

https://linuxer.name/ 스캔 결과

스캔 상세정보

스캔 정보	
시작시간	10/01/2020, 09:55:05
대상 URL	https://linuxer.name/
Host	https://linuxer.name/
소요시간	260 minutes, 18 seconds
Profile	Full Scan

위험수준

취약점 위험도 Level 3

취약점 점검에서 하나 이상의 높은 위험도의 취약점이 발견되었습니다. 악의적인 사용자가 발견된 취약점을 이용하여 웹사이트나 데이터베이스에 영향을 줄수 있습니다.

취약점 현황

Total	129
 High	1
 Medium	5
 Low	11
 Informational	112

! Insecure CORS configuration

분류		
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium 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	
영향을받은 항목		Variation
/wp-json/oembed/1.0/embed		1

! .htaccess file readable

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	
CWE	CWE-16	
영향을받은 항목		Variation
Web Server		1

! 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
/2020/01/gcp-google-kubernetes-engine	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