Sri Lanka Institute of Information Technology

Bug Bounty Report 01

WS Assignment

IE2062 – Web Security

IT23159730

W.H.M.S.R.Bandara

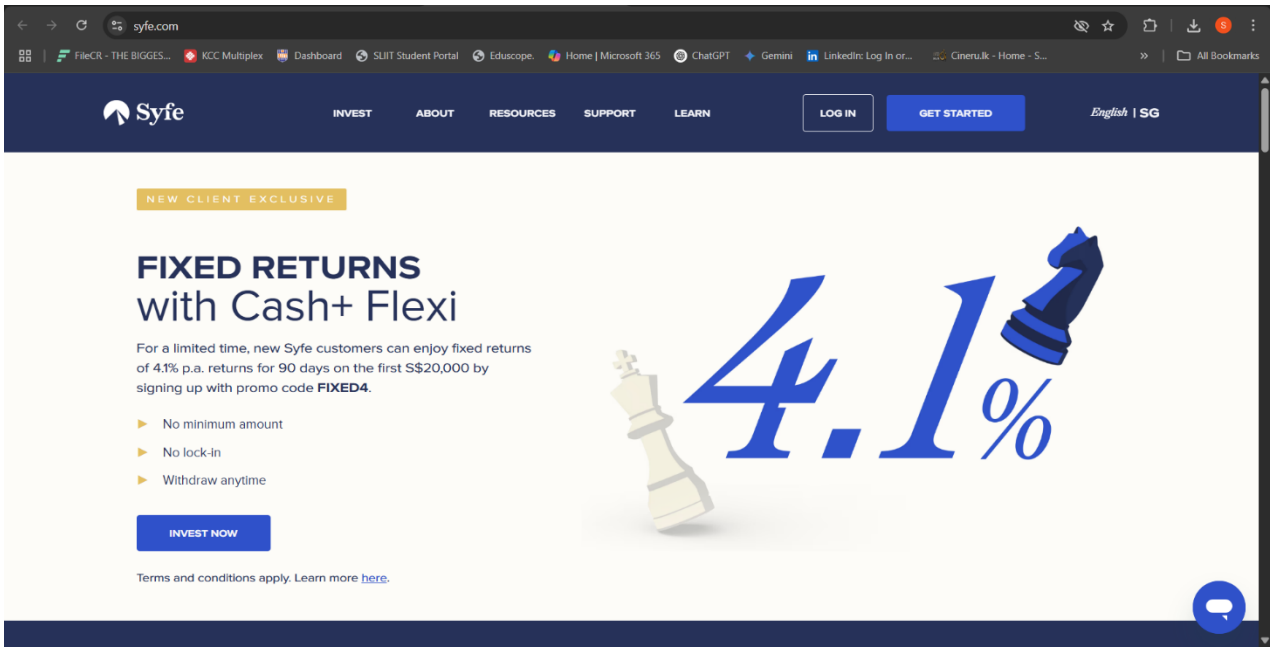
Vulnerability Title

High-Risk Personally Identifiable Information (PII) Disclosure on www.syfe.com

Vulnerability Description

Personally Identifiable Information (PII) refers to information that can be used to identify an individual, such as credit card numbers, names, addresses, and other sensitive personal traits. Its disclosure through a publicly accessible web application is a serious privacy and security concern. During automated scanning using OWASP ZAP (2.16.0), it was discovered that **https://www.syfe.com/security** exposes sensitive PII data, including credit card identification number and brand (Visa), through HTTP responses. This was a high-risk issue with high confidence.

The attack was passive and did not involve any exploitation apart from normal crawling and inspection.



Other Scans

Firewall Detection.

Before the automated scan with OWASP ZAP (2.16.0), Identify the Firewall by using Wafw00f Tool.

Affected Components

- **Domain:** www.syfe.com
- **Page:** /security
- **Request Method:** GET
- **Parameter:** N/A (data disclosed passively)
- **Risk Level:** High
- **Confidence:** High
- **OWASP Classification:** A01:2021 – Broken Access Control (data exposure)

Impact Assessment

If exploited, this vulnerability may result in:

- **Credit Card Fraud:** Hacked BIN (Bank Identification Number) and card type can be used in financial prospecting or social engineering.

- **Disruption of Privacy:** Public exposure of personally identifiable information can infringe on privacy regulations such as GDPR or PDPA.

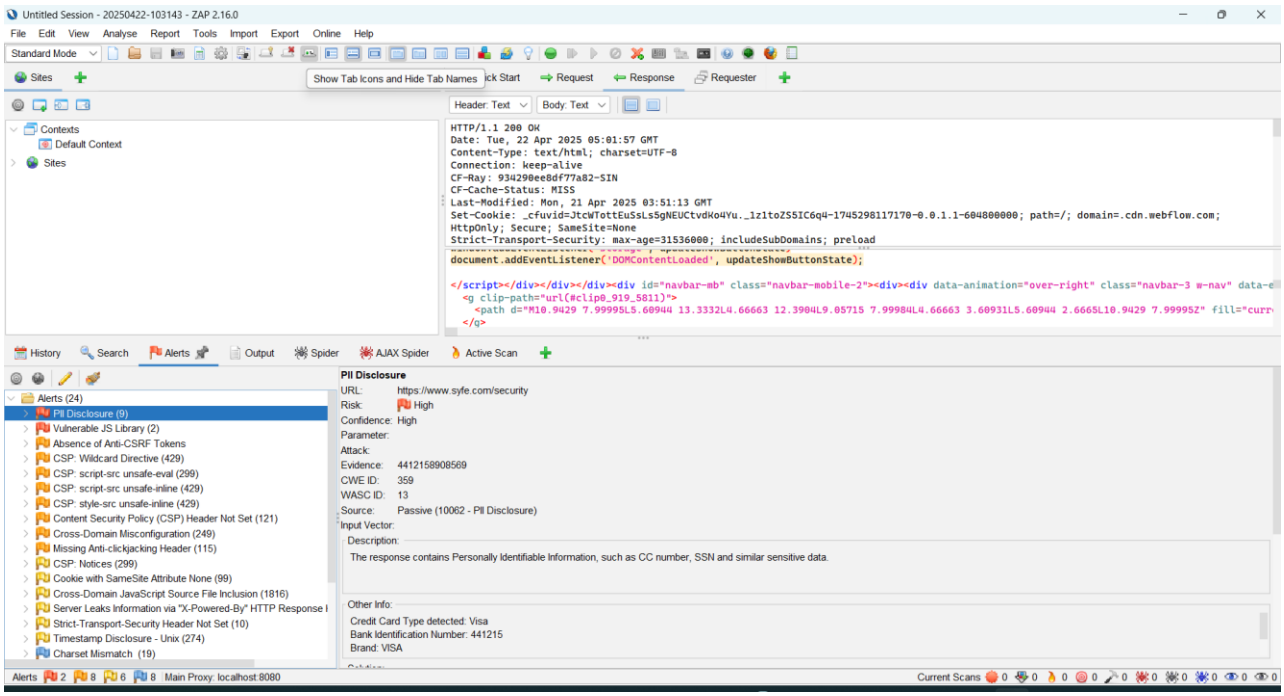
- **Damage to Reputation:** Financial institutions like Syfe are subject to high standards of data security; breaches severely damage trust.

- **Compliance Violation:** Unencrypted exposure of PII can result in litigation or fines.

Steps to Reproduce

1. Launch OWASP ZAP and run a passive scan against https://www.syfe.com/security.
2. In the Alerts tab, filter by **PII Disclosure**.
3. Locate the affected URL: https://www.syfe.com/security
4. Review the HTTP response body for sensitive patterns.
5. Observe data such as:
    - **Card Type:** Visa
    - **Bank Identification Number:** 441215.

Proof of Concept Screenshot



Proposed Mitigation or Fix

- **Do not Confidentiality**: Do not accidentally Disclose PII in http responses unless specifically required and authorized.
- **Tokenization**: substituting raw credit card information with its non-sensitive equivalent, usable only within the issuer.
- **Content security review**: Review application responses to identify and fix inadvertent data leaks.
- **Access Controls**: Contain access to such data only to authenticated and authorized users.
- **Logging & Alerting**: Alerts when sensitive data is used in a response.

Conclusion.

The public exposure of PII on https://www.syfe.com/security remains a serious information security mistake made public. All levels of financial institutions must protect the user's data, and any leaker can lead to wider damage. Immediate review and remediation are highly recommended to be in accordance with industry best practices and legal requirements.