Source Code Inspection Report

ProjectName: 綠色數位行為淨零發展計畫成果展示網站之程式原始碼掃描 **Language:** PHP

Ruleset: PHP OWASP Top 10 2021 **Analyze Date:** 2024.11.28 11:01:28

Summary

File Count :	178
LOC :	10,125
Detected Files :	0
Detected Rules :	0
Detected Rules Count:	0

Detected Files by Priority		Detected Rules by Priority	
Critical	0	Critical	0
Rec.-High	0	Rec.-High	0
Rec.-Middle	0	Rec.-Middle	0
Rec.-Low	0	Rec.-Low	0
Info.	0	Info.	0

Inspection Result

Priority	Category	Rule	Defect	Source File
Critical	Data Handling	[SP] Cross-Site Scripting (XSS)	0	0
Critical	Data Handling	[SP] LDAP Injection	0	0
Critical	Data Handling	[SP] OS Command Injection	0	0
Critical	Data Handling	[SP] Path Traversal	0	0
Critical	Data Handling	[SP] Reliance on DNS Lookups in a Security Decision	0	0
Critical	Data Handling	[SP] SQL Injection	0	0
Critical	Data Handling	[SP] Use of Hard-coded Password	0	0
Critical	Data Handling	[SP] Use of a Broken or Risky Cryptographic Algorithm	0	0
Critical	Data Handling	[SP] XML External Entity Attack (XXE Attack)	0	0
Critical	Poor Code Quality Indicator	[SP] Deserialization of Untrusted Data	0	0
Critical	Security Functions	[SP] Cookie Security: Overly Broad Domain	0	0
Critical	Security Functions	[SP] Empty Password in Configuration File	0	0
Critical	Security Functions	[SP] Improper Authorization	0	0
Rec.-High	Data Handling	[SP] HTTP Response Splitting	0	0
Rec.-High	Data Handling	[SP] Transport Confidential Information in Plain Text	0	0
Rec.-High	Data Handling	[SP] Use of Hard-Coded Cryptographic Key	0	0
Rec.-High	Data Handling	[SP] XPath Injection	0	0
Rec.-High	Data Handling	[SP] XQuery Injection	0	0
Rec.-High	Security Functions	[SP] Cleartext Storage of Sensitive Information	0	0
Rec.-High	Security Functions	[SP] Inadequate Encryption Strength	0	0
Rec.-High	Security Functions	[SP] Information Exposure Through Comments	0	0
Rec.-High	Security Functions	[SP] Sensitive Cookie Without 'HttpOnly' Flag	0	0
Rec.-High	Security Functions	[SP] Sensitive cookie in HTTPS Session without Secure Attribute	0	0
Rec.-High	Security Functions	[SP] Weak Password Requirements	0	0

Rec.–Middle	API Abuse	[SP] Use of Potentially Dangerous Function	0	0
Rec.–Middle	Data Handling	[SP] Use of a One-Way Hash without a Salt	0	0
Rec.–Middle	Security Functions	[SP] Improper Restriction of Excessive Authentication Attempts	0	0
Rec.–Middle	Security Functions	[SP] Missing Authentication for Critical Function	0	0
Rec.–Low	Data Handling	[SP] Use of Externally-Controlled Format String	0	0

Detected Files Info

File	Path	Defects
		0

Detailed Inspection Results

Rule Name:				Priority:	
Category:		Defect:		Source File:	
Rule Desc:					
Bad Code:					
Good Code:					

Violation File:	Line: