Security Assessment Report

Comprehensive Web Application Security Analysis

Target Application
https://mrisa.xyz

Report Generated
2026-02-19 18:58:32

Scanner
Defendrix v1.0

Total Findings
2

Executive Summary

This security assessment identified **2 security findings** across the target application. The overall risk level is classified as **MEDIUM**.

Severity Distribution

Critical	High	Medium
0	0	1

0	1
Low	Informational

Key Recommendations

- Implement input validation and output encoding across all user inputs
- Configure security headers according to OWASP recommendations
- Conduct regular security assessments and penetration testing
- Implement a Web Application Firewall (WAF)
- Train development team on secure coding practices

📊 Attack Surface Analysis

The attack surface represents all possible entry points that could be exploited by an attacker. A larger attack surface increases the potential for vulnerabilities.

1
Endpoints Discovered

0
Parameters Identified

0
Forms Detected

0
Input Vectors Found

🎯 OWASP Top 10 2021 Mapping

Findings categorized according to the OWASP Top 10 2021 security risk classification framework.

A05: Security Misconfiguration

OWASP security vulnerability category.

Findings Count: 1

- Security Headers - Medium severity at https://mrisa.xyz

A08: Software and Data Integrity Failures

OWASP security vulnerability category.

Findings Count: 1

- Threat Intelligence - Informational severity at https://mrisa.xyz

Medium Severity Findings (1)

🔍 Security Headers

Medium

OWASP Category: A05: Security Misconfiguration

Confidence: High%

Affected Endpoint: https://mrisa.xyz

Description:

Missing security headers: X-Frame-Options, Content-Security-Policy, X-Content-Type-Options.

Detection Source: ActiveScan

💡 Vulnerability Details

Impact: Requires assessment

Security vulnerability identified.

🔧 Remediation Steps

- Review finding details
- Consult OWASP guidelines
- Implement security best practices

📚 References & Resources

- OWASP Top 10
- Security best practices documentation

Informational Severity Findings (1)

🔍 Threat Intelligence

Informational

OWASP Category: A08: Software and Data Integrity Failures

Confidence: Low%

Affected Endpoint: https://mrisa.xyz

Description:

External Threat Intelligence: 0 security vendors flagged this URL as malicious, 2 flagged as suspicious. Total scanners: 95. ⚠️ This URL may pose a security risk.

Detection Source: ThreatIntel

💡 Vulnerability Details

Impact: Variable - Depends on threat severity and context.

External threat intelligence indicates potential security risks associated with the target.

🔧 Remediation Steps

- Investigate flagged URLs and domains thoroughly
- Review and validate all external dependencies
- Implement regular threat intelligence monitoring
- Apply security patches and updates promptly
- Consider domain/URL reputation in security policies
- Implement network-level blocking if necessary

📚 References & Resources

- OWASP Threat Modeling
- NIST Cybersecurity Framework
- MITRE ATT&CK Framework

Generated by Defendrix - Advanced Web Application Security Scanner
This report follows OWASP Testing Guide v4.2 methodology and OWASP Top 10 2021 classifications

For questions or support, consult OWASP documentation at owasp.org