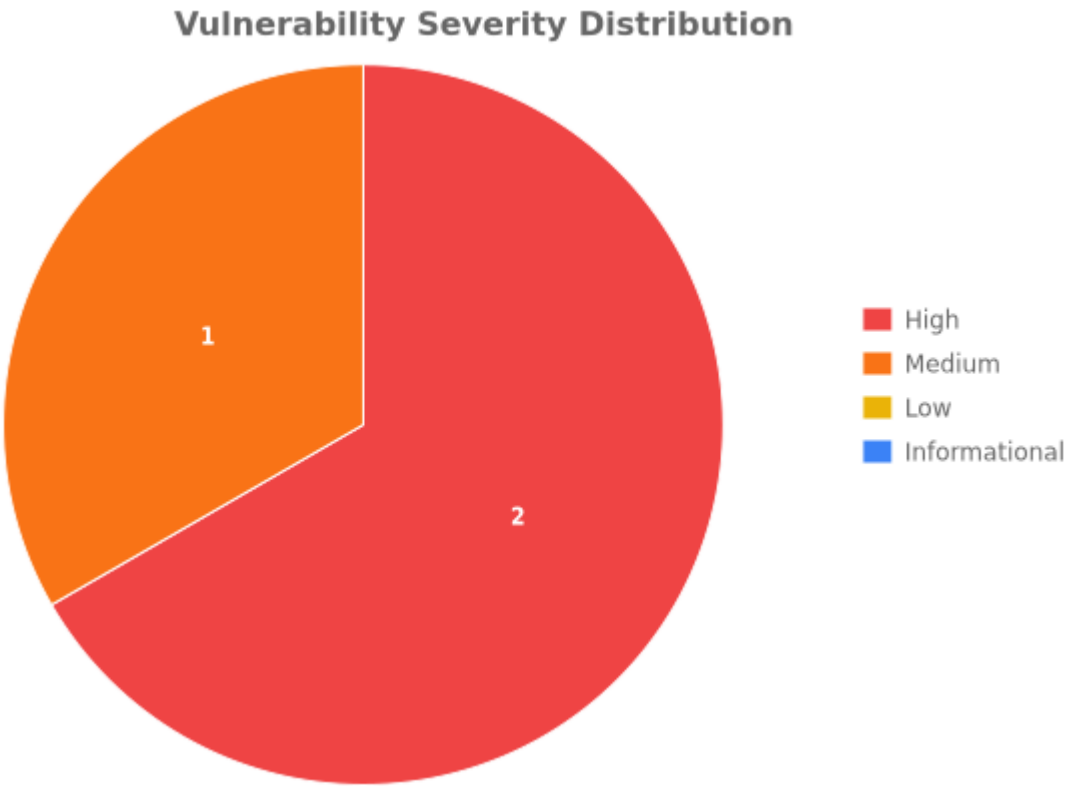
Security Vulnerability Report

Target: https://www.genesisengr.com/

Scan Date: 5/8/2025, 7:50:52 PM

Vulnerability Statistics



Summary of Findings

Severity	
High	**2**
Medium	**1**
Low	**0**
Informational	**0**

Server-Side Request Forgery (HIGH)

Description: Server-Side Request Forgery (SSRF) Test Results:
Target URL: https://www.genesisengr.com/?url=http%3A%2F%2F169.254.169.254%2F
Parameter tested: url
Payload used: http://169.254.169.254/

POTENTIAL VULNERABILITY DETECTED!
The application may be vulnerable to SSRF attacks.
Patterns detected that suggest successful SSRF:
- service_response

Response Status Code: 200
Response Length: 20950 characters

Response Snippet (first 500 chars):
<!DOCTYPE html>Ð
<html lang="en">Ð
Ð
<head>Ð
  <meta charset="UTF-8" />Ð
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />Ð
  <meta name="description" content="Welcome to Genesis Engineering - your trusted partner for exceptional solutions. Our passionate experts use cutting-edge technology and innovative methodologies to elevate your projects to success. From structural design to environmental assessments, we deliver results that surpass expectations. Experience the dif...

Location: https://www.genesisengr.com/

Enhanced analysis not available for this vulnerability.

Technical Proof of Concept

Risk Analysis

Impact Level: high
Business Impact: Critical business impact with potential for data breach or system compromise

Missing HSTS Header (HIGH)

Description: The strict-transport-security security header is missing

Location: https://www.genesisengr.com/

Enhanced analysis not available for this vulnerability.

Technical Proof of Concept

Risk Analysis

Impact Level: high
Business Impact: Critical business impact with potential for data breach or system compromise

Missing X-Frame-Options Header (MEDIUM)

Description: The x-frame-options security header is missing

Location: https://www.genesisengr.com/

Enhanced analysis not available for this vulnerability.

Technical Proof of Concept

Risk Analysis

Impact Level: medium
Business Impact: Moderate risk that could lead to service disruption or information disclosure

Disclaimer

This report is provided for informational purposes only. The findings in this report are based on automated scans and may include false positives or miss certain vulnerabilities. It is recommended to verify all findings manually before taking action. The creators of this report are not responsible for any damages that may arise from the use of this information. Always follow ethical hacking practices and obtain proper authorization before testing any systems.

Report generated on 5/8/2025, 7:50:59 PM