tenable Nessus

Report generated by Nessus™

Lab1 OWASP Web

Wed, 17 Apr 2024 22:27:01 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.0.2.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	5	24	4	40

Severity	CVSS v3.0	VPR Score	Plugin	Name

CRITICAL	9.8	4.9	15780	phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
HIGH	8.3	-	122584	SQLi scanner
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	-	42479	CGI Generic SQL Injection (2nd pass)
HIGH	7.5*	6.7	11938	phpBB < 2.0.7 Multiple Script SQL Injection
HIGH	7.5*	-	13655	phpBB < 2.0.9 Multiple Vulnerabilities
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.7	-	42982	AWStats < 6.95 awredir.pl Arbitrary Site Redirect
MEDIUM	5.0*	-	35975	AWStats 'awstats.pl' Path Disclosure
MEDIUM	4.3*	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	44134	CGI Generic Unseen Parameters Discovery
MEDIUM	6.8*	-	46196	CGI Generic XML Injection

MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	65702	Git Repository Served by Web Server
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	5.0*	-	44670	Web Application SQL Backend Identification
MEDIUM	5.0*	-	29745	WordPress 'query.php' is_admin() Function Information Disclosure
MEDIUM	5.0*	2.5	24237	WordPress Pingback File Information Disclosure
MEDIUM	4.3*	4.7	13840	phpBB < 2.0.10 Multiple XSS
MEDIUM	5.0*	3.7	17205	phpBB <= 2.0.11 Multiple Vulnerabilities
MEDIUM	6.5*	6.6	17301	phpBB <= 2.0.13 Multiple Vulnerabilities
MEDIUM	4.3*	6.0	18124	phpBB <= 2.0.14 Multiple Vulnerabilities
MEDIUM	4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
LOW	3.5*	2.7	18626	phpBB < 2.0.17 Nested BBCode URL Tags XSS
INFO	N/A	-	35974	AWStats Detection

INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	40406	CGI Generic Tests HTTP Errors
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	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
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	-	106658	JQuery Detection
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	-	57323	OpenSSL Version Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	40665	Protected Web Page 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	-	51080	Web Server Uses Basic Authentication over HTTPS
INFO	N/A	-	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	18297	WordPress Detection
INFO	N/A	-	101841	WordPress Outdated Plugin Detection

INFO	N/A	-	101842	WordPress Plugin Detection
INFO	N/A	-	15779	phpBB Detection
INFO	N/A	-	17219	phpMyAdmin Detection

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

Hide