Vulnerability Scan Report

SEO Intrusion Detection System

Scan Summary

Site URL: https://szabist-isb.edu.pk/
Scan Date: 26/10/2025, 20:32:31
Scan Duration: N/A
Total Vulnerabilities: 6
Status: Completed

Severity Breakdown

%Ï Critical: 1
%Ï High: 2
%Ï Medium: 2
%Ï Low: 1

Detailed Findings

1. Weak Password

Severity: Critical
Description: Weak password policy detected. Common passwords may be accepted.
Affected: Authentication System
' Recommendation: Enforce strong password policy: minimum 12 characters, uppercase, lowercase, numbers, and special characters. Implement account lockout after failed attempts.
& þ   PUBLIC EXPLOIT AVAILABLE - PATCH IMMEDIATELY

2. Plugin Vulnerability

Severity: High
Description: WordPress plugins detected. Some may be outdated or vulnerable.
Affected: WordPress Plugins
' Recommendation: Update all plugins and remove unused ones. Use security plugins like Wordfence.

3. Weak Password

Severity: High
Description: Admin login page exposed at /admin. Vulnerable to brute force attacks.
Affected: Admin Panel
' Recommendation: Implement rate limiting, CAPTCHA, and two-factor authentication. Use a custom admin URL.

4. Misconfiguration

Severity: Low

Description: Technology stack exposed: PHP/7.4.32, ASP.NET

Affected: PHP/Server Configuration

' Recommendation: Remove X-Powered-By header to hide technology stack.

5. Security Headers

Severity: Medium

Description: Missing Content-Security-Policy header. No protection against XSS attacks.

Affected: HTTP Headers

' Recommendation: Implement Content-Security-Policy to prevent XSS and data injection attacks.

6. Security Headers

Severity: Medium

Description: Missing X-XSS-Protection header.

Affected: HTTP Headers

' Recommendation: Add 'X-XSS-Protection: 1; mode=block' header (legacy browsers).