Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Vin65	ASV Company:	Comodo CA Limited
Date scan was completed:	01/13/2015	Scan expiration date:	04/13/2015

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) www (80/tcp)	High	7.5	Pass	The vulnerability is not present after inspection and testing
www.vin65.com	CGI Generic XML Injection www (443/tcp)	Medium	6.8	Pass	The vulnerability is not present after inspection and testing
www.vin65.com	CGI Generic Path Traversal (write test) www (443/tcp)	Medium	6.4	Pass	The software uses a secure configuration
www.vin65.com	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
www.vin65.com	Web Server Uses Plain Text Authentication Forms www (80/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Injectable Parameter www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Application Potentially Sensitive CGI Parameter Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server robots.txt Information Disclosure www (443/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	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Office File Inventory www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Allows Password Auto-Completion www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Directory Enumeration www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Perfect Forward Secrecy Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Cipher Block Chaining Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	OpenSSL Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Service Detection www (443/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	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Injectable Parameter www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Allows Password Auto-Completion www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server No 404 Error Code Check www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Web Server Directory Enumeration www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Nessus TCP scanner www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Device Type general/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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	Inconsistent Hostname and IP Address general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
www.vin65.com	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	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.

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Modify the affected CGI scripts so that they properly escape arguments, especially XML tags and special characters (angle brackets and slashes).

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

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.

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.

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

Make sure that every sensitive form transmits content over HTTPS.

Fix the reverse DNS or host file.

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

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: www (80/tcp)		
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: www (443/tcp)		