ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company	:			Company	:		
Contact Name	: Sample Admin			Contact Name	: ASV Support		
Job Title	: PCI Compliance Manager			Job Title	: ASV Support		
Telephone	: +1 555 010 0100			Telephone	:		
E-mail	: admin@example.com			E-mail	:		
Business Addr	: 1 Sample Street			Business Addr	:		
City	: Sample City	State/Province	: State	City	:	State/Province	:
Postal code	: 000000	Country	: Country	Postal code	:	Country	: India
Website / URL	: example.com			Website / URL	:		

A.3 Scan Status	
Date scan completed: 09-12-2025	Scan expiration date (90 days from date scan completed): 09-03-2026
Compliance status: **Fail**	Scan report type: Full scan
Number of unique in-scope components* scanned:	1
Number of identified failing vulnerabilities:	28
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:	0

** A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment.*

A.4 Scan Customer Attestation

attests on 09-12-2025 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, “Scan Status”) includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report were prepared and conducted by under certificate number according to internal processes that meet PCI DSS Requirement 11.3.2 and the ASV Program Guide.
attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by ASV Support.

ASV Scan Report Summary

Part 1. Scan Information			
Scan customer company:		ASV Company:	
Date scan was completed:	09-12-2025	Scan expiration date:	09-03-2026

Part 2. Component Compliance Summary		
Component (IP Address, domain, etc.):	203.0.113.25, example.com	**Fail**

Part 3a. Vulnerabilities Noted for each Component

203.0.113.25,example.com

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
203.0.113.25 example.com 8080/tcp/www	CGI Generic SQL Injection (blind)	High	8.3	**Fail**	
203.0.113.25 example.com 443/tcp/www	CGI Generic SQL Injection (blind)	High	8.3	**Fail**	
203.0.113.25 example.com 80/tcp/www	CGI Generic SQL Injection (blind)	High	8.3	**Fail**	
203.0.113.25 example.com 443/tcp/www	TLS Version 1.0 Protocol Detection (PCI DSS)	High	8.2	**Fail**	
203.0.113.25 example.com 443/tcp/www	TLS Version 1.1 Protocol Detection (PCI DSS)	High	8.2	**Fail**	
203.0.113.25 example.com 8080/tcp/www	Script Src Integrity Check	High	7.1	**Fail**	
203.0.113.25 example.com 443/tcp/www	Script Src Integrity Check	High	7.1	**Fail**	
203.0.113.25 example.com 80/tcp/www	Script Src Integrity Check	High	7.1	**Fail**	
203.0.113.25 example.com 8080/tcp/www	CGI Generic Cross-Site Request Forgery Detection (potential)	Medium	6.5	**Fail**	
203.0.113.25 example.com 443/tcp/www	CGI Generic Cross-Site Request Forgery Detection (potential)	Medium	6.5	**Fail**	
203.0.113.25 example.com	HSTS Missing From HTTPS Server (RFC 6797)	Medium	6.5	**Fail**	

443/tcp/www					
203.0.113.25 example.com 443/tcp/www	TLS Version 1.0 Protocol Detection	Medium	6.5	**Fail**	
203.0.113.25 example.com 443/tcp/www	TLS Version 1.1 Deprecated Protocol	Medium	6.5	**Fail**	
203.0.113.25 example.com 80/tcp/www	CGI Generic Cross-Site Request Forgery Detection (potential)	Medium	6.5	**Fail**	
203.0.113.25 example.com 8080/tcp/www	PCI DSS Compliance : Insecure Communication Has Been Detected	Medium	5.3	**Fail**	
203.0.113.25 example.com 8080/tcp/www	Sensitive File Disclosure	Medium	5.3	**Fail**	
203.0.113.25 example.com 443/tcp/www	Sensitive File Disclosure	Medium	5.3	**Fail**	
203.0.113.25 example.com 80/tcp/www	PCI DSS Compliance : Insecure Communication Has Been Detected	Medium	5.3	**Fail**	
203.0.113.25 example.com 80/tcp/www	Sensitive File Disclosure	Medium	5.3	**Fail**	
203.0.113.25 example.com 443/tcp/www	SSL/TLS Recommended Cipher Suites (PCI DSS)	Medium	4.8	**Fail**	
203.0.113.25 example.com 8080/tcp/www	CGI Generic XSS (comprehensive test)	Medium	4.3	**Fail**	
203.0.113.25 example.com 8080/tcp/www	Web Application Potentially Vulnerable to Clickjacking	Medium	4.3	**Fail**	
203.0.113.25 example.com 443/tcp/www	Web Application Potentially Vulnerable to Clickjacking	Medium	4.3	**Fail**	
203.0.113.25	Web Application Potentially	Medium	4.3	**Fail**	

example.com 80/tcp/www	Vulnerable to Clickjacking				
203.0.113.25 example.com 443/tcp/www	Weak DH Key Exchange Supported (PCI DSS) CVE-2015-4000	Low	3.7	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam) CVE-2015-4000	Low	3.7	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Web Server Transmits Cleartext Credentials	Low	2.6	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web Server Transmits Cleartext Credentials	Low	2.6	**Pass**	
203.0.113.25 example.com 0/icmp/general	ICMP Timestamp Request Remote Date Disclosure CVE-1999-0524	Low	2.1	**Pass**	
203.0.113.25 example.com 8080/tcp/www	PCI DSS compliance	High	0.0	**Fail**	
203.0.113.25 example.com 443/tcp/www	PCI DSS compliance	High	0.0	**Fail**	
203.0.113.25 example.com 80/tcp/www	PCI DSS compliance	High	0.0	**Fail**	
203.0.113.25 example.com 0/tcp/general	PCI DSS compliance	High	0.0	**Fail**	
203.0.113.25 example.com 8080/tcp/www	PCI DSS Compliance - Information Leakage	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	CGI Generic Tests Timeout	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	CGI Generic Tests Load Estimation (all tests)	Low	0.0	**Pass**	
203.0.113.25 example.com	HyperText Transfer Protocol (HTTP) Information	Low	0.0	**Pass**	

8080/tcp/www					
203.0.113.25 example.com 8080/tcp/www	Web Server Office File Inventory	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	CGI Generic Injectable Parameter	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Apache Tomcat Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	HTTP Methods Allowed (per directory)	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	HTTP Server Type and Version	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Missing or Permissive X-Frame-Options HTTP Response Header	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Web Application Cookies Not Marked Secure	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Web Application Sitemap	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	External URLs	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Web Server Allows Password Auto-Completion	Low	0.0	**Pass**	
203.0.113.25 example.com 8080/tcp/www	Web mirroring	Low	0.0	**Pass**	
203.0.113.25 example.com	Service Detection	Low	0.0	**Pass**	

8080/tcp/www					
203.0.113.25 example.com 8080/tcp/www	Nessus SYN scanner	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	PCI DSS Compliance - Information Leakage	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	CGI Generic Tests Timeout	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	CGI Generic Tests Load Estimation (all tests)	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	HyperText Transfer Protocol (HTTP) Information	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	HTTP Cookie 'secure' Property Transport Mismatch	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Web Server Office File Inventory	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	CGI Generic Injectable Parameter	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Apache Tomcat Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	HTTP Methods Allowed (per directory)	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	HSTS Missing From HTTPS Server	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	HTTP Server Type and Version	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Missing or Permissive X-Frame-Options HTTP Response Header	Low	0.0	**Pass**	

203.0.113.25 example.com 443/tcp/www	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Web Application Cookies Not Marked Secure	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Web Application Sitemap	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	External URLs	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Web Server Allows Password Auto-Completion	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Web mirroring	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL Cipher Block Chaining Cipher Suites Supported	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL Perfect Forward Secrecy Cipher Suites Supported	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL/TLS Recommended Cipher Suites	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	TLS Version 1.2 Protocol Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	TLS Version 1.1 Protocol Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL Cipher Suites Supported	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL Root Certification Authority Certificate Information	Low	0.0	**Pass**	

203.0.113.25 example.com 443/tcp/www	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL Certificate Information	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	SSL / TLS Versions Supported	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Service Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 443/tcp/www	Nessus SYN scanner	Low	0.0	**Pass**	
203.0.113.25 example.com 161/udp/snmp?	SNMP Server Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	PCI DSS Compliance - Information Leakage	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	CGI Generic Tests Timeout	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	CGI Generic Tests Load Estimation (all tests)	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	HyperText Transfer Protocol (HTTP) Information	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web Server Office File Inventory	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	CGI Generic Injectable Parameter	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Apache Tomcat Detection	Low	0.0	**Pass**	
203.0.113.25	HTTP Methods Allowed (per	Low	0.0	**Pass**	

example.com 80/tcp/www	directory)				
203.0.113.25 example.com 80/tcp/www	HTTP Server Type and Version	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Missing or Permissive X-Frame-Options HTTP Response Header	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web Application Cookies Not Marked Secure	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web Application Sitemap	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	External URLs	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web Server Allows Password Auto-Completion	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Web mirroring	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Service Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 80/tcp/www	Nessus SYN scanner	Low	0.0	**Pass**	
203.0.113.25 example.com 0/udp/general	Traceroute Information	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	Nessus Scan Information	Low	0.0	**Pass**	
203.0.113.25	PCI DSS Compliance - Information	Low	0.0	**Pass**	

example.com 0/tcp/general	Leakage				
203.0.113.25 example.com 0/tcp/general	Common Platform Enumeration (CPE)	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	PCI DSS Compliance : Handling False Positives	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	Device Type	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	OS Fingerprints Detected	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	OS Identification	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	TCP/IP Timestamps Supported	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	Firewall Detection	Low	0.0	**Pass**	
203.0.113.25 example.com 0/tcp/general	PCI DSS compliance : options settings	Low	0.0	**Pass**	

Consolidated Solution/Correction Plan for above Component:
Modify the affected CGI scripts so that they properly escape arguments.
All processing and third party entities - including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater service offering by June 2016. All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective June 2018.
All processing and third party entities - including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.2 or greater service offering by June 2018. All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective June 2018.
Set script integrity checking on target script or remove target script.
Restrict access to the application vulnerable to cross-site request forgery. Contact the vendor for a patch or upgrade.
Configure the remote web server to use HSTS.
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
Properly encrypt all authenticated and sensitive communications.
Static files that are not necessary should be removed from the web root. If documents are required to be in the web root, and are sensitive in nature, they should require authentication.
Only enable support for recommended cipher suites.
Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
Consult the software's manual and reconfigure the service to use at least 2048-bit DH parameters. Alternatively, disable DH and use only Elliptic-curve Diffie-Hellman (ECDH) instead.
Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
Make sure that every sensitive form transmits content over HTTPS.
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Part 3b. Special Notes to Scan Customer by Component			
Component	**Special Note to Scan Customer**	**Item Noted**	**Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed**

Part 3c. Special Notes – Full Text

Part 4a. Scan Scope Submitted by Scan Customer for Discovery
IP Addresses/ranges/subnets, domains, URLs, etc.
example.com

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.
203.0.113.25, example.com

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc. No out-of-scope components were found.

ASV Scan Report Vulnerability Details

Part 1. Scan Information			
Scan customer company:		ASV Company:	
Date scan was completed:	09-12-2025	Scan expiration date:	09-03-2026

Sample excerpt

This excerpt shows 8 of the 200 pages in the full Vulnerability Details report, with a selection of findings. The full report repeats every finding for each port it appears on. Customer and target details in this sample are fictitious.

Part 2. Vulnerability Details

Component	Detected Open Ports/Protocol/ Services	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status
203.0.113.25 example.com	8080/tcp/www	CGI Generic SQL Injection (blind)	High		8.3	**Fail**
	Automatic Failure: - **Special Note:** -					
	Details					
	Description: By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. **Synopsis:** A CGI application hosted on the remote web server is potentially prone to SQL injection attack. **Solution:** Modify the affected CGI scripts so that they properly escape arguments. **Output:** Using the GET HTTP method, Nessus found that : + The following resources may be vulnerable to blind SQL injection : + The 'btnSubmit' parameter of the /doLogin CGI : /doLogin?uid=&passw=&btnSubmit=Login'||'&passw=&btnSubmit=Login -------- output -------- HTTP/1.1 302 Found -------- vs -------- HTTP/1.1 400 Bad Request ------------------------ + The 'url' parameter of the /disclaimer.htm CGI : /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com'||'http%3a%2f%2fwww.ne tscape.com -------- output -------- HTTP/1.1 200 OK -------- vs --------				

	HTTP/1.1 400 Bad Request ---------- **References:** http://www.securiteam.com/securityreviews/5DP0N1P76E.html http://www.nessus.org/u?ed792cf5 http://www.nessus.org/u?11ab1866 **CVSS V3 Score:** 8.3 **CVSS V3 Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L **CVSS V2 Score:** 7.5 **CVSS V2 Vector:** CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P **BID:** - **CPE:** - **URLS:** -

Component	Detected Open Ports/Protocol/ Services	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status
203.0.113.25 example.com	443/tcp/www	TLS Version 1.0 Protocol Detection (PCI DSS)	High		8.2	**Fail**
	Automatic Failure: - **Special Note:** -					
	Details					
	Description: The remote service accepts connections encrypted using TLS 1.0. This version of TLS is affected by multiple cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. **Synopsis:** The remote service encrypts traffic using a protocol with known weaknesses. **Solution:** All processing and third party entities - including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater service offering by June 2016. All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective June 2018. **Output:** TLSv1 is enabled on port 443 and the server supports at least one cipher. **References:** - **CVSS V3 Score:** 8.2 **CVSS V3 Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N **CVSS V2 Score:** 8.5 **CVSS V2 Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:P/A:N **BID:** - **CPE:** - **URLS:** -					

Component	Detected Open Ports/Protocol/ Services	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status
203.0.113.25 example.com	8080/tcp/www	Script Src Integrity Check	High		7.1	**Fail**
	Automatic Failure: - **Special Note:** -					
	Details					
	Description: The remote host may be vulnerable to payment entry data exfiltration due to javascript included from potentially untrusted and unverified third parties script src. If the host is controlled by a 3rd party, ensure that the 3rd party is PCI DSS compliant. **Synopsis:** Report external script resources not using integrity. **Solution:** Set script integrity checking on target script or remove target script. **Output:** Path : http://analytics.example.com/urchin.js Parent : /index.jsp?content=personal_investments.htm Attributes : - type : text/javascript - src : http://analytics.example.com/urchin.js **References:** http://www.nessus.org/u?c9e76c4f https://www.w3.org/TR/SRI/ http://www.nessus.org/u?f39144f8 **CVSS V3 Score:** 7.1 **CVSS V3 Vector:** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N **CVSS V2 Score:** 7.8 **CVSS V2 Vector:** CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:N **BID:** - **CPE:** - **URLS:** -					

Component	Detected Open Ports/Protocol/ Services	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status
203.0.113.25 example.com	8080/tcp/www	Sensitive File Disclosure	Medium		5.3	**Fail**
	Automatic Failure: - **Special Note:** -					
	Details					
	Description: The remote web application hosts documents or office files that may contain sensitive information. **Synopsis:** The web application hosts static files that may be sensitive in nature. **Solution:** Static files that are not necessary should be removed from the web root. If documents are required to be in the web root, and are sensitive in nature, they should require authentication. **Output:** The following URLs are potentially sensitive documents : /pr/communityannualreport.pdf /pr/communityannualreport.pdf /pr/communityannualreport.pdf **References:** - **CVSS V3 Score:** 5.3 **CVSS V3 Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N **CVSS V2 Score:** 5.0 **CVSS V2 Vector:** CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N **BID:** - **CPE:** - **URLS:** -					

Component	Detected Open Ports/Protocol/ Services	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status
203.0.113.25 example.com	443/tcp/www	Weak DH Key Exchange Supported (PCI DSS)	Low	CVE-2015-4000	3.7	**Pass**
	Automatic Failure: - **Special Note:** -					
	Details					
	Description: At least one of the services on the remote host supports a Diffie-Hellman key exchange using a public modulus smaller than 2048 bits. Diffie-Hellman key exchanges with keys smaller than 2048 bits do not meet the PCI definition of strong cryptography as specified by NIST Special Publication 800-57 Part 1. Diffie-Hellman moduli of up to 1024 bits are considered practically breakable by an attacker with very significant resources. **Synopsis:** A service on the remote host supports a weak key exchange mechanism **Solution:** Consult the software's manual and reconfigure the service to use at least 2048-bit DH parameters. Alternatively, disable DH and use only Elliptic-curve Diffie-Hellman (ECDH) instead. **Output:** The SSL/TLS service on port 443 uses a 1024-bit DH modulus. **References:** https://weakdh.org/ **CVSS V3 Score:** 3.7 **CVSS V3 Vector:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N **CVSS V2 Score:** 4.3 **CVSS V2 Vector:** CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N **BID:** 74733 **CPE:** - **URLS:** -					

Part 3. Port Scan Results			
Component	**Port**	**Protocol**	**Service Name**
203.0.113.25,example.com	0	icmp	general
203.0.113.25,example.com	0	tcp	general
203.0.113.25,example.com	0	udp	general
203.0.113.25,example.com	80	tcp	www
203.0.113.25,example.com	161	udp	snmp?
203.0.113.25,example.com	443	tcp	www
203.0.113.25,example.com	8080	tcp	www