Trustwave®

Report Date: 2019-02-28

Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	DoJiggy LLC		
Contact Name:	Rodrigo Murillo	**Job Title:**	
Telephone:	303-435-5786	**E-mail:**	rodm@dojiggy.com
Business Address:	14525 SW Millikan Way Suite 73730		
City:	Beaverton	**State/Province:**	Oregon
ZIP/Postal Code:	97005	**Country:**	US
Website / URL:			

A.2 Approved Scanning Vendor Information

Company:	Trustwave Holdings, Inc.		
Contact Name:	Trustwave Support	**Job Title:**	
Telephone:	1-800-363-1621	**E-mail:**	support@trustwave.com
Business Address:	70 West Madison St., Ste 1050		
City:	Chicago	**State/Province:**	IL
ZIP/Postal Code:	60602	**Country:**	US
Website / URL:	www.trustwave.com		

A.3 Scan Status

Date scan completed:	2019-02-27	Scan expiration date (90 days from date scan completed):	2019-05-27
Compliance status:	Pass	Scan report type:	Full Scan
Number of unique in-scope components scanned:	3		
Number of identified failing vulnerabilities:	0		
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:	0		

A.4 Scan Customer Attestation

DoJiggy LLC attests on 2019-02-25 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. DoJiggy LLC 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.

Signature

Printed Name

Title

Date

A.5 ASV Attestation

This scan and report was prepared and conducted by Trustwave under certificate number 3702-01-12 (2017), 3702-01-11 (2016), 3702-01-10 (2015), 3702-01-09 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.

Trustwave 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 the Trustwave Quality Assurance Process.

Vulnerability Scan Report: Table of Contents

Attestation of Scan Compliance

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	DoJiggy LLC	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-02-27	Scan Expiration Date	2019-05-28

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	54.227.153.159 - demoprogolf.dojiggy.com (demoprogolf.dojiggy.com) admin.dojiggy.com demopledge.dojiggy.com	Pass

Part 3a. Vulnerabilities Noted for Each Component

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
1	54.227.153.159 (demoprogolf.dojiggy.com)	Non-Secure Session Cookies Identified	Medium	5.00	Pass	**Dispute Confirmed** We have accepted this dispute based on the information provided indicating that your organization can confirm that this cookie is not a session cookie but rather a tracking cookie that has nothing to do with authentication to this system. **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
2	54.227.153.159 (demoprogolf.dojiggy.com)	Non-Secure Session Cookies Identified	Medium	5.00	Pass	**Dispute Confirmed** We have accepted this dispute based on the information provided indicating that your organization can confirm that this cookie is not a session cookie but rather a tracking cookie that has nothing to do with authentication to this system. **Note to scan customer:**

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
						This vulnerability is not recognized in the National Vulnerability Database.
3	54.227.153.159 (demoprogolf.dojiggy.com)	Non-Secure Session Cookies Identified	Medium	5.00	Pass	**Dispute Confirmed** We have accepted this dispute based on the information provided indicating that your organization can confirm that this cookie is not a session cookie but rather a tracking cookie that has nothing to do with authentication to this system. **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
4	54.227.153.159 (demoprogolf.dojiggy.com)	No X-FRAME-OPTIONS Header	Low	2.60	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
5	54.227.153.159 (demoprogolf.dojiggy.com)	Auto-Completion Enabled for Password Fields	Low	1.20	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
6	54.227.153.159 (demoprogolf.dojiggy.com)	Discovered HTTP Methods	Info	0.00	Pass	
7	54.227.153.159 (demoprogolf.dojiggy.com)	Discovered Web Applications	Info	0.00	Pass	
8	54.227.153.159 (demoprogolf.	Discovered Web Directories	Info	0.00	Pass	

ASV Scan Report Summary

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
	dojiggy.com)					
9	54.227.153.159 (demoprogolf.dojiggy.com)	Enumerated Applications	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
10	54.227.153.159 (demoprogolf.dojiggy.com)	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
11	54.227.153.159 (demoprogolf.dojiggy.com)	SSL-TLS Certificate Information	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
12	54.227.153.159 (demoprogolf.dojiggy.com)	URLScan Detected	Info	0.00	Pass	
13	54.227.153.159 (demoprogolf.dojiggy.com)	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
14	54.227.153.159 (demoprogolf.dojiggy.com)	Wildcard SSL Certificate Detected	Info	0.00	Pass	

Consolidated Solution/Correction Plan for the above Component:

- Configure the HTTP service(s) running on this host to adhere to information security best practices.
- Restrict access to any files, applications, and/or network services for which there is no business requirement to be publicly accessible.
- Ensure that any web applications running on this host is configured following industry security best practices.
- Ensure that any web applications running on this host properly validate and transmit user input in a secure manner.

Part 3b. Special Notes by Component

#	Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed
No Special Notes				

Part 3c. Special Notes - Full Text

Note
Customer Note Customer has not validated that all servers behind load balancers are identical and synchronized.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Address/ranges/subnets, domains, URLs, etc.
Domain: admin.dojiggy.com
Domain: demopledge.dojiggy.com
Domain: demoprogolf.dojiggy.com

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

IP Address/ranges/subnets, domains, URLs, etc.
54.227.153.159 / ec2-54-227-153-159.compute-1.amazonaws.com (demoprogolf.dojiggy.com)

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

ASV Scan Report Summary

IP Address/ranges/subnets, domains, URLs, etc.
demoauction.dojiggy.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.
demodonations.dojiggy.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.
get.dojiggy.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.
raiders.dojiggy.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.
www.dojiggy.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.
www.ndnwholesale.com -- Scan customer attests that target or targets are out-of-scope and do not need to be scanned for PCI.

ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	DoJiggy LLC	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-02-27	Scan Expiration Date	2019-05-28

Part 2. Vulnerability Details

The following issues were identified during this scan. Please review all items and address all that items that affect compliance or the security of your system.

In the tables below you can find the following information about each TrustKeeper finding.

- *CVE Number* - The Common Vulnerabilities and Exposure number(s) for the detected vulnerability - an industry standard for cataloging vulnerabilities. A comprehensive list of CVEs can be found at nvd.nist.gov or cve.mitre.org.
- *Vulnerability* - This describes the name of the finding, which usually includes the name of the application or operating system that is vulnerable.
- *CVSS Score* - The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Further information can be found at www.first.org/cvss or nvd.nist.gov/cvss.cfm.
- *Severity* - This identifies the risk of the vulnerability. It is closely associated with the CVSS score.
- *Compliance Status* - Findings that are PCI compliance violations are indicated with a Fail status. In order to pass a vulnerability scan, these findings must be addressed. Most findings with a CVSS score of 4 or more, or a Severity of Medium or higher, will have a Fail status. Some exceptions exist, such as DoS vulnerabilities, which are not included in PCI compliance.
- *Details* - TrustKeeper provides the port on which the vulnerability is detected, details about the vulnerability, links to available patches and other specific guidance on actions you can take to address each vulnerability.

For more information on how to read this section and the scoring methodology used, please refer to the appendix.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/443 This host does not appear to utilize the benefits that the X-FRAME-

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						OPTIONS HTTP header element offers. This header may be implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object). **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:P/A:N **Service:** http **Application:** microsoft:iis **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Evidence:** url: https://admin.dojiggy.com/ng/assets/javascripts/auction/countdown.js?20B243648D1597ACCAE6757001D100F4 Headers: {"date"=>["Wed, 27 Feb 2019 17:56:24 GMT"], "content-type"=>["application/x-javascript"], "content-length"=>["5935"], "connection"=>["keep-alive"], "set-cookie"=>["AWSALB=c193mbApQGgDP7dC3RsDWwKDxR7LZsUtmI/yXWnvt9mSvnyGk/OFB6RyXDM1OSKFrwQQBeYSqbxW/5qFQqtagxeSa7yndd3NWtgncmhD75/0W5VD6btUDjGCHueW; Expires=Wed, 06 Mar 2019 17:56:24 GMT; Path=/"], "last-modified"=>["Wed, 27 Feb 2019 17:19:36 GMT"], "accept-ranges"=>["bytes"], "etag"=>["\"044c89cc0ced41:0\""], "server"=>["Microsoft-IIS/7.5"], "x- **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
2		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/443 This host does not appear to utilize the benefits that the X-FRAME-OPTIONS HTTP header element offers. This header may be implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object). **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:P/A:N **Service:** http **Application:** microsoft:iis **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Evidence:** url: https://demopledge.dojiggy.com/ Headers: {"date"=>["Wed, 27 Feb 2019 17:58:43 GMT"], "content-type"=>["text/html; charset=UTF-8"], "content-length"=>["16061"], "connection"=>["keep-alive"], "set-cookie"=>["AWSALB=Qxo6SUbQqeMxNFwPsdqT93a0NY0z1bLZ8k+WsRUzh55dx5JvQ2VCZb4uF8cRFSka0Xf7IRY8346Rywo5oEWNQTwSki5VJQQ14veDFO6LBC1k0DDYhUl2XAxKLY1+; Expires=Wed, 06 Mar 2019 17:58:43 GMT; Path=/", "CFID=684302;secure;path=/;HTTPOnly", "CFTOKEN=4a77c3b4acb3c7cb-E116BE6A-CA7F-0DE4-4FAB9A8D6CCE3BA6;secure;path=/;HTTPOnly"], "content-language"=>["en-US,en-US"], "server"=>["Microsoft-IIS/7.5"], "x-powered-by"=>["ASP.NET"]} **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						jacking type of attacks.
3		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/443 This host does not appear to utilize the benefits that the X-FRAME-OPTIONS HTTP header element offers. This header may be implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object). **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:P/A:N **Service:** http **Application:** microsoft:iis **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Evidence:** url: https://demoprogolf.dojiggy.com/ Headers: {"date"=>["Wed, 27 Feb 2019 18:02:08 GMT"], "content-type"=>["text/html; charset=UTF-8"], "content-length"=>["12693"], "connection"=>["keep-alive"], "set-cookie"=>["AWSALB=aT3c65VkoGLF2YJaR0uRb91/Eb65inzDwJkdlwOwWiuXTOpuFWvL0W/8+oSx0zFLY9P2cm9PEipixVdHmEDw4b24PUqSx1+mt8XXZxbOcPIGwAyU7Zw4CGbNpJ/d; Expires=Wed, 06 Mar 2019 18:02:08 GMT; Path=/", "CFID=1811059;secure;path=/;HTTPOnly", "CFTOKEN=ff9679996531c36d-E127AA30-A8A7-671F-BB9938F6448EF29D;secure;path=/;HTTPOnly"], "content-language"=>["en-US,en-US"], "server"=>["Microsoft-IIS/7.5"], "x-powered-by"=>["ASP.NET"]}

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
4		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg-signup/pledge Form Name: (no name) Action: Fields: objMember[password] (password), objMember[passwordConfirmation] (password) **Remediation:**

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
5		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg-signup/volunteer Form Name: (no name) Action: Fields: objMember[password] (password), objMember[passwordConfirmation] (password)

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
6		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/my-account/login Form Name: Action: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/my-account/login Fields: password (password)

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
7		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg-catalog/registration-form/b7160949?returnUrl=https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg- Form Name: (no name)

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Action: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg-catalog/registration-form/b7160949 Fields: player_1_279344_46025857[password] (password), player_1_279344_46025857[passwordConfirmation] (password) **Remediation:** Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
8		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Location: cfm/ac3ce9/reg-catalog/registration-form/b7160949?returnUrl=https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg- Form Name: (no name) Action: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/reg-catalog/registration-form/b7160949 Fields: teamPlayer_279344_75165939_1_1[password] (password), teamPlayer_279344_75165939_1_1[passwordConfirmation] (password) **Remediation:** Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
9		Auto-Completion Enabled for Password Fields	1.20	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://demoprogolf.dojiggy.com/ng/index.cfm/ad2e68/my-account/login Form Name: Action: https://demoprogolf.dojiggy.com/ng/index.cfm/ad2e68/my-account/login Fields: password (password) **Remediation:** Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
10		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: microsoft:iis URI: / Version: 7.5

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is required.
11		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: adobe:coldfusion URI: / Version: unknown **Remediation:** No remediation is required.
12		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:**

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CPE: microsoft:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
13		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: microsoft:asp.net URI: / Version: 2.0.50727 **Remediation:** No remediation is required.
14		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://54.227.153.159/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
15		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/80 The following web applications were discovered on the remote HTTP server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** No remediation is required.
16		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/80 It was possible to guess one or more directories contained in the publicly accessible path of this web server.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://54.227.153.159:80/admin/ HTTP Response Code: 302 URL: http://54.227.153.159:80/Admin/ URL: http://54.227.153.159:80/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
17		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://admin.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
18		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/80 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://admin.dojiggy.com:80/admin/ HTTP Response Code: 302 URL: http://admin.dojiggy.com:80/Admin/ URL: http://admin.dojiggy.com:80/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
19		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://demopledge.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
20		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/80 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://demopledge.dojiggy.com:80/admin/ HTTP Response Code: 302 URL: http://demopledge.dojiggy.com:80/Admin/ URL: http://demopledge.dojiggy.com:80/cfdocs/ HTTP Response Code: 500

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review these directories and verify that there is no unintentional content made available to remote users.
21		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://demoprogolf.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
22		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/80 It was possible to guess one or more directories contained in the publicly accessible path of this web server.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://demoprogolf.dojiggy.com:80/admin/ HTTP Response Code: 302 URL: http://demoprogolf.dojiggy.com:80/Admin/ URL: http://demoprogolf.dojiggy.com:80/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
23		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /CN=*.dojiggy.com Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon Certificate Chain Depth: 0 Wildcard Subject Name: *.dojiggy.com

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review your certificate configurations to assure that wildcard certificates are suitable for your application.
24		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /CN=*.dojiggy.com Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon Certificate Chain Depth: 0 Wildcard Subject Name: *.golfreg.com **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
25		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /CN=*.dojiggy.com Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon Certificate Chain Depth: 0 Wildcard Subject Name: *.teeblockersonline.com **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
26		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/443 The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA). A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
27		SSL-TLS Certificate Information	0.00	Info	Pass	**Port:** tcp/443 Information extracted from a certificate discovered on a TLS or SSL wrapped service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Verified: true Today: 2019-02-27 11:42:42 -0600 Start date: 2018-06-29 00:00:00 UTC End date: 2019-07-29 12:00:00 UTC Expired: false Fingerprint: E3:B3:F5:10:0F:34:A7:EE:41:4E:8E:20:99:11:64:5A Subject: /CN=*.dojiggy.com Common name: *.dojiggy.com Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon Signature Algorithm: sha256WithRSAEncryption Version: 2
28		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: CPE: microsoft:iis URI: / Version: 7.5 **Remediation:** No remediation is required.
29		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: adobe:coldfusion URI: / Version: unknown **Remediation:** No remediation is required.
30		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: microsoft:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
31		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** CPE: microsoft:asp.net URI: / Version: 2.0.50727 **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
32		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://54.227.153.159/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
33		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/443 The following web applications were discovered on the remote HTTP server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** No remediation is required.

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
34		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://54.227.153.159:443/admin/ HTTP Response Code: 302 URL: https://54.227.153.159:443/Admin/ URL: https://54.227.153.159:443/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
35		URLScan Detected	0.00	Info	Pass	**Port:** tcp/443 The web server appears to be using Microsoft's URLScan tool, an ISAPI filter that can be configured to block specified web requests. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://technet.microsoft.com/en-us/security/cc242650.aspx **Evidence:** Method: urlscan.ini 'MaxQueryString' is set to the default of 2048. Query strings longer than 2048 characters are rejected. **Remediation:** No remediation necessary. This is identified for informational purposes.
36		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://admin.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
37		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://admin.dojiggy.com:443/admin/ HTTP Response Code: 302 URL: https://admin.dojiggy.com:443/Admin/ URL: https://admin.dojiggy.com:443/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
38		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Application: microsoft:iis **Evidence:** Location: https://admin.dojiggy.com/ng/index.cfm/a/admin-login/login Parameter: username (Possible username; manipulation could allow user impersonation) Parameter: password (Possible password, vulnerable to dictionary attack) Location: https://admin.dojiggy.com/ng/index.cfm/a/adminLogin/login/ Location: https://admin.dojiggy.com/ng/index.cfm/a/adminLogin/login/?error=6&pi=48040A081B074C020B1D021D40061404&qs=&CFID=1810056&CFTOKEN=9d0bafbdbaedb82f-E0EA67B6-00DA-2205-8B9DBB87CEC5DE48 **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
39		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: URL: https://demopledge.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
40		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://demopledge.dojiggy.com:443/admin/ HTTP Response Code: 302 URL: https://demopledge.dojiggy.com:443/Admin/ URL: https://demopledge.dojiggy.com:443/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
41		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Location: https://demopledge.dojiggy.com/ng/index.cfm/ac3ce9/my-account/login Parameter: password (Possible password, vulnerable to dictionary attack) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
42		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Application: microsoft:iis **Evidence:** URL: https://demoprogolf.dojiggy.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
43		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://demoprogolf.dojiggy.com:443/admin/ HTTP Response Code: 302 URL: https://demoprogolf.dojiggy.com:443/Admin/ URL: https://demoprogolf.dojiggy.com:443/cfdocs/ HTTP Response Code: 500 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.

ASV Scan Report Vulnerability Details

54.227.153.159 (demoprogolf.dojiggy.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
44		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Location: https://demoprogolf.dojiggy.com/ng/index.cfm/ad2e68/my-account/login Parameter: password (Possible password, vulnerable to dictionary attack) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.

ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a usable format at https://www.pcisecuritystandards.org. Please send this completed form to PCI SSC at: asv@pcisecuritystandards.org.

ASV FEEDBACK FORM	
Client Name (merchant or service provider):	**Approved Scanning Vendor Company (ASV):**
Name	Name
Contact	Contact
Telephone	Telephone
E-Mail	E-Mail
Business location where assessment took place:	**ASV employee who performed assessment:**
Street	Name
City	Telephone
State/Zip	E-Mail
For each question, please indicate the response that best reflects your experience and provide comments. **4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree**	
1) During the initial engagement, did the ASV explain the objectives, timing, and review process, and address your questions and concerns?	
Response:	
Comments:	

2) Did the ASV employee(s) understand your business and technical environment, and the payment card industry?
Response:
Comments:
3) Did the ASV employee(s) have sufficient security and technical skills to effectively perform this PCI Scanning Service?
Response:
Comments:
4) Did the ASV sufficiently understand the PCI Data Security Standard and the PCI Security Scanning Procedures?
Response:
Comments:
5) Did the ASV effectively minimize interruptions to operations and schedules?
Response:
Comments:
6) Did the ASV provide an accurate estimate for time and resources needed?
Response:
Comments:
7) Did the ASV provide an accurate estimate for scan report delivery?
Response:
Comments:

8) Did the ASV attempt to market products or services for your company to attain PCI compliance?
Response:
Comments:
9) Did the ASV imply that use of a specific brand of commercial product or service was necessary to achieve compliance?
Response:
Comments:
10) In situations where remediation was required, did the ASV present product and/or solution options that were not exclusive to their own product set?
Response:
Comments:
11) Did the ASV use secure transmission to send any confidential reports or data?
Response:
Comments:
12) Did the ASV demonstrate courtesy, professionalism, and a constructive and positive approach?
Response:
Comments:
13) Was there sufficient opportunity for you to provide explanations and responses during the scans?
Response:
Comments:

14) During the review wrap-up, did the ASV clearly communicate findings and expected next steps?
Response:
Comments:
15) Did the ASV provide sufficient follow-up to address false positives until eventual scan compliance was achieved?
Response:
Comments:
Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.

ASV FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS	
Name of ASV Client (merchant or service provider reviewed):	**ASV Company Name:**
Payment Brand Reviewer:	ASV employee who performed assessment:
Name	Name
Telephone	Telephone
E-Mail	E-Mail
For each question, please indicate the response that best reflects your experience and provide comments. **4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree**	
1) Does the ASV clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?	
Response:	
Comments:	
2) Did you receive any complaints about ASV activities related to this scan?	
Response:	
Comments:	
3) Did the ASV demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures?	
Response:	
Comments:	