

<https://linuxer.name/> 스캔 결과

스캔 상세정보

스캔 정보	
시작 시간	30/01/2020, 12:09:34
대상 URL	https://linuxer.name/
Host	https://linuxer.name/
소요 시간	245 minutes, 19 seconds
Profile	Full Scan

위험수준

취약점 위험도 Level 2

취약점점검에서 하나이상의 중간 위험도의 취약점이 발견되었습니다. 취약점을 확인하여 더 심각한 문제가 발생하지 않도록 보완해야합니다.

취약점 현황

Total	129
❗ High	0
❗ Medium	4
ⓘ Low	10
ⓘ Informational	115

취약점 요약정보

! Error message on page

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200
영향을 받은 항목	Variation
/manual/howto/cgi.html	1

! HTML form without CSRF protection

분류	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352
영향을 받은 항목	Variation
Web Server	1

! Vulnerable Javascript library

분류	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-16
영향을 받은 항목	Variation
/wp-includes/js/jquery/jquery.js	1

! Clickjacking: X-Frame-Options header missing

분류	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693
영향을 받은 항목	Variation
Web Server	1

! Cookie(s) without HttpOnly flag set

분류	
	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None