nessus®

vulnerability Assessment Project

Vulnerabilities by Host

Vulnerabilities by Host

testphp.vulnweb.com

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	13	16	2	28
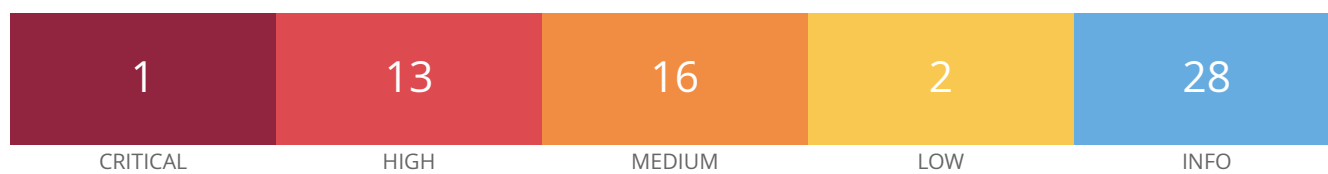
Vulnerabilities   Total: 60

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	7.5	17797	PHP 5.x < 5.2.2 Multiple vulnerabilities
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	25368	PHP < 5.2.3 Multiple Vulnerabilities
HIGH	7.5*	11139	CGI Generic SQL Injection
HIGH	7.5*	42479	CGI Generic SQL Injection (2nd pass)
HIGH	7.5*	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	7.5*	31649	PHP 5.x < 5.2 Multiple Vulnerabilities
HIGH	7.5*	24907	PHP < 5.2.1 Multiple Vulnerabilities
HIGH	7.5*	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	32123	PHP < 5.2.6 Multiple Vulnerabilities
HIGH	7.5*	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5*	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	57537	PHP < 5.3.9 Multiple Vulnerabilities
MEDIUM	5.3	40984	Browsable Web Directories
MEDIUM	5.3	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	4.3*	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	49067	CGI Generic HTML Injections (quick test)

MEDIUM	4.3*	39466	CGI Generic XSS (quick test)
MEDIUM	5.1*	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	6.8*	43351	PHP < 5.2.12 Multiple Vulnerabilities
MEDIUM	6.8*	25971	PHP < 5.2.4 Multiple Vulnerabilities
MEDIUM	4.4*	28181	PHP < 5.2.5 Multiple Vulnerabilities
MEDIUM	5.0*	35750	PHP < 5.2.9 Multiple Vulnerabilities
MEDIUM	6.8*	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4*	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	4.3*	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	5.0*	44670	Web Application SQL Backend Identification
LOW	N/A	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	47830	CGI Generic Injectable Parameter
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	39470	CGI Generic Tests Timeout
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	49704	External URLs
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header

INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	49705	Web Server Harvested Email Addresses
INFO	N/A	72427	Web Site Client Access Policy File Detection
INFO	N/A	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	10662	Web mirroring
INFO	N/A	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown