

Part 1. Scan Information

Scan Customer Company:	vadimlab	ASV Company:	Comodo CA Limited
Date scan was completed:	06-19-2017	Scan expiration date:	09-17-2017







Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):52.37.50.95	Pass <input checked="" type="checkbox"/>	Fail <input type="checkbox"/>
--	--	-------------------------------

Part 3a. Vulnerabilities Noted for each Component

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
52.37.50.95	Web Server Uses Plain Text Authentication Forms 80 / tcp / www	Low	2.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Service Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Nessus SYN scanner 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Web Application Potentially Sensitive CGI Parameter Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Device Type 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	HTTP Server Type and Version 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	OS Identification 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Drupal Software Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Web Server Allows Password Auto-Completion 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
52.37.50.95	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	CGI Generic Injectable Parameter 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Web Application Cookies Not Marked Secure 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	HTTP X-Frame-Options Response Header Usage 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	Web Application Sitemap 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
52.37.50.95	CGI Generic Tests Load Estimation (all tests) 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Protect your target with an IP filter.
Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.
Ensure that the use of this software aligns with your organization's security and acceptable use policies.
Set a properly configured Content-Security-Policy header for all requested resources.
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
Make sure that every sensitive form transmits content over HTTPS.
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.

Set a properly configured X-Frame-Options header for all requested resources.

Part 3b. Special notes by IP Address

Component	Special Note	Item Noted	Scan customer`s description of action taken and declaration that software is either implemented securely or removed

Part 3c. Special notes -- Full Text
Note

Load Balancing

As you were unable to validate that the configuration of the environment behind your load balancers is synchronized, it is your responsibility to ensure that the environment is scanned as part of the internal vulnerability scans required by the PCI DSS.

Directory Browsing

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.

Remote Access

Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/removed. Please consult your ASV if you have questions about this Special Note.

Pos Software detected

Due to increased risk to the cardholder data environment when a point-of-sale system is visible on the Internet, please 1) confirm that this system needs to be visible on the Internet, that the system is implemented securely, and that original default passwords have been changed to complex passwords, or 2) confirm that the system has been reconfigured and is no longer visible to the Internet. Please consult your ASV if you have questions about this Special Note.

Embedded links or code from out-of-scope domains

Note to scan customer: Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.

Insecure Services / industry-deprecated protocols

Note to scan customer: Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Unknown services

Note to scan customer: Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

IP_ADDRESS:52.37.50.95

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

52.37.50.95

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)

Requires description for each IP Address/range/subnet, domain, URL