Web Security Scan Report

This report summarizes the findings of the security scan conducted on http://192.168.78.43:5000. The scan included vulnerability testing, subdomain discovery, and security header analysis. Below are the detailed results and recommendations.

Vulnerabilities Found

Type	URL	Parameter	Severity	CVSS	CWE
Missing Security Header	http://192.168.78.43:5000	Strict-Transport-Security	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	X-Frame-Options	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	X-Content-Type-Options	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	Content-Security-Policy	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	X-XSS-Protection	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	Referrer-Policy	Medium	5.0	CWE-693
Missing Security Header	http://192.168.78.43:5000	Permissions-Policy	Medium	5.0	CWE-693

Recommendations for Vulnerabilities

Vulnerability: Missing Security Header
Description: Missing Strict-Transport-Security header: Ensures secure HTTPS connections
Recommendation: Add the Strict-Transport-Security header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing X-Frame-Options header: Prevents clickjacking attacks
Recommendation: Add the X-Frame-Options header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing X-Content-Type-Options header: Prevents MIME-type sniffing
Recommendation: Add the X-Content-Type-Options header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing Content-Security-Policy header: Controls resource loading
Recommendation: Add the Content-Security-Policy header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing X-XSS-Protection header: Provides XSS filtering
Recommendation: Add the X-XSS-Protection header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing Referrer-Policy header: Controls referrer information
Recommendation: Add the Referrer-Policy header with appropriate values
Proof of Concept: N/A

Vulnerability: Missing Security Header
Description: Missing Permissions-Policy header: Controls browser features
Recommendation: Add the Permissions-Policy header with appropriate values
Proof of Concept: N/A

General Security Recommendations

General Recommendations:
1. Implement all missing security headers.
2. Conduct regular security header audits.
3. Use HTTPS across all pages and subdomains.
4. Maintain a minimal attack surface by disabling unused features.
5. Monitor security headers using tools like SecurityHeaders.com.