

Report Summary - SAMPLE

Scan Start Date 2009-10-02 21:40:02 EST
 Scan End Date 2009-10-02 22:17:06 EST
 Report Date 2009-11-02 22:27:19 EST
 ASPL Version 320
 Target IPs - 167.11.33.21



This is a sample PCI compliance report, which is generated only for the purpose of evaluating the Merchant Safe PCI Scan capabilities and in no way constitutes a certification that the networks scanned are either compliant or non-compliant with the PCI data security initiative's requirements.

Merchant Safe has determined that test would be **NOT COMPLIANT** with the PCI scan validation requirements had this been an authoritative assessment from an actual SCAN.

Vulnerability Name	Vulnerability ID	IP Address	Protocol/Port	Amendment Status
Apache Remote Username Enumeration Vulnerability	1854	167.11.33.21	tcp/8880	Required
Apache Remote Username Enumeration Vulnerability	1854	167.11.33.21	tcp/8443	Required
Multiple Linux Vendor rpc.statd Remote Format String Vulnerability	2243	167.11.33.21	tcp/955	Required
Multiple Linux Vendor rpc.statd Remote Format String Vulnerability	2243	167.11.33.21	udp/952	Required
Multiple Vendor rpc.statd Arbitrary File Creation / Deletion Vulnerability	2247	167.11.33.21	tcp/955	Required
MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability	2995	167.11.33.21	tcp/3306	Required
Apache Web Server ETag Header Information Disclosure Weakness	3267	167.11.33.21	tcp/80	Required
Apache Web Server ETag Header Information Disclosure Weakness	3267	167.11.33.21	tcp/443	Required
Sun XDR Library Available	3981	167.11.33.21	tcp/111	Required
Sun XDR Library Available	3981	167.11.33.21	udp/111	Required
SSL Server Supports Weak Encryption	6174	167.11.33.21	tcp/995	Required
SSL Server Supports Weak Encryption	6174	167.11.33.21	tcp/8443	Required
Apache Expect Header Cross-Site Scripting Vulnerability	6463	167.11.33.21	tcp/8443	Required

Apache Expect Header Cross-Site Scripting Vulnerability	6463	167.11.33.21	tcp/8880	Required
SSLv2 Enabled	6766	167.11.33.21	tcp/443	Required
SSLv2 Enabled	6766	167.11.33.21	tcp/465	Required
MySQL Rename Table Function Access Validation Vulnerability	10441	167.11.33.21	tcp/3306	Required
BIND 9 OpenSSL 'DSA_verify' Function Signature Verification Vulnerability	14510	167.11.33.21	udp/53	Required
BIND DNS Protocol Insufficient Transaction ID Randomization DNS Spoofing Vulnerability	14511	167.11.33.21	udp/53	Required
BIND 'inet_network()' Off-by-One Buffer Overflow Vulnerability	14512	167.11.33.21	udp/53	Required
MySQL MyISAM Table Privileges Security Bypass Vulnerability (III)	14529	167.11.33.21	tcp/3306	Required
PHP 'imagemagick' Buffer Overflow Vulnerability	14555	167.11.33.21	tcp/8880	Required
PHP 'memnstr' Buffer Overflow Vulnerability	14556	167.11.33.21	tcp/8443	Required
PHP 'memnstr' Buffer Overflow Vulnerability	14556	167.11.33.21	tcp/8880	Required
PHP ZipArchive::extractTo() '.zip' Files Directory Traversal Vulnerability	14559	167.11.33.21	tcp/8443	Required
PHP ZipArchive::extractTo() '.zip' Files Directory Traversal Vulnerability	14559	167.11.33.21	tcp/8880	Required
PHP 'mbstring' Extension Buffer Overflow Vulnerability	14560	167.11.33.21	tcp/8443	Required
PHP 'mbstring' Extension Buffer Overflow Vulnerability	14560	167.11.33.21	tcp/8880	Required
PHP 'error_log' Safe Mode Restriction-Bypass Vulnerability	14561	167.11.33.21	tcp/8443	Required
PHP 'error_log' Safe Mode Restriction-Bypass Vulnerability	14561	167.11.33.21	tcp/8880	Required
PHP SAPI 'php_getuid()' Safe Mode Restriction-Bypass Vulnerability	14563	167.11.33.21	tcp/8443	Required
PHP SAPI 'php_getuid()' Safe Mode Restriction-Bypass Vulnerability	14563	167.11.33.21	tcp/8880	Required
PHP 5 'posix_access()' Function 'safe_mode' Bypass Directory Traversal Vulnerability	14568	167.11.33.21	tcp/8443	Required
PHP 5 'posix_access()' Function 'safe_mode'	14568	167.11.33.21	tcp/8880	Required

Bypass Directory Traversal Vulnerability				
PHP 'chdir()' and 'ftok()' 'safe_mode' Multiple Security Bypss Vulnerabilities	14569	167.11.33.21	tcp/8443	Required
PHP 'chdir()' and 'ftok()' 'safe_mode' Multiple Security Bypss Vulnerabilities	14569	167.11.33.21	tcp/8880	Required
PHP 'php_imap.c' Code Execution Vulnerability	14573	167.11.33.21	tcp/8443	Required
PHP 'php_imap.c' Code Execution Vulnerability	14573	167.11.33.21	tcp/8880	Required
PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability	14714	167.11.33.21	tcp/8443	Required
PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability	14714	167.11.33.21	tcp/8880	Required
PHP 'popen()' Function Buffer Overflow Vulnerability	14715	167.11.33.21	tcp/8443	Required
PHP 'popen()' Function Buffer Overflow Vulnerability	14715	167.11.33.21	tcp/8880	Required
PHP 'proc_open()' Environment Parameter Safe Mode Restriction-Bypass Vulnerability	14717	167.11.33.21	tcp/8443	Required
PHP 'proc_open()' Environment Parameter Safe Mode Restriction-Bypass Vulnerability	14717	167.11.33.21	tcp/8880	Required
PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability	21405	167.11.33.21	tcp/8443	Required
PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability	21405	167.11.33.21	tcp/8880	Required
MySQL 'sql_parse.cc' Multiple Format String Vulnerability	22037	167.11.33.21	tcp/3306	Required

NEXT STEPS:

The above list contains some of the vulnerabilities found during your FREE PCI Scan. In order to get a comprehensive list of all security threats on your domain/IP, please follow the steps below.

1. Signup for a Merchant Safe PCI Scan package.
2. Your Business verification processes starts.
3. A detailed security verification / PCI Scan of your IP/domain is conducted.
4. Receive detailed Report with solutions to fix them, in the event of a failed test.
5. Receive and display Merchant Safe Security Seal. (Clicking on the seal will display additional scan details)
6. Optional Bank submission - Receive the PCI scan pass report, along with SAQ (pdf), and submit to bank.

Scanning will be done daily or quarterly based on the package you selected.

Your detailed report will have each of these vulnerabilities listed along with solutions to fix them. In most cases the solution will have the description of the problem, how to fix it, along with links to the patch/fix downloads. If you are on a shared hosting account or have a dedicated server managed by your hosting provider, you will need to contact your webhosting company and have them install the patches and fix the issues, prior to attempting a re-scan of the IPs.