wissem_nasri

Report generated by Nessus™ Wed, 20 Mar 2024 03:05:34 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

testphp.vulnweb.com

1	14	16	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 54

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	7.5	6.6	17797	PHP 5.x < 5.2.2 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	6.7	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*	-	43160	CGI Generic SQL Injection (blind, time based)
HIGH	7.5*	6.7	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	7.5*	6.7	31649	PHP 5.x < 5.2 Multiple Vulnerabilities
HIGH	7.5*	6.7	24907	PHP < 5.2.1 Multiple Vulnerabilities
HIGH	7.5*	6.7	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	8.4	32123	PHP < 5.2.6 Multiple Vulnerabilities
HIGH	7.5*	6.3	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5*	8.9	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	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*	4.4	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	43351	PHP < 5.2.12 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	25971	PHP < 5.2.4 Multiple Vulnerabilities
MEDIUM	4.4*	6.7	28181	PHP < 5.2.5 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	35750	PHP < 5.2.9 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4*	5.3	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	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	-	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	-	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	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
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