Web Application Tests MS2

Report generated by Nessus™ Thu, 22 Feb 2024 20:22:49 IST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.2.5

Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	9.8	-	70728	Apache PHP-CGI Remote Code Execution
HIGH	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	9.8	-	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
HIGH	8.8	-	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	-	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	-	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	-	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	11411	Backup Files Disclosure
MEDIUM	4.3*	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	5.0*	-	57640	Web Application Information Disclosure

MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	-	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3*	-	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
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	-	19941	TWiki Detection
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	85601	Web Application Cookies Not Marked HttpOnly

INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
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	-	11419	Web Server Office File Inventory
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	17219	phpMyAdmin Detection

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