COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Vin65	ASV Company:	Comodo CA Limited
Date scan was completed:	12/18/2016	Scan expiration date:	03/18/2017

Part 2. Component Compliance Summary

IP Address : www.vin65.com Pass Fail

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.vin65.com	CGI Generic SQL Injection (HTTP Headers) 443 / tcp / www	High	7.5	Pass	The vulnerability is not present after inspection and testing
www.vin65.com	CGI Generic SQL Injection (HTTP Headers) 80 / tcp / www	High	7.5	Pass	The vulnerability is not present after inspection and testing
www.vin65.com	Web Server Uses Plain Text Authentication Forms 80 / tcp / www	Low	2.6	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Cookies Not Marked HttpOnly 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Cookies Not Marked HttpOnly 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Harvested Email Addresses 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.vin65.com	Web Server Harvested Email Addresses 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Allows Password Auto-Completion 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Allows Password Auto-Completion 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Inconsistent Hostname and IP Address 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server robots.txt Information Disclosure 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server robots.txt Information Disclosure 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Cookies Not Marked Secure 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Cookies Not Marked Secure 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	OS Identification 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.vin65.com	OpenSSL Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Sitemap 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Sitemap 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Server Type and Version 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Server Type and Version 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server No 404 Error Code Check 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Nessus SYN scanner 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Nessus SYN scanner 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Tests Load Estimation (all tests) 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Tests Load Estimation (all tests) 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Device Type 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.vin65.com	Service Detection 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HyperText Transfer Protocol (HTTP) Redirect Information 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Certificate Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Injectable Parameter 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Office File Inventory 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Injectable Parameter 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Modify the affected CGI scripts so that they properly escape arguments.
Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
Fix the reverse DNS or host file.
Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.
Configure the remote web server to use HSTS.

Consolidated Solution/Correction Plan for above IP address:
Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.
Make sure that every sensitive form transmits content over HTTPS.
Set a properly configured Content-Security-Policy header for all requested resources.
Protect your target with an IP filter.
Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.
Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Part 3b. Special notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
www.vin65.com	Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	Directory Browsing: 80 / tcp / www	The customer declares the software is implemented securely.	
www.vin65.com	Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	Directory Browsing: 443 / tcp / www	The customer declares the software is implemented securely.	