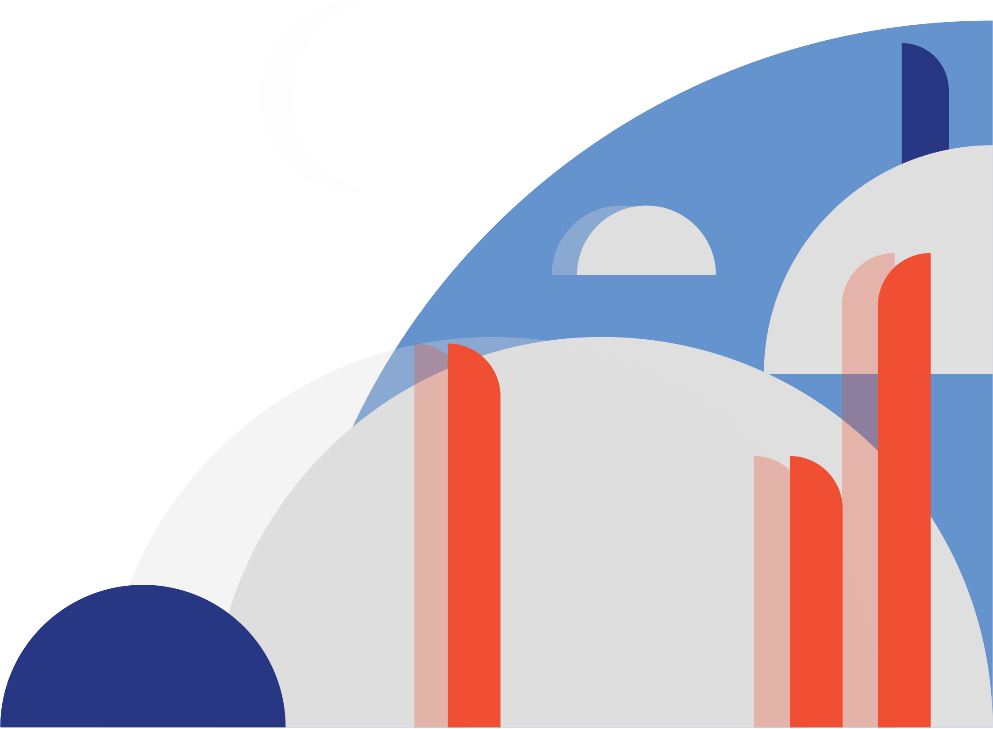
**Vulnerability Assessment Scanner**

**{{replace\_company}}**

**Website Vulnerability Report**

{{replace\_date\_2}}

1. Abstract

1.1. Detection Rules

**Vulnerability scan methods：**

Follow NIST 800-115 Technical Guide to Information Security Testing and Assessment.

**Vulnerability scan content：**

Based on NVD and CVE website related vulnerabilities, combined with the National Center for Cyber Security Technology (NCCST), the scan target is evaluated for known security vulnerabilities and compared to the Open Web Application Security Project(OWASP) criteria categorize the problems and finally make patch suggestions and report on the scan results.

**Vulnerability scanning tools：**

In addition to the self-developed Vulnerability Scanner, the VAS (Vulnerability Assessment as a Service) service integrates well-known scanning tools to verify weaknesses from multiple angles, thereby improving the accuracy of scans and providing more complete testing.

All tools have been updated to the latest version of {{replace\_date\_1}}, the following is the version information and tool introduction

1. Vulnerability Scanner:

Version: 1.0

Introduction: Combining OWASP TOP 10, CWE and CVE compliance standards with the latest security intelligence, we will complete automated and continuous vulnerability assessments more comprehensively and in depth.

2. OWASP ZAP:

Version: 2.11.1

Introduction: ZAP is a project led by the OWASP organization, the full name is OWASP Zed attack proxy, it is an open-source web application security scanner.

3. Nessus:

Version:10.1.2

Introduction: Nessus scans cover a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure.

1.2. Scope

**Date:** {{replace\_date\_2}}–{{replace\_date\_3}}

**Total:** 1 domain (only 1 target detected website)

|  |  |
| --- | --- |
| **Name** | **Target** |

1.3. Summary of Results

{{image\_score}}{{image\_dis}}

Table 2：Summary of risk information

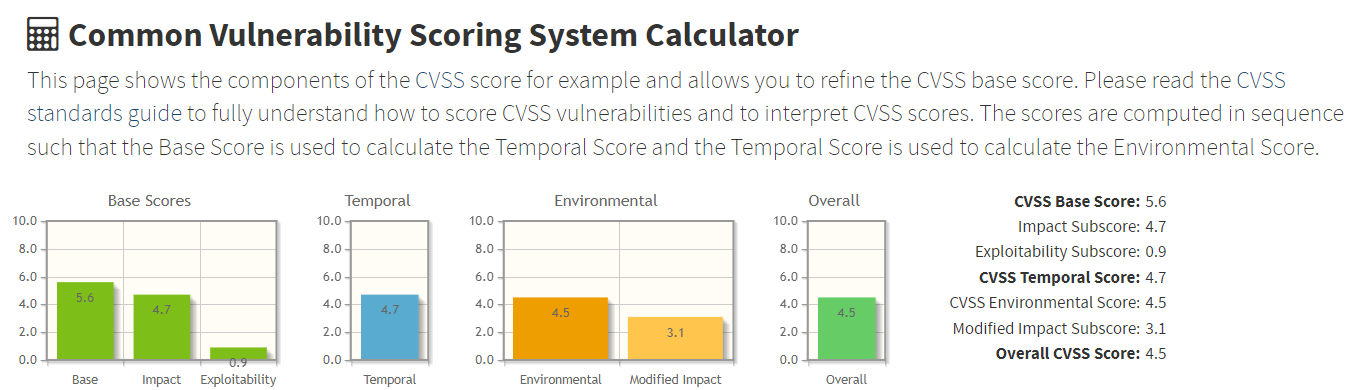
|  |  |  |
| --- | --- | --- |
| **Number** | **Risk Name** | **Risk Level** |

2. Scan results

2.1. Risk Assessment Methods

The risk assessment methodology is based on CVSSv3, a public set of evaluation criteria commissioned by the National Infrastructure Advisory Committee (NIAC) and often used to evaluate the security of enterprise information technology systems.

According to the CVSS scoring score, the vulnerability is divided into four levels, 1 to 3 is low risk, 4 to 6 is medium risk, 7 to 8 is high risk, and 9 to 10 is the highest risk, and suggested measures for various levels of problems.



|  |
| --- |
| Table 3：Risk Calculation Metrics |
| |  |  |  | | --- | --- | --- | | **Risk level** | **Score** | **Description** | | Low | 1~3 | Vulnerabilities that are less likely to be exploited or attacked do not require immediate remedial action. | | Medium | 4~6 | Important information is revealed that, combined with other identified risks. It recommended to continue to observe and plan for improvement. | | High | 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. | | Critical | 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. | |

2.2. Risk Category

The category method mainly refers to the latest version of OWASP Top 10. The Open Web Application Security Project (OWASP) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

The Open Web Application Security Project (OWASP) provides free and open resources. It is led by a non-profit called The OWASP Foundation. The OWASP Top 10 - 2021 is the published result of recent research based on comprehensive data compiled from over 40 partner organizations.

**Top 10 Web Application Security Risks**

**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**

2.3. Risk Description

# 3. Conclusion

{{image\_9}}

{{ replace\_summary}}

4. References

[1] CVE(https://cve.mitre.org/)

[2] NIST(https://www.nist.gov/)

[3] NVD(https://nvd.nist.gov/)

[4] OWASP(https://owasp.org/)