



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
2. Reconnaissance	4
3. Vulnerability	6
4. Vulnerability description.....	6
5. Affected Components	6
6. Impact Assessment.....	7
7. Steps to reproduce.....	8
8. Proof of concept.....	9
9. Proposed mitigation or fix	9

1. Introduction

Q Search

All scopes

Any

All

...


[Download Burp Suite Project Configuration File](#)

[Download CSV](#)

[View changes](#) (Last updated on March 25, 2025)

1-8 of 8

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	La
stay-invested/id149/156434 Syfe IOS application.	Store				
api.syfe.com API domain for the user services.	Domain	In scope	Critical	Eligible	On
www.syfe.com Main domain for Syfe. Please self sign-up for the accounts only using your @wearehackerone.com address at https://www.syfe.com/create-account?utm_source=bug_bounty&medium=bug_bounty to perform any testing on production. Refer to non-qualifying bugs and disqualifiers in program guidelines.	Domain	In scope	Critical	Eligible	Mi 20

 Syfe

<https://syfe.com>

[@syfesg](#)

Syfe is a digital investment platform offering expert-built portfolios and seamless trading in Singapore and US markets.

Bug Bounty Program launched in Mar 2025

● Response efficiency: 76%

[Submit report](#)

Rewards

Severity	Rewards
Low	\$50-\$75

Avg. bounty \$63

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

Listed by: Syfe


2. Reconnaissance

- Subdomain enumeration using Amass

```
suga@Sugreewa:/mnt/c/Users/hp-pc$ amass enum -d syfe.com
blog.syfe.com
alfred.syfe.com
www.egiro-transport-26112024.nonprod.syfe.com
internal.nonprod.syfe.com
app-au.syfe.com
jpmc-transport-15012025.nonprod.syfe.com
blog-au.syfe.com
www.jpmc-transport-15012025.nonprod.syfe.com
www.syfe.com
email.syfe.com
blog-hk.syfe.com
autodash.internal.syfe.com
syfe.com
internal.saas.syfe.com
api-au.syfe.com
www.jpmc-digital-15012025.nonprod.syfe.com
jpmc-digital-15012025.nonprod.syfe.com
app.syfe.com
egiro-transport-26112024.nonprod.syfe.com
assets.syfe.com
api.syfe.com
app-hk.syfe.com
url6224.syfe.com
ol.support-hk.syfe.com
ol.support-sg.syfe.com
ol.support-au.syfe.com
retool.syfe.com
careers.syfe.com
hk.syfe.com
invest.syfe.com
url374.syfe.com
autoqueue.internal.syfe.com
preprod-sg.internal.syfe.com
preprod.internal.syfe.com
preprod-hk.internal.syfe.com
mark8.syfe.com
www.jpmc-transport.nonprod.syfe.com
uat-bugbounty.nonprod.syfe.com
webflow-hk.syfe.com
www.jpmc-transport-15012024.nonprod.syfe.com
```

- Firewall detection

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ wafw00f https://www.syfe.com
```



```

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway 500 Internal Error

~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.syfe.com
[+] The site https://www.syfe.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

```

- Nmap scan

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ nmap syfe.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 14:27 +0530
Nmap scan report for syfe.com (104.18.6.131)
Host is up (0.042s latency).
Other addresses for syfe.com (not scanned): 104.18.7.131 2606:4700::6812:783 2606:4700::6812:683
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```

3. Vulnerability

- **PII Disclosure**

<u>PII Disclosure</u>	
URL:	https://www.syfe.com/security
Risk:	 High
Confidence:	High
Parameter:	
Attack:	
Evidence:	4412158908569
CWE ID:	359
WASC ID:	13
Source:	Passive (10062 - PII Disclosure)

4. Vulnerability description

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

5. Affected Components

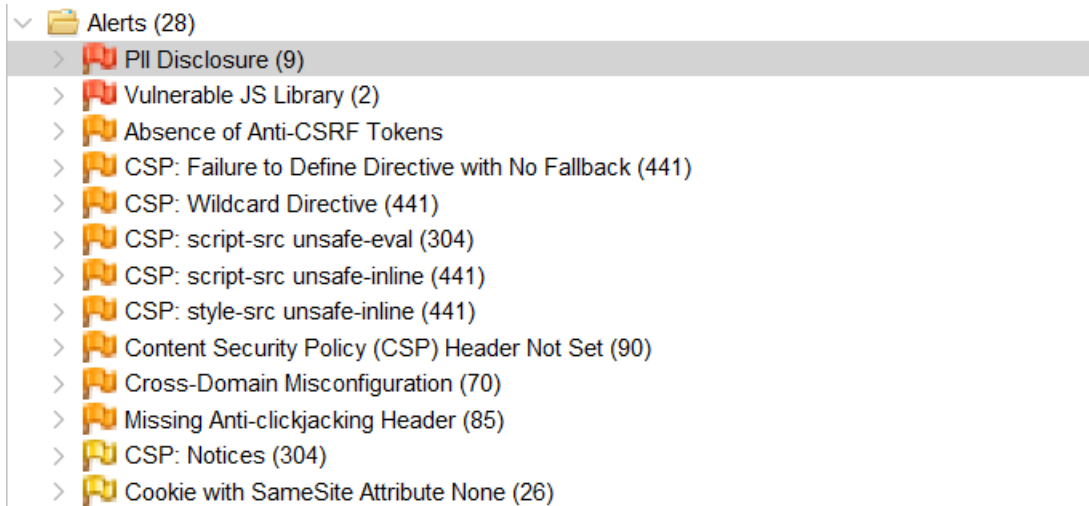
- **Component:** HTTP Response Body
- **Data Detected:**
 - Credit Card Number: 4412158908569
- **Card Details:**
 - **Type:** Visa
 - **Bank Identification Number (BIN):** 441215
 - **Issuer:** Bank of Hanover and Trust Company
 - **Category:** Business

6. 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

7. 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

8. Proof of concept

```
GET https://www.syfe.com/security HTTP/1.1
host: www.syfe.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.syfe.com/sitemap.xml
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 06:16:24 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
CF-Ray: 9363f37e055132-CMB
CF-Cache-Status: HIT
Last-Modified: Thu, 24 Apr 2025 04:05:10 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Vary: Accept-Encoding
content-security-policy: frame-ancestors 'self'
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://npmcdn.com https://challenges.cloudflare.com
https://assets.syfe.com https://analytics.tiktok.com https://*.website-files.com/ https://unpkg.com https://cdn.jsdelivr.net https://cdnjs.cloudflare.com
https://*.cloudfront.net https://accounts.google.com https://appleid.cdn-apple.com https://www.gstatic.com https://www.redditstatic.com
https://www.google.com https://static.ads-twitter.com https://*.srv.stackadapt.com https://qvdt3feo.com https://*.g.doubleclick.net
https://*.google-analytics.com https://*.bing.com https://*.googletagmanager.com https://*.yahoo.com https://*.yahoodns.net https://*.yimg.com sp.
analytics.yahoo.com s.yimg.com https://fonts.gstatic.com https://www.google.com.hk https://www.google.com.au https://s.yimg.com https://www.buzzsprout.com
https://www.googleoptimize.com https://*.outbrain.com https://websdk.appsflyer.com https://calendly.com https://www.googleadservices.com
https://app.intercom.io https://widget.intercom.io https://js.intercomcdn.com https://www.youtube.com https://s.yimg.com http://static.hotjar.com
https://static.hotjar.com https://script.hotjar.com https://static.zdassets.com https://assets.calendly.com https://ekr.zdassets.com
https://syfe.zendesk.com wss://syfe.zendesk.com wss://*.zopim.com https://stats.g.doubleclick.net https://connect.facebook.net https://fast.wistia.com
https://optimize.google.com https://sjs.bizographics.com https://px.ads.linkedin.com https://tagmanager.google.com https://snap.lidn.com
https://amplify.outbrain.com https://cdn.taboola.com https://trc.taboola.com https://www.datadoghq-browser-agent.com
https://rum-http-intake.logs.datadoghq.eu https://api.smooch.io https://www.syfe.com https://stable-production-v1-www-assets-sync-bucket.s3.amazonaws.com;
img-src 'self' data: https://cdnjs.cloudflare.com https://assets.syfe.com https://*.website-files.com https://*.cloudfront.net
```

9. Proposed mitigation or fix

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