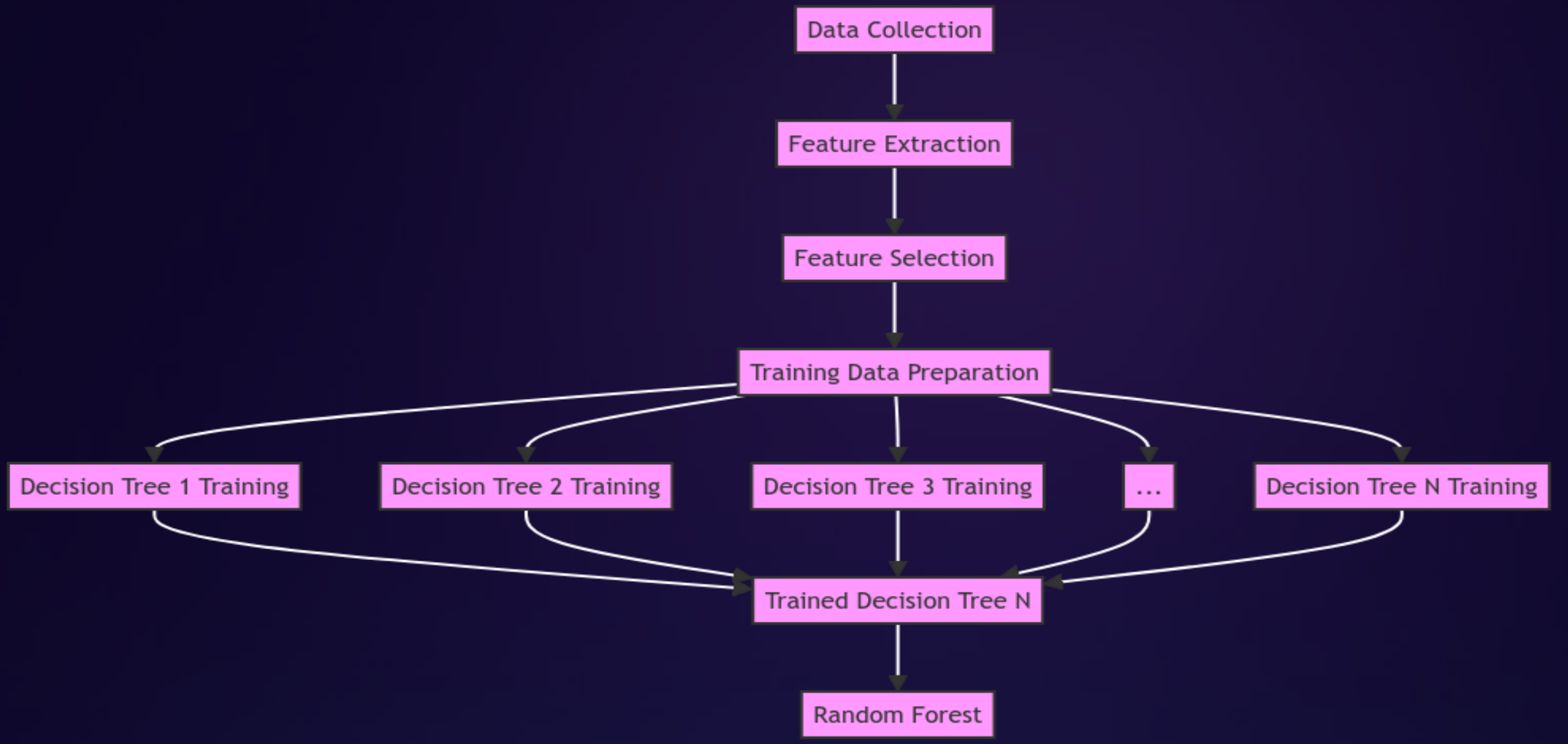
- How it work?
- Why we Choose it ?

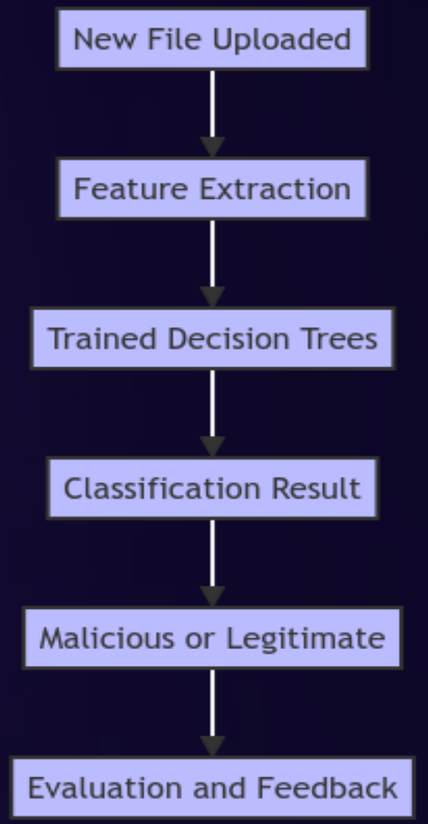


Random Forests:

Random Forests is a **supervised** learning algorithm.
It constructs multiple decision trees during training and outputs the mode of the classes for classification or the mean prediction for regression from all the individual trees

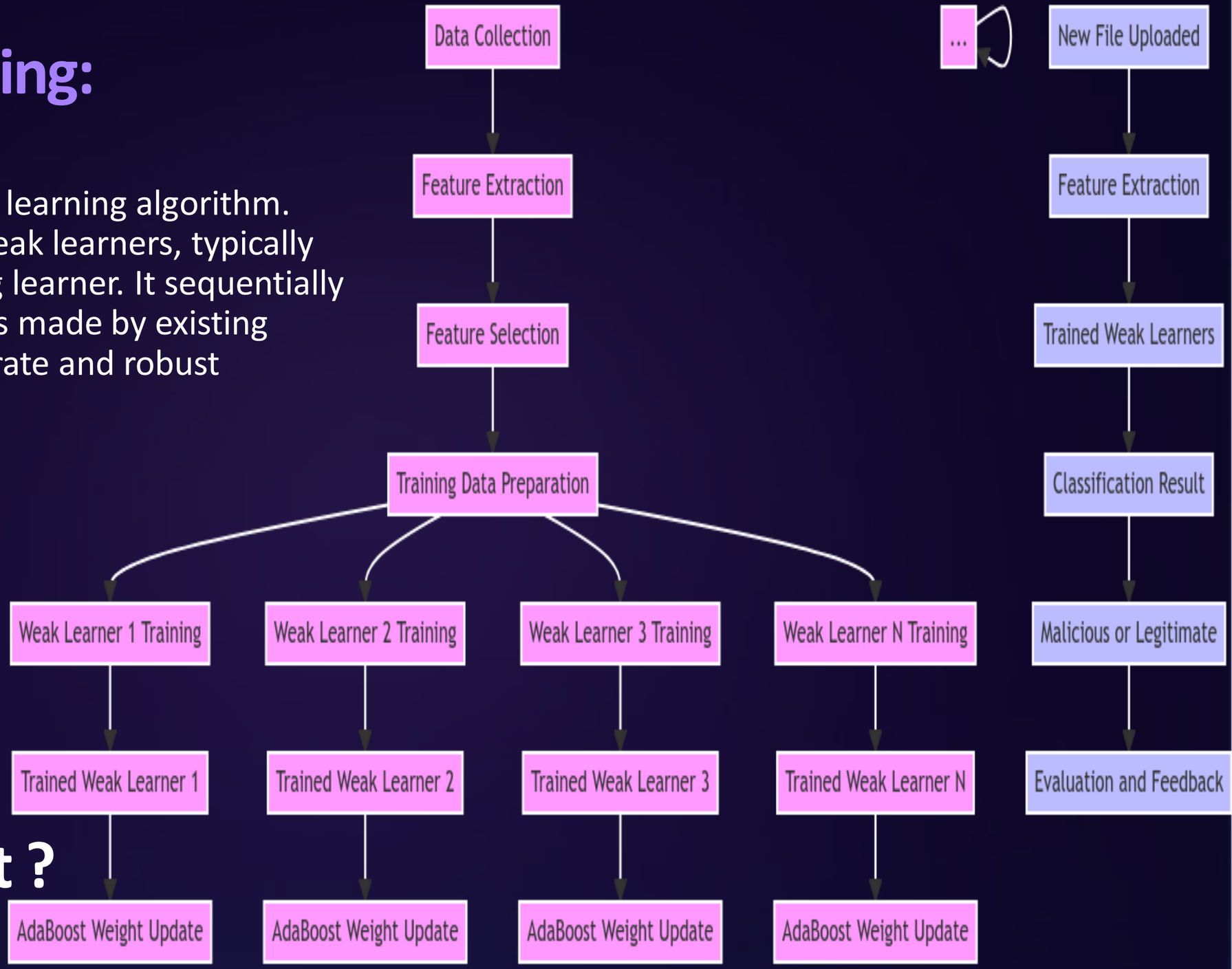
- How it work?
- Why we Choose it ?





Gradient Boosting:

Gradient Boosting is a **supervised** learning algorithm. It works by combining multiple weak learners, typically decision trees, into a single strong learner. It sequentially adds new models to correct errors made by existing models, resulting in a highly accurate and robust predictive model.

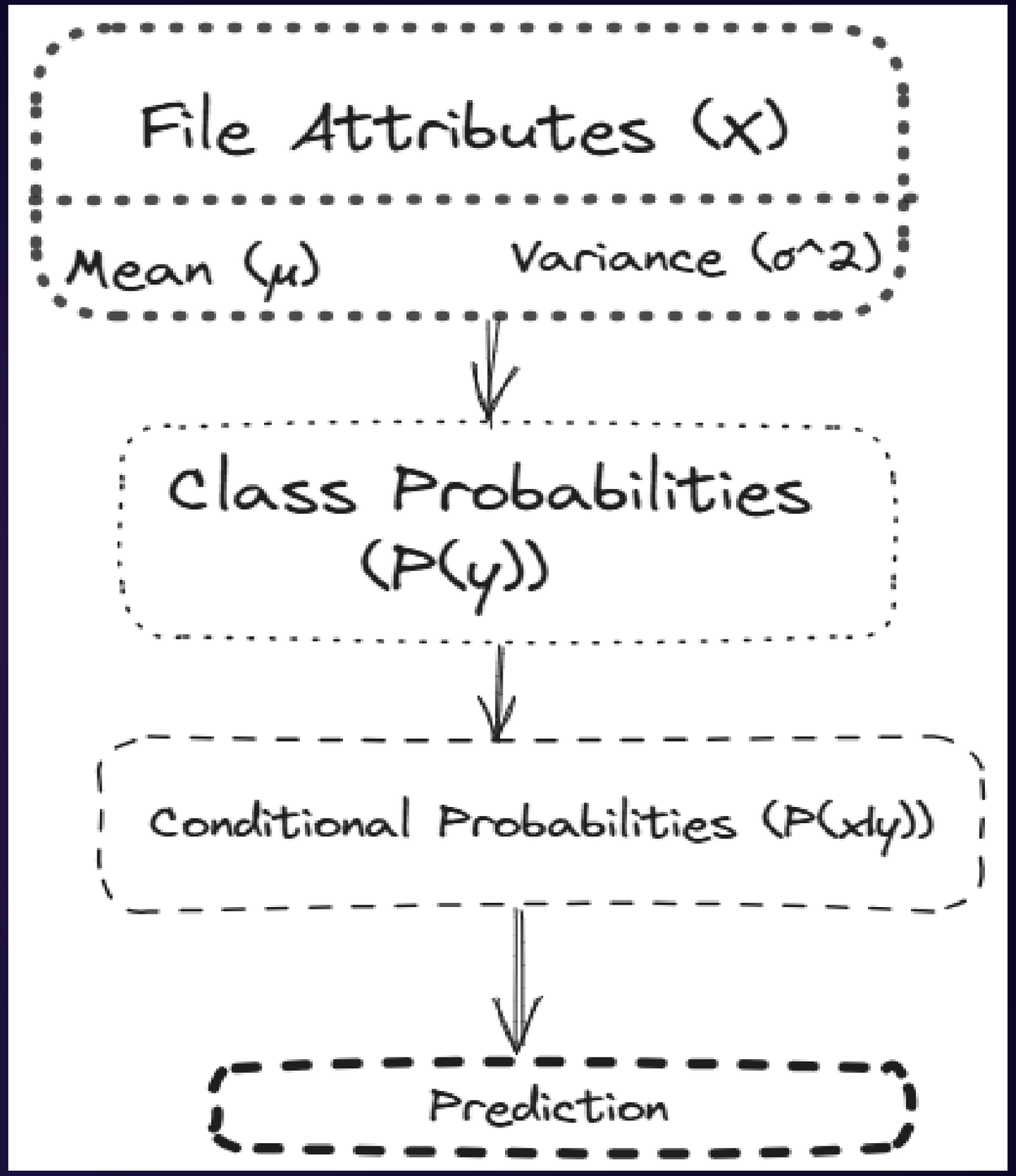


- **How it work?**
- **Why we Choose it ?**

Gaussian Naïve Bayes:

Gaussian Naive Bayes is a supervised learning algorithm based on Bayes' theorem. It assumes that features are independent and follow a Gaussian distribution. This simplifies probability calculations and makes it computationally efficient. The algorithm predicts the class label with the highest probability for an input instance. It's versatile, easy to implement, and suitable for classification tasks, particularly with limited computational resources or datasets with many features."

- **How it work?**
- **Why we Choose it ?**

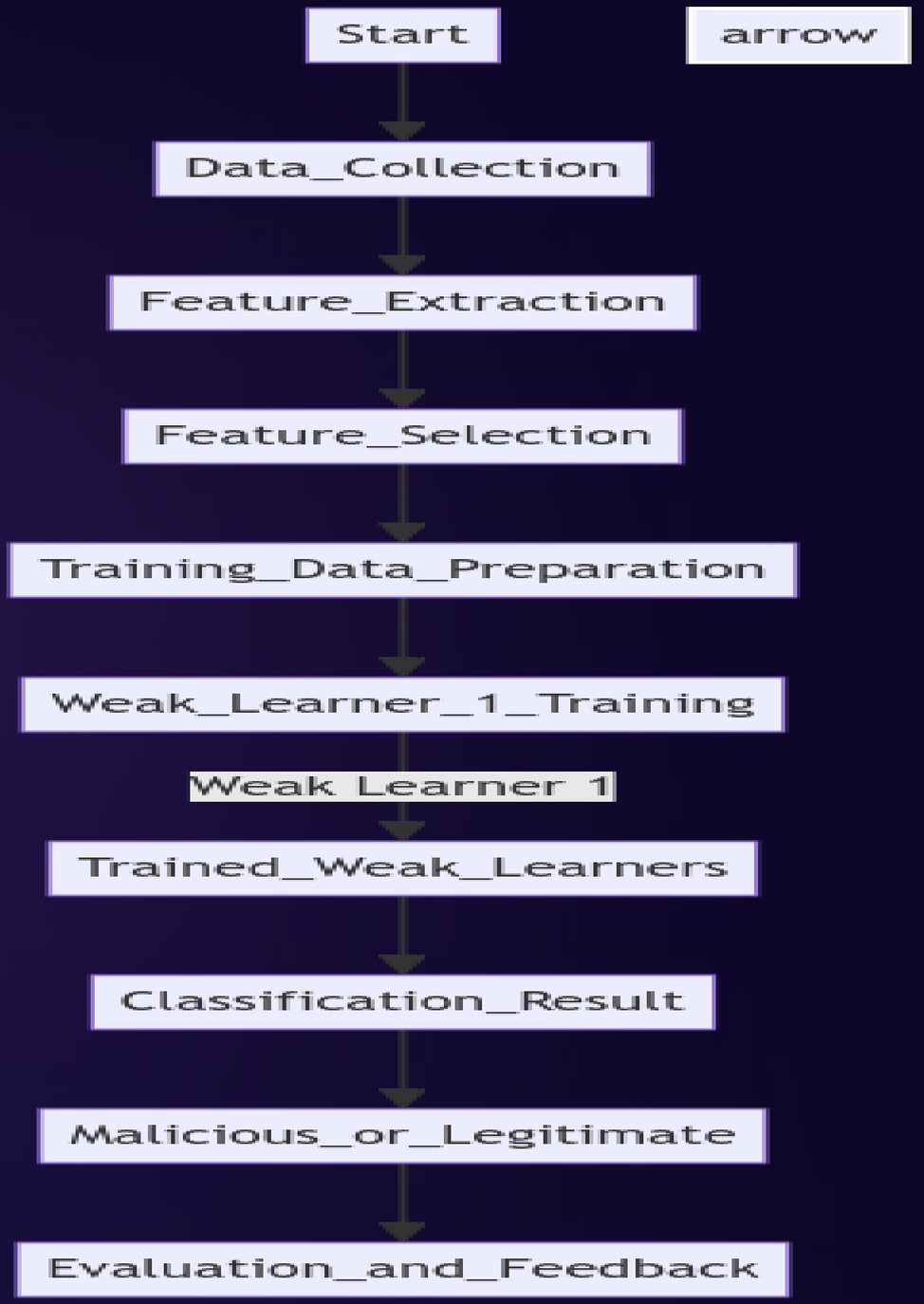


AdaBoost:

AdaBoost is a supervised learning algorithm.

It works by combining multiple weak learners sequentially to create a strong classifier. Each weak learner is trained on a subset of the data, with more emphasis given to the instances that were misclassified by previous learners. This adaptive training process allows AdaBoost to focus on the instances that are difficult to classify, improving its overall performance.

- How it work?
- Why we Choose it ?



WEB SCANNER:

Vulnerability web application scanners are powerful tools that meticulously analyze web applications, databases, and server configurations to uncover potential security flaws. These scanners use advanced techniques to detect vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms, helping organizations strengthen their web application security.

Capabilities of the WEB SCANNER:

Comprehensive Scanning

Vulnerability scanners perform in-depth scans of web applications, databases, and servers to uncover a wide range of security vulnerabilities.

Automated Reporting

These tools generate detailed reports that prioritize identified vulnerabilities and provide remediation guidance to help organizations address security risks.

Continuous Monitoring

Vulnerability scanners can be configured to regularly monitor web applications, ensuring continuous security assessment and rapid response to new threats.

Common Vulnerabilities Detected by WEB SCANNER:

Cross-Site Scripting (XSS)

SQL Injection (SQLi)

Server-Side Request Forgery (SSRF)

Directory Traversal/Path Traversal

XML External Entity (XXE) Injection

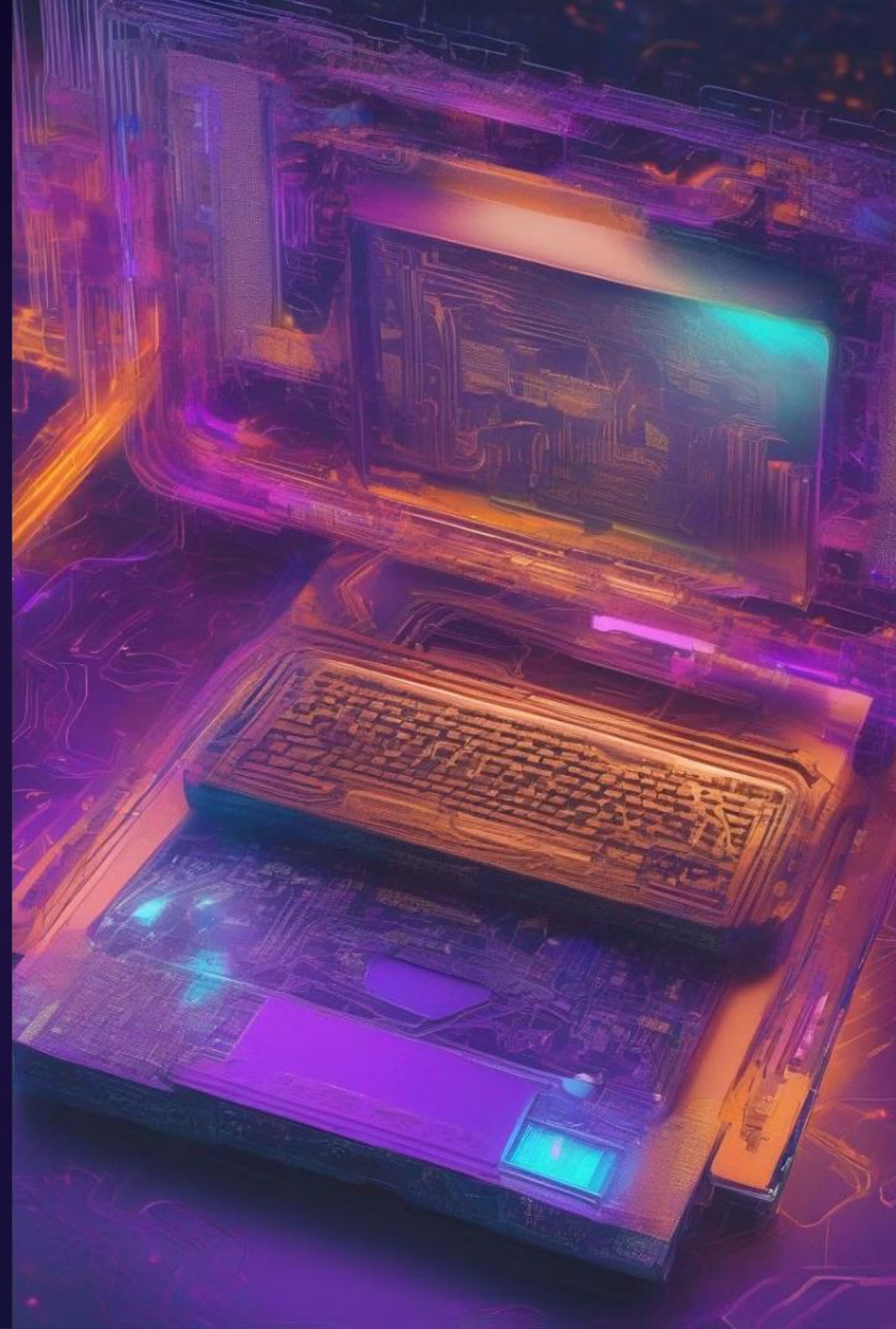
OS Command Line Injection

Headers Injection

Misconfigurations

Network Scanner

provides network scanners tailored to detect vulnerabilities in various network infrastructure components like routers and switches. These scanners analyze network security configurations, identifying potential misconfigurations and vulnerabilities that attackers could exploit to gain unauthorized access or disrupt network operations.



Network Scanner:

Scanning Methodology

1. Perform /UDP Scan and finding Opening poTCPrts
2. Perform Service Version Scan
3. Perform OS Fingerprinting Scan
4. Scan for Vulnerabilities for Versions of Services

Deployment and Scalability

Cloud Infrastructure

The application is deployed on a robust and scalable scalable cloud platform

Automatic Scaling

Intelligent autoscaling mechanisms adapt to fluctuating user demands and file processing loads. loads.

Containerization

Docker containers ensure seamless deployment and easy and easy scaling of the application.

Future work:

Mobile App Development

Build a feature-rich mobile app for for both Android and iOS platforms platforms to expand our reach and and accessibility.

Tool Publication

Release our vulnerability scanning tool to the public, enabling users to proactively secure their digital environments.

Automation & Optimization

Implement advanced automation automation and optimization techniques to streamline the vulnerability management process, process, ensuring greater efficiency efficiency and responsiveness.

At the forefront of cybersecurity, we are committed to staying ahead of the curve. Our future work will focus on anticipating emerging threats, incorporating the most innovative vulnerability detection techniques, and streamlining our processes through automation and optimization. This unwavering dedication to continuous improvement will ensure our clients' digital assets remain secure and resilient in the face of evolving challenges.

Thank you

We appreciate your trust and Attaching.