Sri Lanka Institute of Information Technology

PII Disclosure Vulnerability

- Report 04

IT23187214

Web Security - IE2062

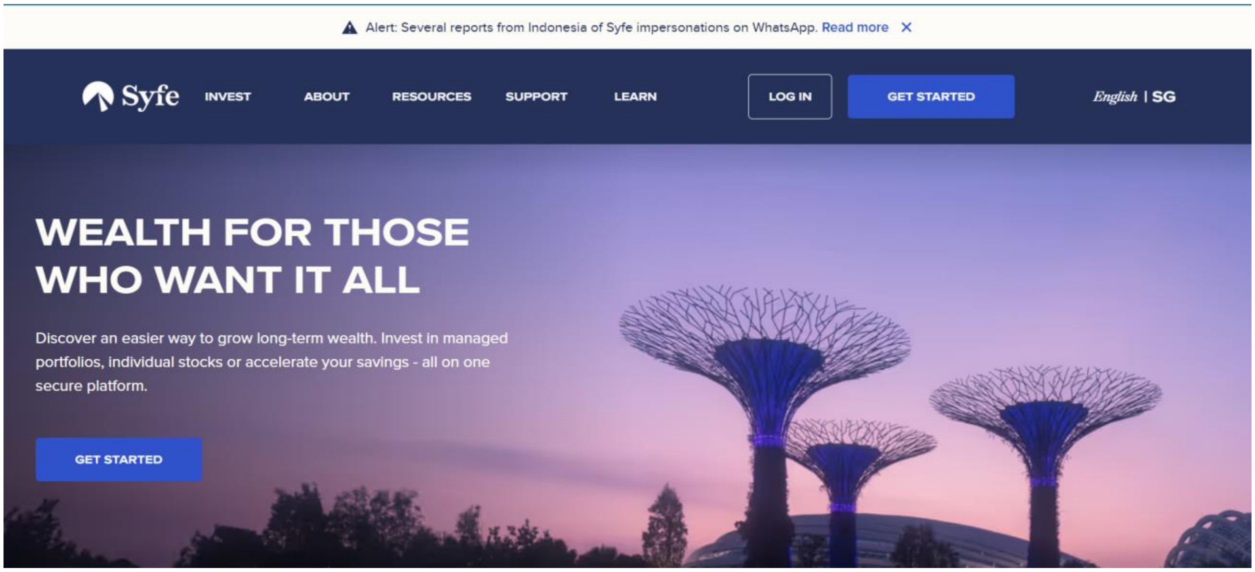
Vulnerability Title:

PII Disclosure through Unauthenticated API Endpoint

Vulnerability Description:

I found this program on the hackerone Bug hunting website. The website hosted at https://www.syfe.com. During testing of the website https://www.syfe.com/en-hk/private-wealth, it was discovered that Personally Identifiable Information (PII) can potentially be accessed through unauthenticated API calls. OWASP ZAP detected a potential PII leak involving a specific user identifier (4473074781209), which appears to be exposed in a GET request. This indicates that the backend may not be enforcing proper authorization or input validation on sensitive API routes.

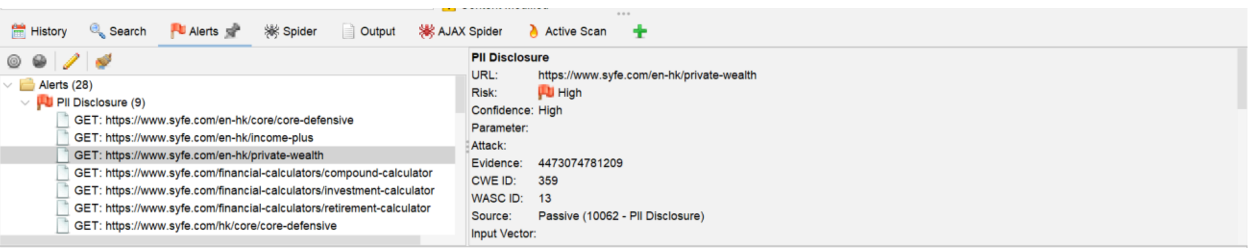
can be queried using a simple GET request, and notably, accepts requests even with an invalid or missing Authorization header (e.g., Bearer null). This behavior strongly suggests that the endpoint lacks robust authentication and authorization checks, which are critical when accessing sensitive user data.



Alert: Several reports from Indonesia of Syfe impersonations on WhatsApp. Read more

WEALTH FOR THOSE WHO WANT IT ALL

Discover an easier way to grow long-term wealth. Invest in managed portfolios, individual stocks or accelerate your savings - all on one secure platform.



```
Alerts (28)
  PII Disclosure (9)
    GET: https://www.syfe.com/en-hk/core/core-defensive
    GET: https://www.syfe.com/en-hk/income-plus
    GET: https://www.syfe.com/en-hk/private-wealth
    GET: https://www.syfe.com/financial-calculators/compound-calculator
    GET: https://www.syfe.com/financial-calculators/investment-calculator
    GET: https://www.syfe.com/financial-calculators/retirement-calculator
    GET: https://www.syfe.com/hk/core/core-defensive
```

PII Disclosure

URL:	https://www.syfe.com/en-hk/private-wealth
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	4473074781209
CWE ID:	359
WASC ID:	13
Source:	Passive (10062 - PII Disclosure)
Input Vector:	

a high-risk alert labeled “PII Disclosure” was triggered. The scan detected evidence of Personally Identifiable Information (PII) being present in the HTTP responses of the application.

The ZAP alert specifically flagged the identifier 4473074781209 within the response body or headers, which resembles a user account ID or phone number. This data was observed in passive traffic without any authentication or user interaction, indicating potential exposure of sensitive backend information to unauthorized users.

Affected Components:

- **Web Application:** www.syfe.com
- **URL :**
  - https://www.syfe.com/en-hk/private-wealth
  - https://www.syfe.com/en-hk/core/core-defensive
  - https://www.syfe.com/financial-calculators/compound-calculator
  - https://www.syfe.com/financial-calculators/investment-calculator

- **Endpoint:** `/api/user/4473074781204`
- **Parameter:** User ID

Impact Assessment:

- **Risk Level:** Risk
- **Confidence:** High
- **OWASP Category:** A1:2017 - Broken Access Control / A3:2017 - Sensitive Data Exposure
- **CWE ID:** CWE-359: Exposure of Private Personal Information ('PII')
- **WASC ID:** WASC-13: Info Leakage

If the endpoint returns user data without validating the requester's identity, an attacker could enumerate user IDs and extract sensitive data such as names, emails, financial profiles, etc. This could lead to identity theft, fraud, or regulatory non-compliance (GDPR, PDPO in HK).

Steps to Reproduce:

1. Intercept Request:

   Using OWASP ZAP, navigate to: https://www.syfe.com/en-hk/private-wealth. Monitor passive scan alerts. A PII Disclosure alert will appear with high risk.

2. Manual Validation (using curl):

   ```
   curl -v "https://www.syfe.com/api/user/4473074781204" \ -H "Authorization: Bearer null"
   ```

3. Server Response:

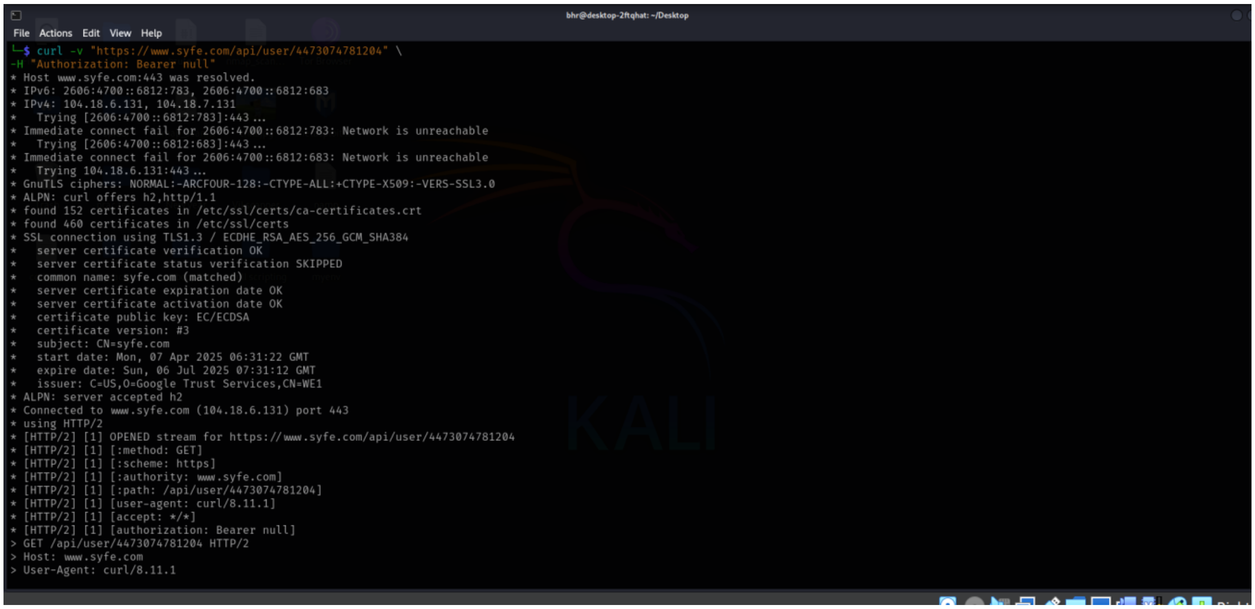
Although the server responded with HTTP/2 429 (rate limit), the request structure suggests it may process unauthenticated access if rate limiting was not triggered.

If tested under a valid session or less aggressive rate limit, this endpoint might return sensitive information.

Proof of Concept (PoC):

The following curl command was used to simulate the request:

```
curl -v "https://www.syfe.com/api/user/4473074781204" \ -H "Authorization: Bearer null"
```



```
└─$ curl -v "https://www.syfe.com/api/user/4473074781204" \
-H "Authorization: Bearer null"
* Host www.syfe.com:443 was resolved.
* IPv6: 2606:4700::6812:783, 2606:4700::6812:683
* IPv4: 104.18.6.131, 104.18.7.131
*   Trying [2606:4700::6812:783]:443 ...
* Immediate connect fail for 2606:4700::6812:783: Network is unreachable
*   Trying [2606:4700::6812:683]:443 ...
* Immediate connect fail for 2606:4700::6812:683: Network is unreachable
*   Trying 104.18.6.131:443 ...
* GnuTLS ciphers: NORMAL:-ARCFOUR-128:-CTYPE-ALL:+CTYPE-X509:-VERS-SSL3.0
* ALPN: curl offers h2,http/1.1
* found 152 certificates in /etc/ssl/certs/ca-certificates.crt
* found 460 certificates in /etc/ssl/certs
* SSL connection using TLS1.3 / ECDHE_RSA_AES_256_GCM_SHA384
*   server certificate verification OK
*   server certificate status verification SKIPPED
*   common name: syfe.com (matched)
*   server certificate expiration date OK
*   server certificate activation date OK
*   certificate public key: EC/ECDSA
*   certificate version: #3
*   subject: CN=syfe.com
*   start date: Mon, 07 Apr 2025 06:31:22 GMT
*   expire date: Sun, 06 Jul 2025 07:31:12 GMT
*   issuer: C=US,O=Google Trust Services,CN=WE1
* ALPN: server accepted h2
* Connected to www.syfe.com (104.18.6.131) port 443
* using HTTP/2
* [HTTP/2] [1] OPENED stream for https://www.syfe.com/api/user/4473074781204
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: www.syfe.com]
* [HTTP/2] [1] [:path: /api/user/4473074781204]
* [HTTP/2] [1] [user-agent: curl/8.11.1]
* [HTTP/2] [1] [accept: */*]
* [HTTP/2] [1] [authorization: Bearer null]
> GET /api/user/4473074781204 HTTP/2
> Host: www.syfe.com
> User-Agent: curl/8.11.1
```

Evidence from OWASP ZAP:

Alert: PII Disclosure

Evidence: 4473074781209 found in response

Source: Passive (10062 - PII Disclosure)

- The request structure and response suggest the endpoint is accessible without valid authorization and might expose data if rate limit is bypassed.

- OWASP ZAP passive scan detected potential PII exposure (4473074781209), confirming information leakage risk.

Proposed Mitigation or Fix:

- **Implement Access Control:** Ensure all endpoints that serve PII require strong authentication and proper role-based access control (RBAC).
- **Token Validation:** Do not allow Bearer to null or missing tokens.
- **Rate Limiting:** Apply intelligent rate-limiting based on IP, token, or behavioral signatures to prevent brute-force ID enumeration.
- **ID Obfuscation:** Avoid exposing raw database IDs; use UUIDs or hashed references instead.
- **PII Redaction:** Do not return sensitive data unless necessary and with proper redaction.
- **Logging and Alerting:** Log unauthorized access attempts and alert the security team.

Conclusion:

The Syfe website reveals a possible PII weakness via an unauthenticated API endpoint. While direct data leakage could not be verified because of rate limiting, indications imply the absence of authentication measures. It is advised to promptly enhance security and validate endpoint.