External Cyber Threat Analysis

Live security assessment for ng

55.1 MEDIUM RISK

Scanned: July 15, 2025

10	0	F	
Active Vulnerabilities	Open Ports	Web Security Grade	

2 Medium Risk Vulnerabilities

Unknown Vulnerability - HSTS header missing (HTTPS only)

Unknown Vulnerability - HTTP used for potentially sensitive content (consider H

⚠ Critical Security Gaps Discovered

Email Security Weakness

DKIM: ✗, DMARC policy: none - vulnerable to email spoofing and phishing attacks

DNS Security Gap

DNSSEC not enabled - vulnerable to DNS spoofing, cache poisoning, and traffic redirection attacks

Web Application Exposure

7 missing critical security headers create exposure to XSS, clickjacking, and content injection attacks across all endpoints

Information Disclosure

Server type (Microsoft-IIS/10.0) and infrastructure details exposed, providing attackers with reconnaissance intelligence

🚨 Immediate Action Required

These vulnerabilities are being actively scanned by cybercriminals daily. Your exposed infrastructure with missing email authentication and web security headers makes you an immediate target for phishing campaigns and web-based attacks.