Cymetrics

ABC Company

2024 / Mar / 20

Exposure Assessment
Report

Table of Contents

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.

ABC Company

Scope

www.offices355.com

Scan Date

2024 / Mar / 20

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.

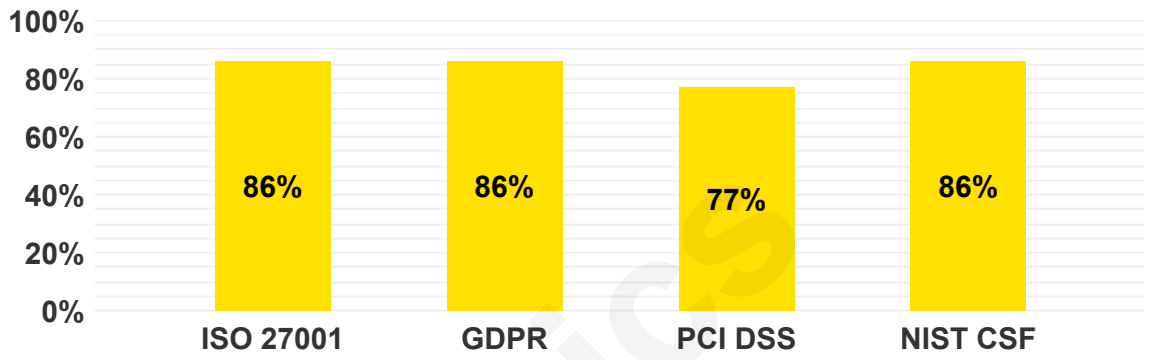
A B C D F

A+	External Service	Remote Control	Database	Remote Service	Blacklist
D	Web	Web Server	Web Application	Certificate	Domain
C-	Email	Email Service	DMARC	SPF	
A+	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.

Compliance

Compliance Percentage



Compliance Score

Cymetrics' compliance score is assessed by classifying the technical exposures and weaknesses according to the compliance standards, and then comprehensively considering the risk value and the proportion of the exposures and weaknesses in the technical aspects of the compliance standards. However, regarding to the level of compliance, besides considering the weaknesses from technical aspects, it is also necessary to consider the maturity of the management level. The percentage of this score cannot represent the completed level of compliance. It is recommended that compliance audits (for example, ISO 27001) are still required to be considered.

External Asset Inventory

The inventory of information assets that can be accessed externally under the same network domain is as follows. It is recommended that the company should assess information assets that have not yet undergone an exposure assessment to understand their possible cybersecurity risks.

Subdomains Accessed in This Report

www.offices355.com

List of Subdomains(Total:2 subdomains)

1. ctfd.offices355.com
2. outlook.offices355.com

Issue Summary

There are 21 vulnerabilities found in this scan session, including 3 high-risk, 12 medium-risk, and 6 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.

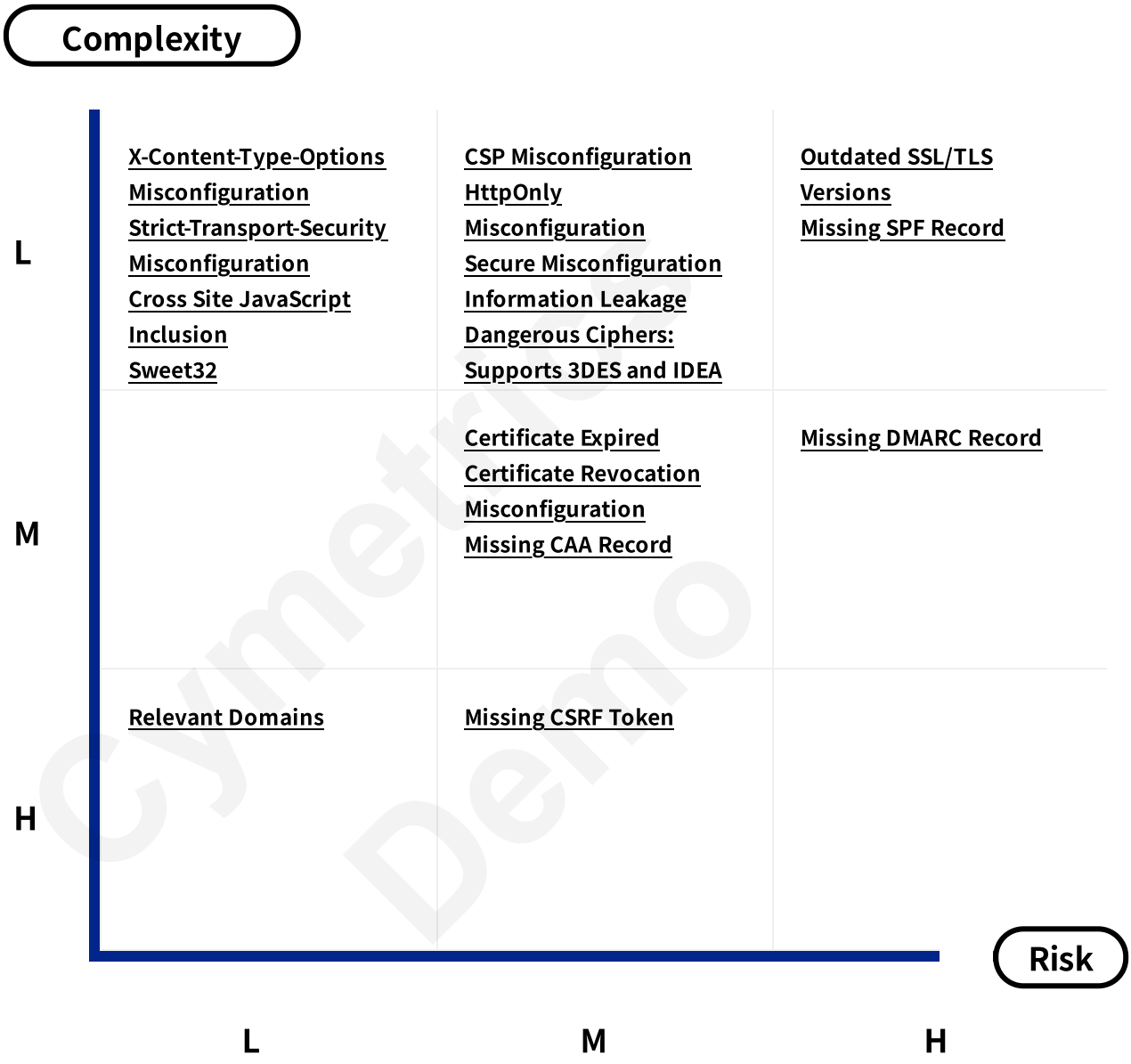
High Risk	Medium Risk	Low Risk
3	12	6

Vulnerability Comparison Chart

Vulnerability Comparison Chart

	Issue Gain or Loss	Last Scan ()
High	+3	0
Medium	+12	0
Low	+6	0

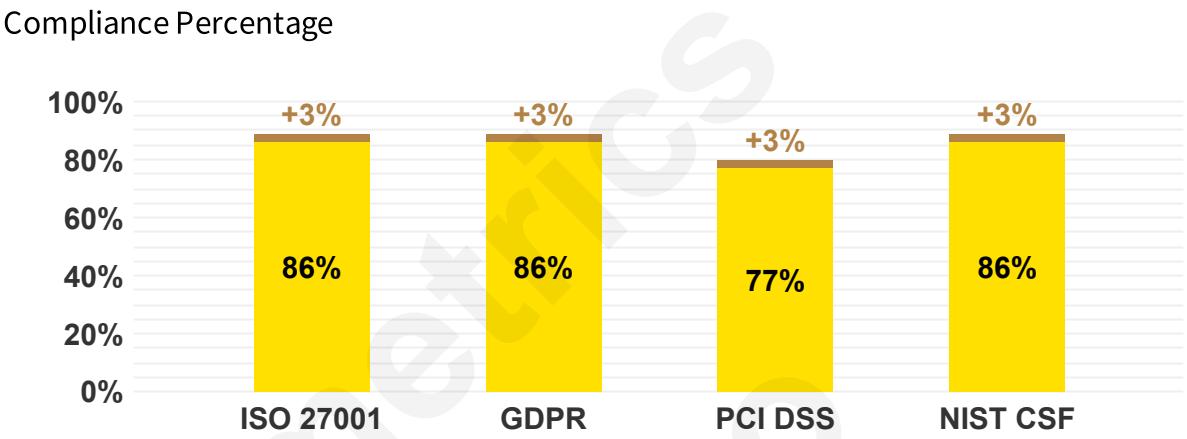
Risk Matrix



This cybersecurity rating improvement quadrant chart provides our customers with a reference for the priority order of cybersecurity rating improvement based on the two dimensions of risk and complexity. The company could mitigate or transfer the risks from the upper right (high risk and low complexity) items and further to the lower left corner (low risk and high complexity) items. Also, the company could choose to accept risks for the items in the lower left corner based on its own risk appetite.

Fix the following items can increase the cybersecurity rating and compliance score

D → C-

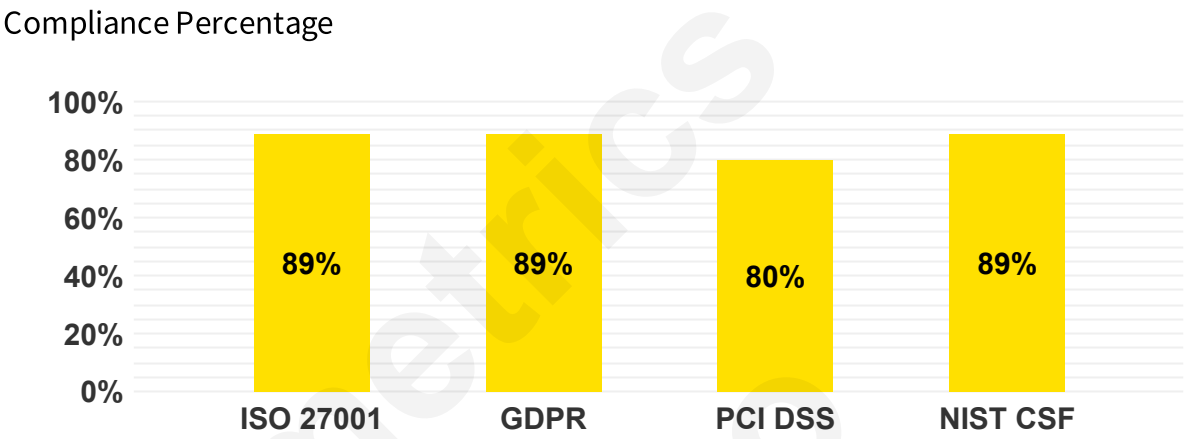


L M H

Category	Subcategory	Item	Risk	Complexity
Web	Certificate	Outdated SSL/TLS Versions	H	L

Fix the following items can increase the cybersecurity rating and compliance score

C- → C



L M H

M Web | Web Server | CSP Misconfiguration NEW

We detected that your website is missing Content Security Policy (CSP) headers, which may allow an adversary to inject malicious code into your website and steal potentially sensitive information or distribute malware. CSP is designed to reduce the attack surface of Cross Site Scripting (XSS) attacks and other code injection attempts.

We detected that your Content Security Policy (CSP) header 'style-src' is misconfigured to use the wildcard directive: '*', which permits loading files from arbitrary sources. This allows an adversary to inject malicious code into your website and steal potentially sensitive information or distribute malware.
CSP is designed to reduce the attack surface of Cross Site Scripting (XSS) attacks and other code injection attempts, but using dangerous directives may nullify the protections CSP provides.

We detected that your Content Security Policy (CSP) header 'style-src' is misconfigured to use unsafe directives: 'unsafe–inline' 'unsafe–eval'. This allows an adversary to inject malicious code into your website and steal potentially sensitive information or distribute malware.
CSP is designed to reduce the attack surface of Cross Site Scripting (XSS) attacks and other code injection attempts, but using dangerous directives may nullify the protections CSP provides.

L Suggestions

To mitigate this vulnerability, we suggest the following:
- Configure the HTTP Header 'Content-Security-Policy' to support Chrome 25 +,Firefox 23+ , and Safari 7
- Configure the HTTP Header 'X-Content-Security-Policy' to support Firefox 4.0+ , and Internet Explorer 10+
- Configure the HTTP Header 'X-WebKit-CSP' to support Chrome 14 + and Safari 6+

To mitigate this vulnerability, we suggest the following:
- Reconfigure your CSP header to use "Content-Security-Policy: default-src 'self';"

To mitigate this vulnerability, we suggest the following:
- Reconfigure your CSP header and remove "style-src: 'unsafe-inline'"
- Explicitly list trusted css style sources with: "style-src: 'self', https://csssecurityservices.com/"

For configuration steps, refer to:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/style-src

Targets

https://www.offices355.com/vulnerabilities/csp/ (script-src 'self' https://pastebin.com hastebin.com example.com code.jquery.com https://ssl.google-analytics.com ;)

https://www.offices355.com/vulnerabilities/csp/ (script-src 'self' https://pastebin.com hastebin.com example.com code.jquery.com https://ssl.google-analytics.com ;)

https://www.offices355.com/vulnerabilities/csp/ (script-src 'self' https://pastebin.com hastebin.com example.com code.jquery.com https://ssl.google-analytics.com ;)

https://www.offices355.com/vulnerabilities/csp/ (script-src 'self' https://pastebin.com hastebin.com example.com code.jquery.com https://ssl.google-analytics.com ;)

https://www.offices355.com/

https://www.offices355.com/instructions.php

https://www.offices355.com/setup.php

https://www.offices355.com/vulnerabilities/brute/

https://www.offices355.com/vulnerabilities/captcha/

https://www.offices355.com/vulnerabilities/csrf/

https://www.offices355.com/vulnerabilities/exec/

https://www.offices355.com/vulnerabilities/fi/?page=include.php

https://www.offices355.com/vulnerabilities/sqli/

https://www.offices355.com/vulnerabilities/sqli_blind/

https://www.offices355.com/vulnerabilities/upload/

https://www.offices355.com/

https://www.offices355.com/instructions.php

https://www.offices355.com/setup.php

https://www.offices355.com/vulnerabilities/brute/

https://www.offices355.com/vulnerabilities/captcha/

https://www.offices355.com/vulnerabilities/csrf/

https://www.offices355.com/vulnerabilities/exec/

https://www.offices355.com/vulnerabilities/fi/?page=include.php

https://www.offices355.com/vulnerabilities/sqli/

https://www.offices355.com/vulnerabilities/sqli_blind/

https://www.offices355.com/vulnerabilities/upload/

Related Compliance Items

PCI DSS

6. Develop and maintain secure systems and applications

L Web | Web Server | X-Content-Type-Options Misconfiguration NEW

[redacted]

L Suggestions

[redacted]

Targets

https://www.offices355.com/

https://www.offices355.com/instructions.php

https://www.offices355.com/robots.txt

https://www.offices355.com/setup.php

https://www.offices355.com/vulnerabilities/brute/

https://www.offices355.com/vulnerabilities/captcha/

https://www.offices355.com/vulnerabilities/csrf/

https://www.offices355.com/vulnerabilities/exec/

https://www.offices355.com/vulnerabilities/fi/?page=include.php

https://www.offices355.com/vulnerabilities/sqli/

https://www.offices355.com/vulnerabilities/sqli_blind/

https://www.offices355.com/vulnerabilities/upload/

Related Compliance Items

PCI DSS

6. Develop and maintain secure systems and applications

Methodology

The assessment was conducted by Cymetrics, a Cybersecurity - as - a - Service platform that automatically crawls the web applications and simulates the harmless penetration test. The test is based on NIST SP 800 - 115 Technical Guide to Information Security Testing and Assessment to identify following common vulnerabilities and weaknesses of the web applications:

MITRE ATT&CK

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Drive by Compromise
Exploit Public-Facing application
External Remote Service
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationships
Valid Accounts

CVSS: Common Vulnerability Scoring System v3.1: Specification Document

The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities. Its outputs include numerical scores indicating the severity of a vulnerability relative to other vulnerabilities.

CVSS is composed of three metric groups (Base, Temporal, and Environmental) :

1.The Base Score reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst case impact across different deployed environments.

2.The Temporal Metrics adjust the Base severity of a vulnerability based on factors that change over time, such as the availability of exploit code.

3.The Environmental Metrics adjust the Base and Temporal severities to a specific computing environment. They consider factors such as the presence of mitigations in that environment.

The benefits of CVSS include the provision of a standardized vendor and platform agnostic vulnerability scoring methodology. It is an open framework, providing transparency to the individual characteristics and methodology used to derive a score.

Compliance Standards Reference

Standards listed below were those we use as reference for Cymetrics' EAS scan.

- **ISO/IEC 27001 Third-edition 2022**
- **NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1**
- **2016/679 GDPR in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018**
- **PCI DSS Requirements and Testing Procedures Version 4.0 March 2022**

- ## ISO/IEC 27001 Third-edition 2022

  ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

  Cymetrics focus on guidance that aims to account data security, such as Protect all systems against malware, Develop and Maintain system and applications, Protect stored cardholder data and such. We recommend to refer to https://www.pcisecuritystandards.org/ for additional informations.

- ## NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

  The National Institute of Standards and Technology (NIST) launched this Framework for Improving Critical Infrastructure Cybersecurity has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

  Cymetrics focus on protection functions listed on the framework, such as Identity Management and Access Control, Awareness and Training, Data Security, Maintanence and such. We recommend to refer to https://www.nist.gov/cyberframework/framework for additional informations.

Compliance Standards Reference

- **2016/679 GDPR in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018**
  The General Data Protection Regulation (EU) (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.

  Cymetrics focus on Articles that aims to personal data security, such as Data Protection by Design and by Default, Responsibility of controller, Security of proccessing and etc. We recommend to refer to https://gdpr-info.eu/ for additional informations.

- **PCI DSS Requirements and Testing Procedures Version 4.0 March 2022**
  The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

  Cymetrics focus on guidance that aims to account data security, such as Protect all systems against malware, Develop and Maintain system and applications, Protect stored cardholder data and such. We recommend to refer to https://www.pcisecuritystandards.org/ for additional informations.