**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 10**

**Name:** Peiris W.S.S.N

**Registration Number:** IT23227286

Contents

[1. Introduction 3](#_Toc196570383)

[2. Reconnaissance 4](#_Toc196570384)

[3. Vulnerability 6](#_Toc196570385)

[4. Vulnerability description 6](#_Toc196570386)

[5. Affected Components 6](#_Toc196570387)

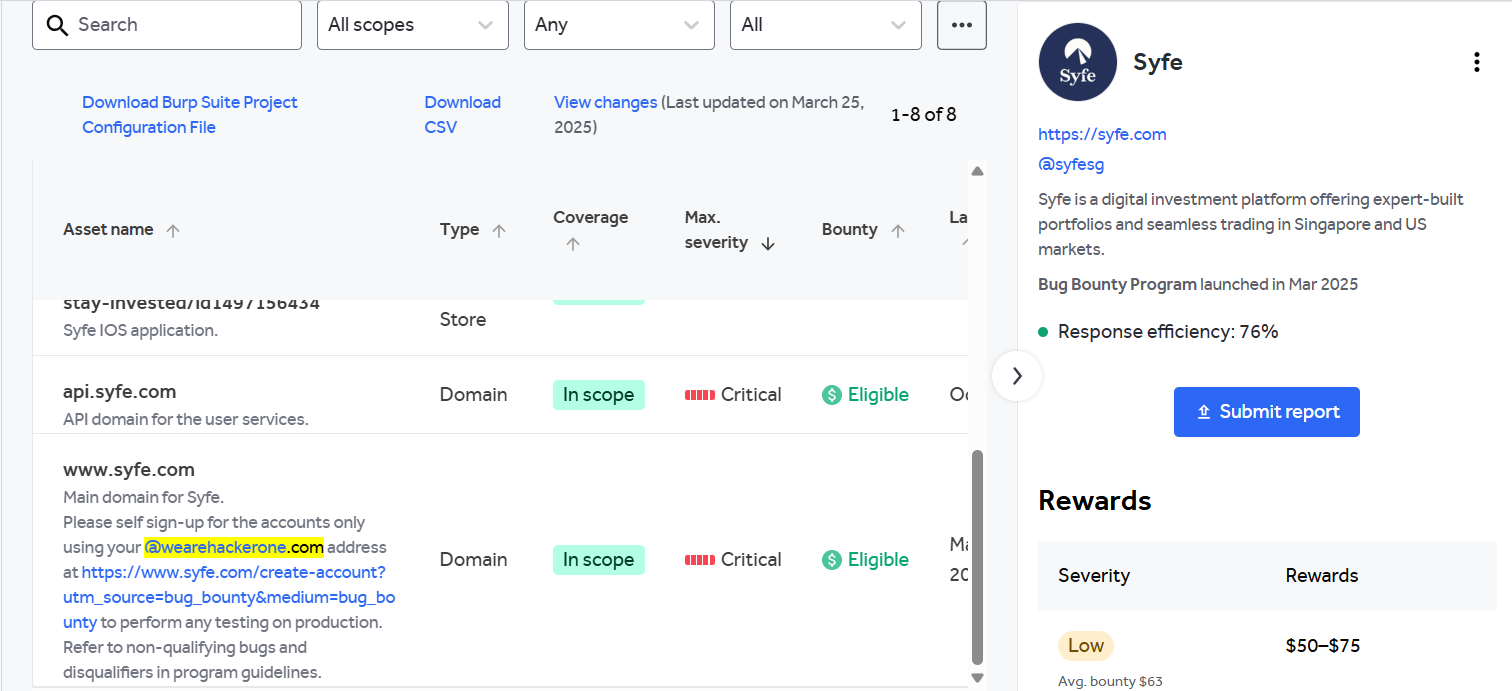
[6. Impact Assessment 7](#_Toc196570388)

[7. Steps to reproduce 8](#_Toc196570389)

[8. Proof of concept 9](#_Toc196570390)

[9. Proposed mitigation or fix 9](#_Toc196570391)

# Introduction

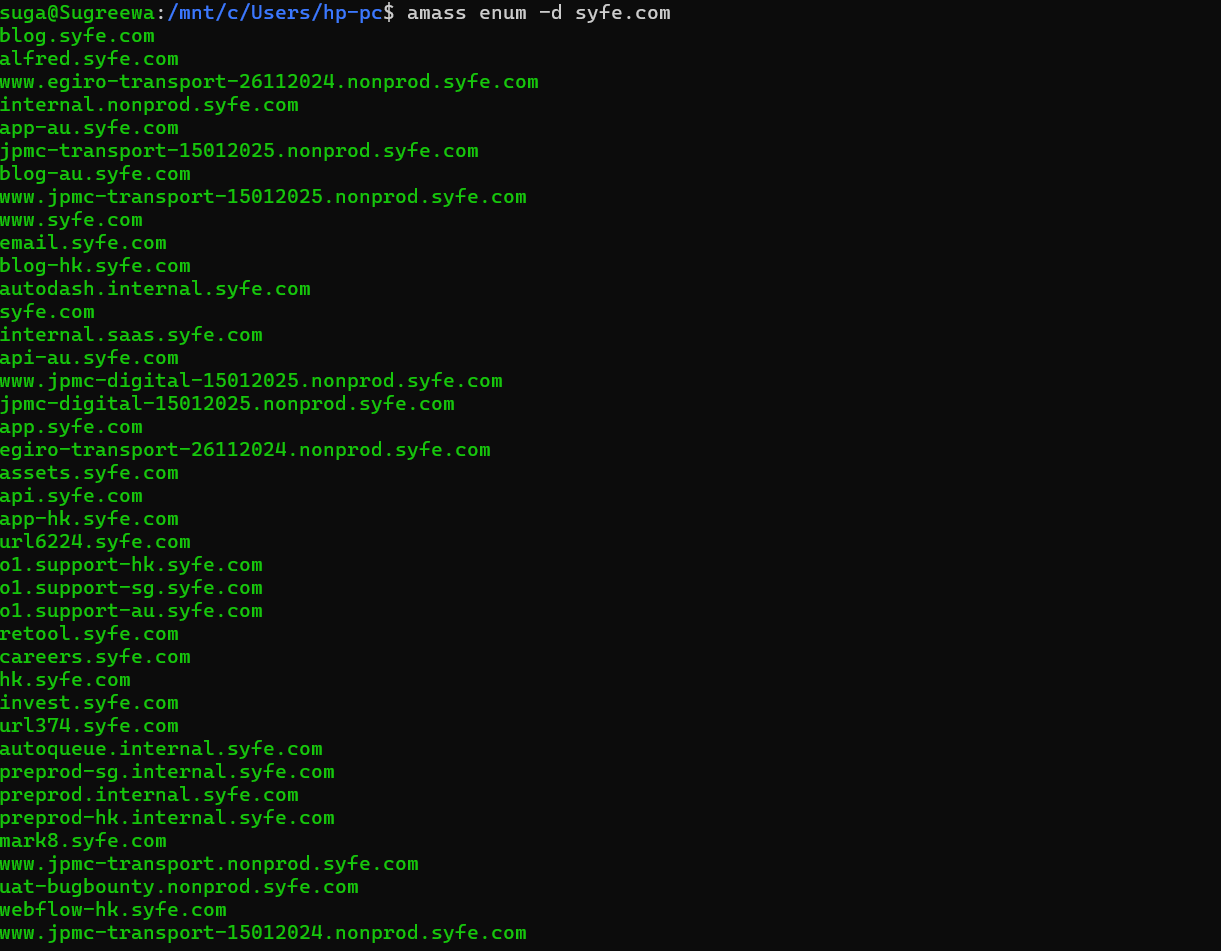


**Website:** <https://www.syfe.com/>

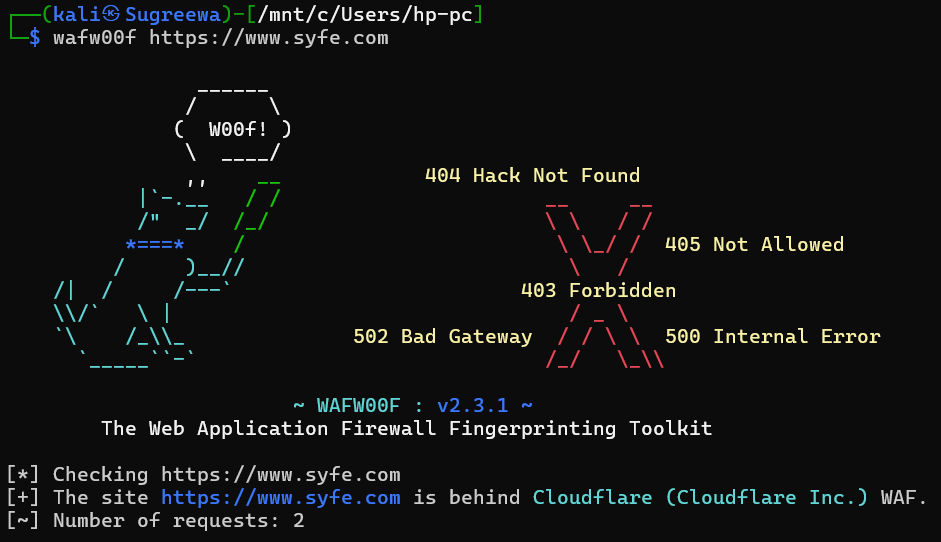
**Listed by:** Syfe

# Reconnaissance

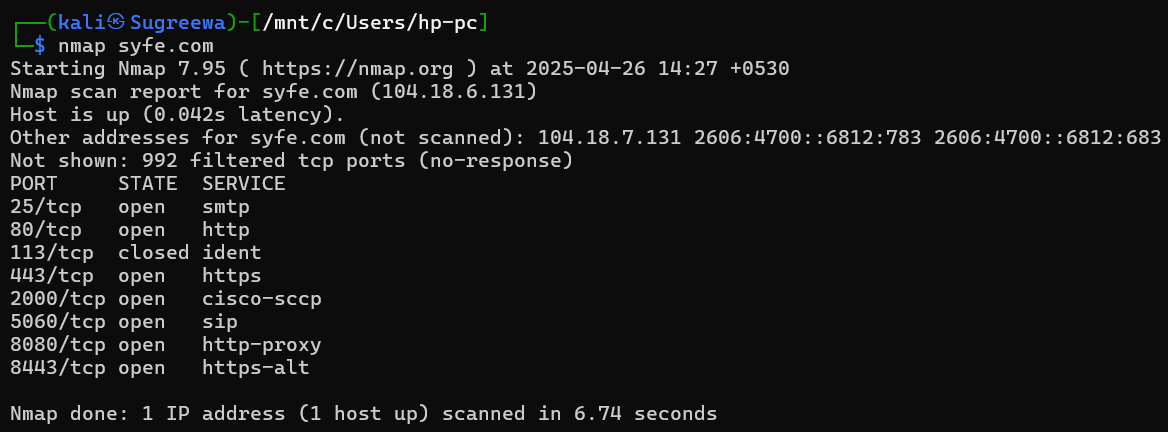
* **Subdomain enumeration using Amass**

****

* **Firewall detection**

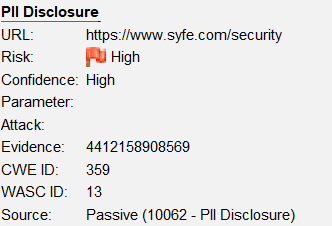
****

* **Nmap scan**

****

# Vulnerability

* **PII Disclosure**

****

# Vulnerability description

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

1. Affected Components

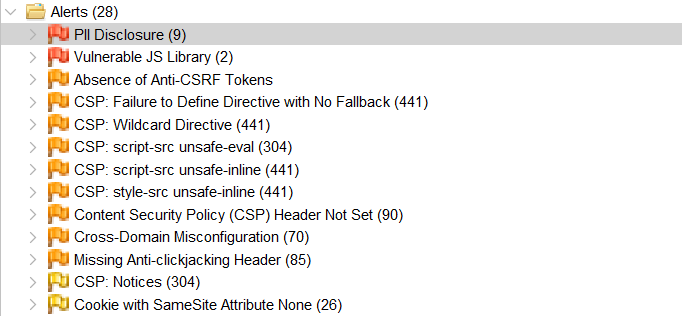
* **Component:** HTTP Response Body
* **Data Detected:**
  + Credit Card Number: 4412158908569
* **Card Details:**
  + **Type:** Visa
  + **Bank Identification Number (BIN):** 441215
  + **Issuer:** Bank of Hanover and Trust Company
  + **Category:** Business

# Impact Assessment

* **Risk Level:** **High**
* **Potential Impacts:**
  + **PCI-DSS compliance failure**
  + **User identity theft or fraud**
  + **Reputation damage**
  + **Regulatory penalties** (e.g., GDPR, CCPA)
  + **Data breaches** involving exposed financial information

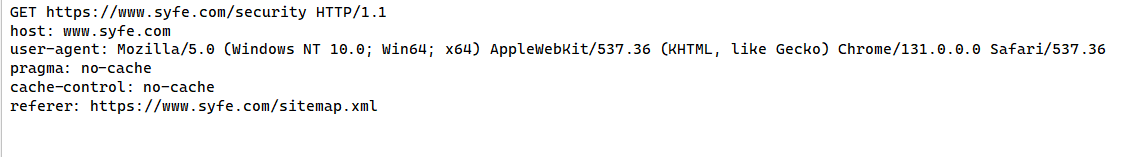
# Steps to reproduce

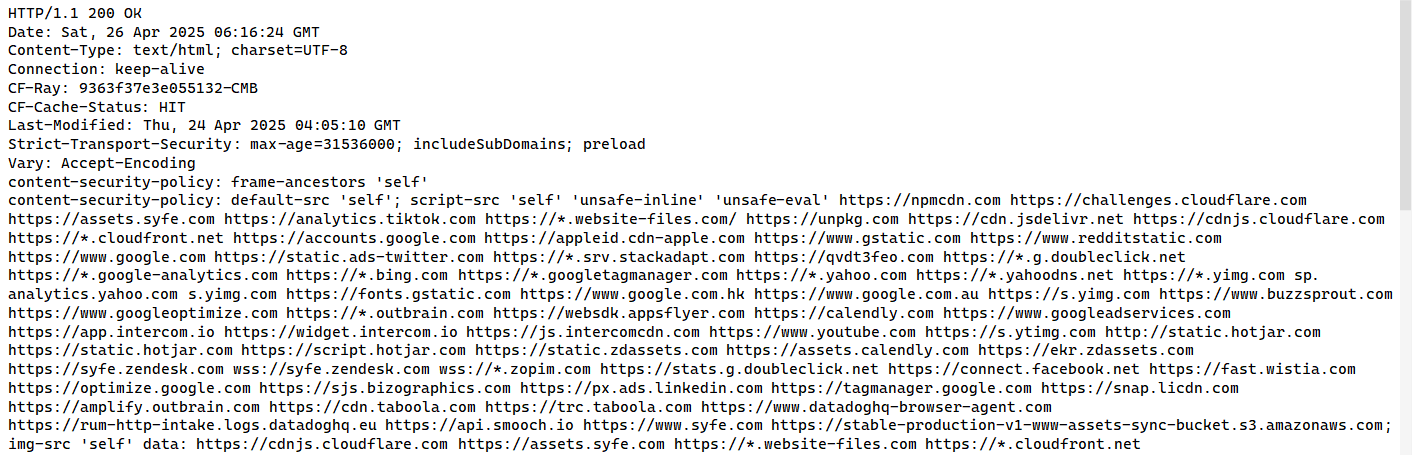
* Use a tool like **ZAP**, **Burp Suite**, or browser **DevTools**.



* Navigate to the affected endpoint or form submission page.
* Intercept the **HTTP response**.
* Search the body for credit card patterns
* Confirm presence of exposed CC data in plaintext

# Proof of concept





# Proposed mitigation or fix

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.