**I. Phần mềm phát hiện tấn công Phishing**

**Phishing** là một loại tấn công an ninh mạng trong đó những kẻ xấu gửi tin nhắn giả mạo là một cá nhân hoặc tổ chức đáng tin cậy. Tin nhắn lừa đảo thao túng người dùng, khiến họ thực hiện các hành động như cài đặt tệp độc hại, nhấp vào liên kết độc hại hoặc tiết lộ thông tin nhạy cảm như thông tin xác thực truy cập.

**Mail Phishing.** Những kẻ tấn công thường đăng ký tên miền giả mạo bắt chước các tổ chức và gửi hàng nghìn yêu cầu chung cho nạn nhân.Đối với các miền giả mạo, những kẻ tấn công có thể thêm hoặc thay thế các ký tự (ví dụ: my-bank.com thay vì mybank.com), sử dụng các miền phụ (ví dụ: mybank.host.com) hoặc sử dụng tên của tổ chức đáng tin cậy làm tên người dùng email (ví dụ: mybank @ host. com).Nhiều email lừa đảo sử dụng cảm giác khẩn cấp hoặc đe dọa để khiến người dùng nhanh chóng tuân thủ mà không kiểm tra nguồn hoặc tính xác thực của email.

Thư lừa đảo qua email có một trong các mục tiêu sau:

- Nhấp vào liên kết đến một trang web độc hại để cài đặt phần mềm độc hại.

- Tải xuống tệp độc hại.

- Nhấp vào liên kết đến một trang web giả mạo và gửi dữ liệu cá nhân.

- Khiến người dùng trả lời và cung cấp dữ liệu cá nhân.

**URL(web) Phising** là hành vi gian lận nhằm dụ các cá nhân đến một trang web mạo danh, nơi họ sẽ tải xuống phần mềm độc hại hoặc tiết lộ thông tin cá nhân. Trang web thường yêu cầu người dùng đặt lại mật khẩu, nhập lại thông tin cá nhân và thông tin tín dụng để xác thực tài khoản hoặc tải xuống bản cập nhật.

|  |  |  |
| --- | --- | --- |
|  | **Phishing Websites** | **Phishing Mails** |
| **Tổng quan** | Chrome add-on cảnh báo người dùng khi truy cập vào 1 website được xác định là malicious. | - Webapp cho phép người dùng nhập các trường thông tin của email (sender, receiver, time, subject, content,...) để xác định liệu email có phải lừa đảo hay không.  - ***Maybe***: add-on cảnh báo khi người dùng mở mail lừa đảo. |
| **Hệ thống** | **Front-tier**  - User tool:  + Chrome add-on thu thập được input theo yêu cầu của mô hình (**cần làm rõ**), gửi về cho Back-tier và nhận kết quả, đưa ra cảnh báo nếu phát hiện lừa đảo.  + Đưa ra cảnh báo nếu URL trong blacklist DB.  - Admin tool:  + Giao diện đăng nhập  + Giao diện quản lý log (url, thời gian chạy mô hình, kết quả)  + Giao diện quản lý blacklist (tự động thêm url hại, cho phép thêm, sửa, xoá bởi admin) | **Front-tier**  - User tool:  + Giao diện đăng nhập.  + Giao diện thay đổi thông tin người dùng.  + Giao diện nhập các trường thông tin của email.  + Giao diện trả về kết quả.  - Admin tool:  + Giao diện đăng nhập  + Giao diện quản lý người dùng  + Giao diện quản lý log (url, thời gian chạy mô hình, kết quả) |
| **Back-tier:**  - User tool:  + API cảnh báo nếu URL trong blacklist  + API phát hiện phishing (tự động thêm URL lừa đảo vào bảng blacklist)  - Admin tool:  + API đăng nhập  + API get log  + API CRUD blacklist | **Back-tier:**  - User tool:  + API đăng nhập  + API cập nhật thông tin người dùng  + API phát hiện phishing  - Admin tool:  + API đăng nhập  + API CRUD người dùng  + API get log  + API CRUD blacklist |
| **Ngôn ngữ** | - Front-tier: Javascript (user), ReactJS (admin)  - Back-tier: | - Front-tier: ReactJS for both  - Back-tier: |

**II. Phần mềm phát hiện hình ảnh chứa văn bản có nội dung nhạy cảm**

Phát hiện nội dung văn bản nhạy cảm trong các file ảnh.

|  |  |  |
| --- | --- | --- |
| **Tổng quan** | Webapp cho phép người dùng upload ảnh để kiểm tra văn bản trong ảnh có nội dung nhạy cảm. | ***Maybe***: Chrome add-on thu thập tất cả hình ảnh khi truy cập vào 1 trang web và cảnh báo nếu có nội dung nhạy cảm. |
| **Hệ thống** | **Front-tier**  - User tool:  + Giao diện đăng nhập.  + Giao diện thay đổi thông tin người dùng.  + Giao diện tải ảnh.  + Giao diện trả về kết quả.  + ***Maybe***: Giao diện hiển thị kết quả các bước trung gian - văn bản trích xuất được, những đoạn nào là nhạy cảm.  - Admin tool:  + Giao diện đăng nhập  + Giao diện quản lý người dùng  + Giao diện quản lý log (ảnh, thời gian chạy mô hình, ***văn bản trích xuất được***, kết quả) | **Front-tier**  - User tool:  + Chrome add-on thu thập được tất cả ảnh, gửi về cho Back-tier và nhận kết quả, đưa ra cảnh báo nếu phát hiện có nội dung nhạy cảm.  + Đưa ra cảnh báo nếu URL trong blacklist DB.  - Admin tool:  + Giao diện đăng nhập  + Giao diện quản lý log (url, thời gian chạy mô hình, kết quả)  + Giao diện quản lý blacklist (tự động thêm url hại, cho phép thêm, sửa, xoá bởi admin) |
| **Back-tier:**  - User tool:  + API đăng nhập  + API cập nhật thông tin người dùng  + API phát hiện ảnh có text nhạy cảm  + ***Maybe***: API get các kết quả trung gian  - Admin tool:  + API đăng nhập  + API CRUD người dùng  + API get log | **Back-tier:**  - User tool:  + API cảnh báo nếu URL trong blacklist  + API phát hiện nhạy cảm (tự động thêm URL vào bảng blacklist)  - Admin tool:  + API đăng nhập  + API get log  + API CRUD blacklist |
| **Ngôn ngữ** | - Front-tier: ReactJS for both  - Back-tier: | - Front-tier: Javascript (user), ReactJS (back)  - Back-tier: |

**III. Phần mềm tấn công captcha**

Phát hiện và bypass captcha validation, request dữ liệu liên tục từ máy chủ.

|  |  |
| --- | --- |
| **Tổng quan** | Chrome add-on **liên tục** thu thập captcha gửi về cho back-tier, nhận văn bản được xác định, fill vào captcha form. |
| **Hệ thống** | **Front-tier**  - User tool:  + Giao diện bật/tắt trên add-ons.  + Khi bật, Chrome add-on thu thập captcha, gửi về cho Back-tier và nhận kết quả, fill vào form.  + Gửi lại case trích xuất lỗi.  - Admin tool:  + Giao diện đăng nhập  + Giao diện quản lý log (url, thời gian chạy mô hình, kết quả)  + Giao diện quản lý các captcha trích xuất lỗi |
| **Back-tier:**  - User tool:  + API nhận captcha, trả lại extracted text.  + API nhận cases lỗi.  - Admin tool:  + API đăng nhập  + API get log  + API get cases lỗi |
| **Ngôn ngữ** | - Front-tier: ReactJS (admin), Javascript (user)  - Back-tier: |

**Chú ý**: Có thể thêm các module sau cho tất cả project

- Xây dựng cơ sở dữ liệu.

- Đóng gói ứng dụng dạng Docker Image.

- Triển khai trên môi trường Windows.

- Triển khai trên môi trường Linux.