GenZai IoT Security Toolkit Project

1. Objective

The primary objective of the **GenZai IoT Security Toolkit** project is to develop a comprehensive tool for identifying and addressing vulnerabilities in IoT devices. The goals include:

- **Scanning Target URLs**: Identify IoT devices hosted on target URLs and detect potential security weaknesses.
- **Assessing Vendor Vulnerabilities**: Utilize vendor-specific databases to check for default credentials and known vulnerabilities.
- **Demonstrating IoT Security Risks**: Emphasize the importance of securing IoT devices through practical demonstrations.

2. Tools Used

1. **Programming Language**:
    - Golang for backend functionality.
    - Python and Streamlit for UI development.
2. **Libraries and Frameworks**:
    - os, net/http, and encoding/json for Go backend processing.
    - requests, pandas, and streamlit for the frontend.
3. **Databases**:
    - signatures.json: Contains IoT signature data for identifying devices.
    - vendor-logins.json: Stores default vendor credentials for password scanning.
    - vendor-vulns.json: Lists vendor-specific vulnerabilities.
4. **Tools and Platforms**:
    - **Postman**: API testing and development.
    - **VS Code**: Code development and debugging.

3. Methodology

Step 1: Setup Environment

- Configure the development environment with necessary dependencies:
    - Install Go and Python.
    - Install Streamlit and Python libraries from requirements.txt.
    - Set up the JSON databases in the project directory.

Step 2: Initialize the Toolkit

- **Run the Backend**:
    - Start the Go server with go run main.go.
- **Launch the Frontend**:
    - Run the Streamlit UI with streamlit run ui-main.py.

Step 3: Enter Target Information

- Users can either manually input target URLs or upload a file containing URLs.
- Change API endpoint configuration if required for specialized scanning.

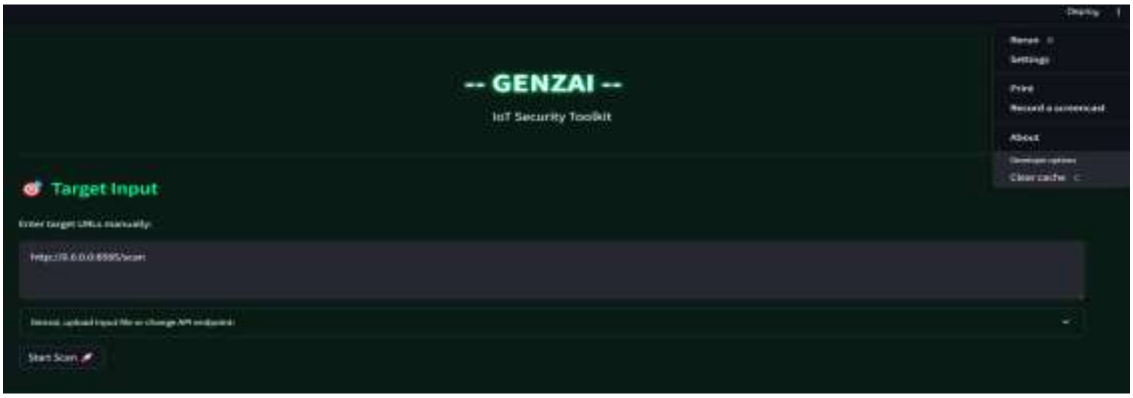
Step 4: Scan Targets

- For each target URL, perform the following:
    - Identify IoT devices using signatures from signatures.json.
    - Check for default vendor credentials using vendor-logins.json.
    - Scan for known vulnerabilities using vendor-vulns.json.

Step 5: Capture Results

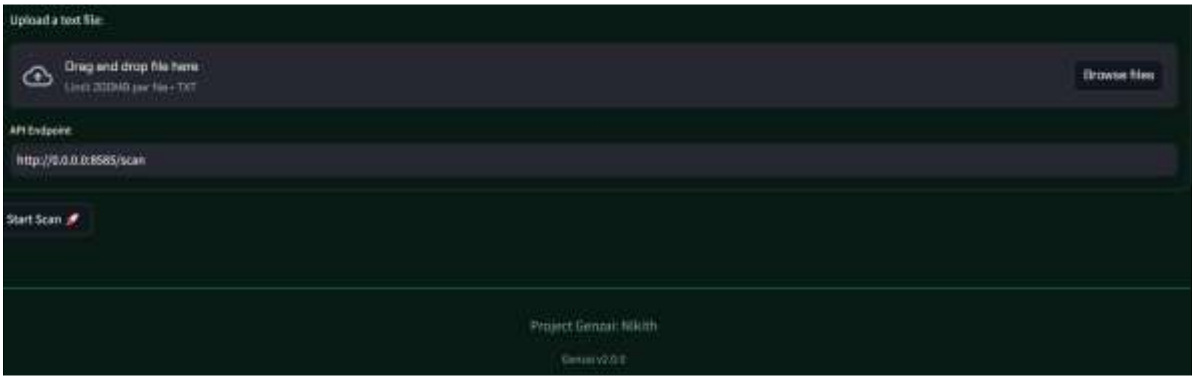
- Log detailed results, including detected vulnerabilities and recommendations, into a specified output file (results.log).

5.**Proof of Concept**



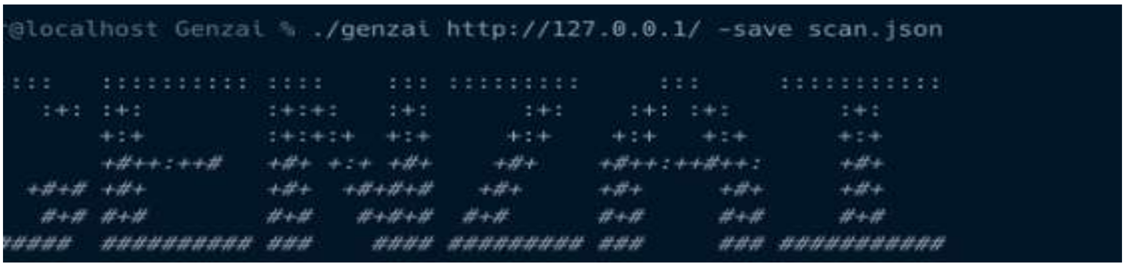
Enter target URLs manually:

http://0.0.0.0:8585/scan



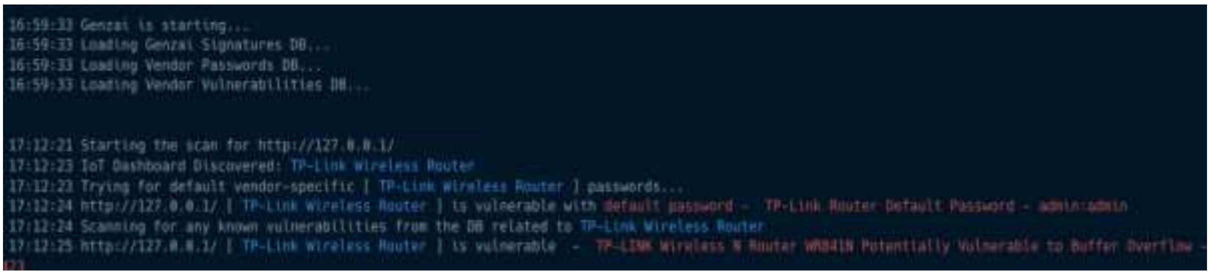
API Endpoint:

http://0.0.0.0:8585/scan



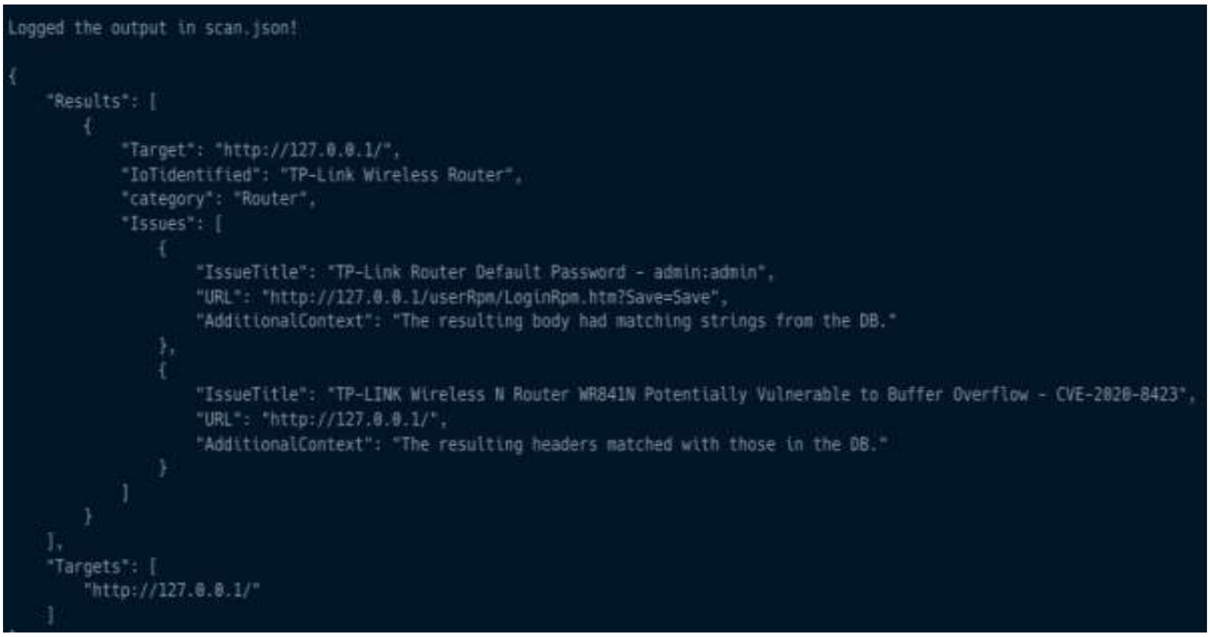
```
r@localhost Genzai % ./genzai http://127.0.0.1/ -save scan.json

:::    :::::::::: ::::    ::: :::::::::     :::     :::::::::::
   :+: :+:        :+:+:   :+:      :+:    :+: :+:       :+:
       +:+        :+:+:+  +:+     +:+    +:+   +:+      +:+
       +#++:++#   +#+ +:+ +#+    +#+    +#++:++#++:     +#+
  +#+# +#+        +#+  +#+#+#   +#+     +#+     +#+     +#+
   #+# #+#        #+#   #+#+#  #+#      #+#     #+#     #+#
#####  ########## ###    #### ######### ###     ### ###########
```



```
16:59:33 Genzai is starting...
16:59:33 Loading Genzai Signatures DB...
16:59:33 Loading Vendor Passwords DB...
16:59:33 Loading Vendor Vulnerabilities DB...


17:12:21 Starting the scan for http://127.0.0.1/
17:12:23 IoT Dashboard Discovered: TP-Link Wireless Router
17:12:23 Trying for default vendor-specific [ TP-Link Wireless Router ] passwords...
17:12:24 http://127.0.0.1/ [ TP-Link Wireless Router ] is vulnerable with default password -  TP-Link Router Default Password - admin:admin
17:12:24 Scanning for any known vulnerabilities from the DB related to TP-Link Wireless Router
17:12:25 http://127.0.0.1/ [ TP-Link Wireless Router ] is vulnerable  -  TP-LINK Wireless N Router WR841N Potentially Vulnerable to Buffer Overflow -
823
```



```
Logged the output in scan.json!

{
    "Results": [
        {
            "Target": "http://127.0.0.1/",
            "IoTidentified": "TP-Link Wireless Router",
            "category": "Router",
            "Issues": [
                {
                    "IssueTitle": "TP-Link Router Default Password - admin:admin",
                    "URL": "http://127.0.0.1/userRpm/LoginRpm.htm?Save=Save",
                    "AdditionalContext": "The resulting body had matching strings from the DB."
                },
                {
                    "IssueTitle": "TP-LINK Wireless N Router WR841N Potentially Vulnerable to Buffer Overflow - CVE-2020-8423",
                    "URL": "http://127.0.0.1/",
                    "AdditionalContext": "The resulting headers matched with those in the DB."
                }
            ]
        }
    ],
    "Targets": [
        "http://127.0.0.1/"
    ]
```

5. Conclusion

The **GenZai IoT Security Toolkit** highlights the critical need for robust security practices in IoT environments by demonstrating how insecure configurations can lead to vulnerabilities. Key takeaways include:

- The importance of securing IoT devices with strong credentials and firmware updates.

- Leveraging tools like GenZai to proactively identify and mitigate IoT vulnerabilities.

This project emphasizes the value of IoT security in safeguarding against unauthorized access and data breaches.