Trustwave®

Report Date: 2018-02-05

Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	HEMKO Systems Corporation		
Contact Name:	Harry Hemstreet	**Job Title:**	
Telephone:	970-667-0460	**E-mail:**	hhemstreet@hemko.com
Business Address:	5560 Stone Church Court		
City:	Loveland	**State/Province:**	Colorado
ZIP/Postal Code:	80537	**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:	2018-02-02	Scan expiration date (90 days from date scan completed):	2018-05-02
Compliance status:	Pass	Scan report type:	Full Scan
Number of unique in-scope components scanned:	2		
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

HEMKO Systems Corporation attests on 2018-02-02 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. HEMKO Systems Corporation 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 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

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	HEMKO Systems Corporation	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2018-02-02	Scan Expiration Date	2018-05-03

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	67.227.238.130	Pass
Component (IP Address, domain, etc):	69.167.163.100	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	67.227.238.130	TLSv1.0 Supported	Medium	5.00	Pass	**Auto-confirming appeal by false positive analysis** AUTO_CONFIRMED by false positive analysis **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
2	67.227.238.130	TLSv1.0 Supported	Medium	5.00	Pass	**Auto-confirming appeal by false positive analysis** AUTO_CONFIRMED by false positive analysis **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
						Note to scan customer:

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)
3	67.227.238.130	No X-FRAME-OPTIONS Header	Low	2.60	Pass	This vulnerability is not recognized in the National Vulnerability Database.
4	67.227.238.130	Auto-Completion Enabled for Password Fields	Low	1.20	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
5	67.227.238.130	.ida/idq ISAPI Mappings	Low	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
6	67.227.238.130	.htr ISAPI Mappings	Info	0.00	Pass	
7	67.227.238.130	Discovered Web Applications	Info	0.00	Pass	
8	67.227.238.130	Discovered Web Directories	Info	0.00	Pass	
9	67.227.238.130	Enumerated Applications	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
10	67.227.238.130	Enumerated Hostnames	Info	0.00	Pass	
11	67.227.238.130	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
12	67.227.238.130	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
13	67.227.238.130	No Hostname Entered For This Web Server	Info	0.00	Pass	
14	67.227.238.130	Non-HttpOnly Session Cookies	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
		Identified				Database.
15	67.227.238.130	Non-Secure Session Cookies Identified	Info	0.00	Pass	
16	67.227.238.130	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
17	67.227.238.130	SSL Certificate is Not Trusted	Info	0.00	Pass	
18	67.227.238.130	SSL-TLS Certificate Information	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
19	67.227.238.130	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST), CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 4.30 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0.
20	67.227.238.130	Unknown services found	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.
- Configure the SSL service(s) running on this host to adhere to information security best practices.
- Ensure that any web applications running on this host is configured following industry security best practices.

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
• Ensure that any web applications running on this host properly validate and transmit user input in a secure manner.						
21	69.167.163.100	TLSv1.0 Supported	Medium	5.00	Pass	**Auto-confirming appeal by false positive analysis** AUTO_CONFIRMED by false positive analysis **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
22	69.167.163.100	TLSv1.0 Supported	Medium	5.00	Pass	**Auto-confirming appeal by false positive analysis** AUTO_CONFIRMED by false positive analysis **Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
23	69.167.163.100	No X-FRAME-OPTIONS Header	Low	2.60	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
24	69.167.163.100	Auto-Completion Enabled for Password Fields	Low	1.20	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
25	69.167.163.100	.ida/idq ISAPI Mappings	Low	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.

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)
26	69.167.163.100	.htr ISAPI Mappings	Info	0.00	Pass	
27	69.167.163.100	Discovered Web Applications	Info	0.00	Pass	
28	69.167.163.100	Discovered Web Directories	Info	0.00	Pass	
29	69.167.163.100	Enumerated Applications	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
30	69.167.163.100	Enumerated Hostnames	Info	0.00	Pass	
31	69.167.163.100	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
32	69.167.163.100	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
33	69.167.163.100	No Hostname Entered For This Web Server	Info	0.00	Pass	
34	69.167.163.100	Non-HttpOnly Session Cookies Identified	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
35	69.167.163.100	Non-Secure Session Cookies Identified	Info	0.00	Pass	
36	69.167.163.100	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
37	69.167.163.100	SSL Certificate is Not Trusted	Info	0.00	Pass	

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
38	69.167.163.100	SSL-TLS Certificate Information	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
39	69.167.163.100	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST), CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 4.30 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0.
40	69.167.163.100	Unknown services found	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.
- Configure the SSL service(s) running on this host to adhere to information security best practices.
- 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
1	67.227.238.130	Unknown services		

#	Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed
2	69.167.163.100	Unknown services		

Part 3c. Special Notes - Full Text

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 Address/ranges/subnets, domains, URLs, etc.
IP Address: 67.227.238.130
IP Address: 69.167.163.100

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

IP Address/ranges/subnets, domains, URLs, etc.
67.227.238.130 / e.mybookingmanager.com
69.167.163.100 / webmail.planetreg.com

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

IP Address/ranges/subnets, domains, URLs, etc.
No Data

ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	HEMKO Systems Corporation	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2018-02-02	Scan Expiration Date	2018-05-03

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.

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/80 This host does not appear to utilize the benefits that the X-FRAME-

ASV Scan Report Vulnerability Details

67.227.238.130						
#	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: http://67.227.238.130/Admin/ Headers: {"cache-control"=>["private"], "content-length"=>["1179"], "content-type"=>["text/html"], "server"=>["Microsoft-IIS/7.5"], "set-cookie"=>["ASPSESSIONIDCARCARTB=KMPPANCCOJNIKALKPLFLHNHH; path=/"], "x-powered-by"=>["ASP.NET"], "date"=>["Fri, 02 Feb 2018 18:29:09 GMT"]} **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
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

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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://67.227.238.130/Admin/ Headers: {"cache-control"=>["private"], "content-length"=>["1179"], "content-type"=>["text/html"], "server"=>["Microsoft-IIS/7.5"], "set-cookie"=>["ASPSESSIONIDCARCARTB=MGFABNCCIJCKOLOAFCBMKGBF; path=/"], "x-powered-by"=>["ASP.NET"], "date"=>["Fri, 02 Feb 2018 18:32:27 GMT"]} **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
3		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

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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://67.227.238.130/login_MBM.asp Form Name: form1 Action: https://67.227.238.130/login_MBM.asp?1=LI Fields: txtPassword (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.
4		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/80 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	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:** Request: GET /trustkeeper12345.ida HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 1513 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=GBOABNCCFGHOBADBMELDJGJP; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:45 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
5		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/80 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.idq HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 1513 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=HBOABNCCFNBHLLCDBLMMBEAH; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:45 GMT

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
6		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/443 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.ida HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cache-Control: private Content-Length: 1513 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=MBOABNCCLEJLOMHPDEEAFMMB; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:45 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
7		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/443 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.idq HTTP/1.1

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 1513 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=KBOABNCCHIGHJCMFHHHJLHHK; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:45 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
8		No Hostname Entered For This Web Server	0.00	Info	Pass	**Port:** tcp/80 This host is running a web server and does not have a fully-qualified domain name (i.e. www.example.com) associated with it. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: If your organization owns a domain name that corresponds to this web server, add it to the scan parameters from within the TrustKeeper portal.
9		.htr ISAPI Mappings	0.00	Info	Pass	**Port:** tcp/80 Microsoft HTR extensions are known to have numerous serious security vulnerabilities. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.htr HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 1513 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=EBOABNCCJFDHKNLMEHOGEDGE; path=/

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:44 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
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 **Remediation:** No remediation is required.
11		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	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.
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:** CPE: microsoft:asp.net URI: / Version: 2.0.50727 **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
13		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.
14		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://67.227.238.130:80/admin/ HTTP Response Code: 200 URL: http://67.227.238.130:80/_utils/ HTTP Response Code: 403 URL: http://67.227.238.130:80/api/soap/?wsdl HTTP Response Code: 302 URL: http://67.227.238.130:80/_archive/

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://67.227.238.130:80/_backup/ URL: http://67.227.238.130:80/_cti_pvt/ URL: http://67.227.238.130:80/_derived/ URL: http://67.227.238.130:80/_errors/ URL: http://67.227.238.130:80/_fpclass/ URL: http://67.227.238.130:80/_mem_bin/ URL: http://67.227.238.130:80/_notes/ URL: http://67.227.238.130:80/_objects/ URL: http://67.227.238.130:80/_old/ URL: http://67.227.238.130:80/_pages/ URL: http://67.227.238.130:80/_passwords/ URL: http://67.227.238.130:80/_private/ URL: http://67.227.238.130:80/_ScriptLibrary/ URL: http://67.227.238.130:80/_scripts/ URL: http://67.227.238.130:80/_sharedtemplates/ URL: http://67.227.238.130:80/_tests/ URL: http://67.227.238.130:80/_themes/ URL: http://67.227.238.130:80/_vti_bin/ URL: http://67.227.238.130:80/_vti_bot/ URL: http://67.227.238.130:80/_vti_log/ URL: http://67.227.238.130:80/_vti_pvt/ URL: http://67.227.238.130:80/_vti_shm/ URL: http://67.227.238.130:80/_vti_txt/ URL: http://67.227.238.130:80/Admin/ URL: http://67.227.238.130:80/css/ URL: http://67.227.238.130:80/datafiles/ URL: http://67.227.238.130:80/db/ URL: http://67.227.238.130:80/graphics/ URL: http://67.227.238.130:80/images/

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://67.227.238.130:80/includes/ URL: http://67.227.238.130:80/stylesheets/ URL: http://67.227.238.130:80/temp/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
15		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:**

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130/Admin/stylesheets/default.css **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
16		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack.

67.227.238.130						
#	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://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130/Admin/stylesheets/index.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
17		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130/Admin/stylesheets/login_MBM.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
18		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130/Admin/stylesheets/stylesheets/default.css **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
19		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130/Admin/stylesheets/stylesheets/index.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
20		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://67.227.238.130:80/Admin/

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
21		Non-HttpOnly Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/80 The website software running on this server appears to be setting session cookies without the HttpOnly flag set. This means the session identifier information in these cookies is susceptible to attacks such as Cross-site Scripting which may allow attackers to read this cookie's data. **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly.aspx https://www.owasp.org/index.php/HttpOnly **Evidence:** URL: http://67.227.238.130/Admin/ Cookie Name: ASPSESSIONIDCARCARTB Cookie Value: KMPPANCCOJNIKALKPLFLHNHH Cookie HttpOnly Flag: false **Remediation:**

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Contact the vendor of this web application and request the HttpOnly flag be set on session cookies.
22		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/443 It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /OU=Domain Control Validated/CN=e.mybookingmanager.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starfieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired. Please note the port associated with this finding. This finding may NOT be originating from port 443,

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						which is what most online testing tools check by default.
23		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/443 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /OU=Domain Control Validated/CN=e.mybookingmanager.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starfieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2 Certificate Chain Depth: 0 Hostnames provided to scanner: 67.227.238.130 Subject Name: e.mybookingmanager.com Subject Alternative Name: e.mybookingmanager.com Subject Alternative Name: www.e.mybookingmanager.com **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally,

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						check your DNS servers to ensure that the domain name is properly mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
24		No Hostname Entered For This Web Server	0.00	Info	Pass	**Port:** tcp/443 This host is running a web server and does not have a fully-qualified domain name (i.e. www.example.com) associated with it. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** If your organization owns a domain name that corresponds to this web server, add it to the scan parameters from within the TrustKeeper portal.
25	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/443 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g.

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
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

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 **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 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA 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

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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-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.
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: false Today: 2018-02-02 12:34:45 -0600 Start date: 2017-02-07 13:56:02 UTC End date: 2018-05-08 22:48:03 UTC Expired: false

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Fingerprint: DB:5E:38:B7:97:27:81:AB:BD:64:D2:1A:60:B3:D6:00 Subject: /OU=Domain Control Validated/CN=e.mybookingmanager.com Common name: e.mybookingmanager.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starfieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2 Signature Algorithm: sha256WithRSAEncryption Version: 2
28		.htr ISAPI Mappings	0.00	Info	Pass	**Port:** tcp/443 Microsoft HTR extensions are known to have numerous serious security vulnerabilities. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.htr HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 67.227.238.130 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 1513 Content-Type: text/html

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARCARTB=JBOABNCCEAPINKFIGPJPEMBF; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:49:45 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
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: microsoft:iis URI: / Version: 7.5 **Remediation:** No remediation is required.
30		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:.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

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
32		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.
33		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://67.227.238.130:443/admin/ HTTP Response Code: 200 URL: https://67.227.238.130:443/_utils/ HTTP Response Code: 302 URL: https://67.227.238.130:443/api/soap/?wsdl URL: https://67.227.238.130:443/_archive/

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://67.227.238.130:443/_backup/ URL: https://67.227.238.130:443/_cti_pvt/ URL: https://67.227.238.130:443/_derived/ URL: https://67.227.238.130:443/_errors/ URL: https://67.227.238.130:443/_fpclass/ URL: https://67.227.238.130:443/_mem_bin/ URL: https://67.227.238.130:443/_notes/ URL: https://67.227.238.130:443/_objects/ URL: https://67.227.238.130:443/_old/ URL: https://67.227.238.130:443/_pages/ URL: https://67.227.238.130:443/_passwords/ URL: https://67.227.238.130:443/_private/ URL: https://67.227.238.130:443/_ScriptLibrary/ URL: https://67.227.238.130:443/_scripts/ URL: https://67.227.238.130:443/_sharedtemplates/ URL: https://67.227.238.130:443/_tests/ URL: https://67.227.238.130:443/_themes/ URL: https://67.227.238.130:443/_vti_bin/ URL: https://67.227.238.130:443/_vti_bot/ URL: https://67.227.238.130:443/_vti_log/ URL: https://67.227.238.130:443/_vti_pvt/ URL: https://67.227.238.130:443/_vti_shm/ URL: https://67.227.238.130:443/_vti_txt/ URL: https://67.227.238.130:443/Admin/ URL: https://67.227.238.130:443/css/ URL: https://67.227.238.130:443/datafiles/ URL: https://67.227.238.130:443/db/ URL: https://67.227.238.130:443/graphics/ URL: https://67.227.238.130:443/images/

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://67.227.238.130:443/includes/ URL: https://67.227.238.130:443/stylesheets/ URL: https://67.227.238.130:443/temp/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
34		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:**

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130/Admin/stylesheets/default.css **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
35		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack.

67.227.238.130						
#	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://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130/Admin/stylesheets/index.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
36		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130/Admin/stylesheets/login_MBM.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
37		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130/Admin/stylesheets/stylesheets/default.css **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
38		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130/Admin/stylesheets/stylesheets/index.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
39		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://67.227.238.130:443/Admin/

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
40		Non-HttpOnly Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/443 The website software running on this server appears to be setting session cookies without the HttpOnly flag set. This means the session identifier information in these cookies is susceptible to attacks such as Cross-site Scripting which may allow attackers to read this cookie's data. **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly.aspx https://www.owasp.org/index.php/HttpOnly **Evidence:** URL: https://67.227.238.130/Admin/ Cookie Name: ASPSESSIONIDCARCARTB Cookie Value: MGFABNCCIJCKOLOAFCBMKGBF Cookie HttpOnly Flag: false **Remediation:**

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Contact the vendor of this web application and request the HttpOnly flag be set on session cookies.
41		Non-Secure Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/443 The website software running on this server appears to be setting session cookies without the Secure flag set over HTTPS connections. This means the session identifier information in these cookies would be transmitted even over unencrypted HTTP connections, which might make them susceptible to interception and tampering. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** https://www.owasp.org/index.php/SecureFlag **Evidence:** URL: https://67.227.238.130/ Cookie Name: ASPSESSIONIDCARCARTB Cookie Value: MOHABNCCBKJGFDBKHILNHOJL Cookie Secure Flag: false **Remediation:** Contact the vendor of this web application and request the Secure flag be set on session cookies transmitted over HTTPS.
42		SSL Certificate is Not	0.00	Info	Pass	**Port:** tcp/3389

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Trusted				It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
43		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/3389 This SSL certificate has a common name (CN) that does not appear to

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Hostnames provided to scanner: 67.227.238.130 Subject Name: www.planetreg.com Subject Alternative Name: www.planetreg.com Subject Alternative Name: planetreg.com **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure that the domain name is properly mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
44	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0	0.00	Info	Pass	**Port:** tcp/3389

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Vulnerable to CBC Attacks via chosen-plaintext (BEAST)				This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
45		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/3389 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 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA 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-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-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.
46		SSL-TLS Certificate Information	0.00	Info	Pass	**Port:** tcp/3389 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:** generic_ssl

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Verified: false Today: 2018-02-02 12:34:54 -0600 Start date: 2015-11-26 16:53:38 UTC End date: 2018-11-26 16:53:38 UTC Expired: false Fingerprint: 77:E9:BA:86:FD:E6:98:05:85:97:53:58:E7:EC:AF:EB Subject: /OU=Domain Control Validated/CN=www.planetreg.com Common name: www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Signature Algorithm: sha256WithRSAEncryption Version: 2
47		Enumerated Hostnames	0.00	Info	Pass	This list contains all hostnames discovered during the scan that are believed to belong to this host. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Hostname: e.mybookingmanager.com, Source: SSL Certificate Subject Common Name Hostname: e.mybookingmanager.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: www.e.mybookingmanager.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: www.planetreg.com, Source: SSL Certificate Subject Common Name Hostname: www.planetreg.com, Source: SSL Certificate Subject subjectAltName DNS

ASV Scan Report Vulnerability Details

67.227.238.130						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Hostname: planetreg.com, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.
48		Unknown services found	0.00	Info	Pass	The finding reports all ports and protocols that couldn't be remotely identified. Particular items may indicate uncommon but safe protocols or in-house application that uses custom and/or proprietary protocol. However they can as well indicate malicious activity (backdoors, rootkits, any other types of malware). This finding is purely informational. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Unknown Service: transport protocol: tcp, port: 3389, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 49154, ssl: false, banner: (N/A) **Remediation:** Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/80 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: http://69.167.163.100/Admin/ Headers: {"cache-control"=>["private"], "content-length"=>["1189"], "content-type"=>["text/html"], "server"=>["Microsoft-IIS/7.5"], "set-cookie"=>["ASPSESSIONIDCARABSSA=BLJKKNDCFJKDPLMCCNEPNEAH; path=/"], "x-powered-by"=>["ASP.NET"], "date"=>["Fri, 02 Feb 2018 18:29:09 GMT"]} **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
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-

ASV Scan Report Vulnerability Details

69.167.163.100						
#	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://69.167.163.100/Admin/ Headers: {"cache-control"=>["private"], "content-length"=>["1189"], "content-type"=>["text/html"], "server"=>["Microsoft-IIS/7.5"], "set-cookie"=>["ASPSESSIONIDCARABSSA=PHPKKNDCCPGNFJBCPAJAKIJD; path=/"], "x-powered-by"=>["ASP.NET"], "date"=>["Fri, 02 Feb 2018 18:32:30 GMT"]} **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
3		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.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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://69.167.163.100/login.asp?1=LI Form Name: form1 Action: https://69.167.163.100/login.asp?1=LI Fields: txtPassword (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.
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.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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://69.167.163.100/login.asp Form Name: form1 Action: https://69.167.163.100:443/login.asp?1=LI Fields: txtPassword (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.
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.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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://69.167.163.100/add_account.asp Form Name: form1 Action: https://69.167.163.100/forgot.asp?1=LU Fields: txtPassword (password), txtPassword2 (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.
6		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/80 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.ida HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 7358 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=DFJLKNDCGBNLCPNEICNKBHOD; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:11 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
7		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/80 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.idq HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 7358 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=BFJLKNDCLOKLKOMCJFJJGKGI; path=/

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:11 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
8		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/443 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.ida HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 7358 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=FFJLKNDCPAHHFCBGILJAMOOF; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:12 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
9		.ida/idq ISAPI Mappings	0.00	Low	Pass	**Port:** tcp/443 Microsoft IIS provides a search capability via the Internet Data Query service. This ISAPI extension is known to have numerous serious security vulnerabilities, including the ones that were used in the Code Red exploit. Your service appears to have .ida and .idq file extensions mapped to this ISAPI extension. Note that this test simply checks to see if the mapping is enabled, and does not validate specific vulnerabilities in the service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Request: GET /trustkeeper12345.idq HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 7358 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=HFJLKNDCGCPGJIFKHNEBKAOK; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:12 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
10		No Hostname Entered For This Web Server	0.00	Info	Pass	**Port:** tcp/80 This host is running a web server and does not have a fully-qualified domain name (i.e. www.example.com) associated with it.

69.167.163.100						
#	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 **Remediation:** If your organization owns a domain name that corresponds to this web server, add it to the scan parameters from within the TrustKeeper portal.
11		.htr ISAPI Mappings	0.00	Info	Pass	**Port:** tcp/80 Microsoft HTR extensions are known to have numerous serious security vulnerabilities. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.htr HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private Content-Length: 7358 Content-Type: text/html

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=OEJLKNDCBDMAALJAEBEACLIA; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:11 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
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:** CPE: microsoft:iis URI: / Version: 7.5 **Remediation:** No remediation is required.
13		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
14		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.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
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. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://69.167.163.100:80/admin/ HTTP Response Code: 200 URL: http://69.167.163.100:80/_utils/ HTTP Response Code: 403 URL: http://69.167.163.100:80/api/soap/?wsdl HTTP Response Code: 302

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://69.167.163.100:80/_archive/ URL: http://69.167.163.100:80/_backup/ URL: http://69.167.163.100:80/_cti_pvt/ URL: http://69.167.163.100:80/_derived/ URL: http://69.167.163.100:80/_errors/ URL: http://69.167.163.100:80/_fpclass/ URL: http://69.167.163.100:80/_mem_bin/ URL: http://69.167.163.100:80/_notes/ URL: http://69.167.163.100:80/_objects/ URL: http://69.167.163.100:80/_old/ URL: http://69.167.163.100:80/_pages/ URL: http://69.167.163.100:80/_passwords/ URL: http://69.167.163.100:80/_private/ URL: http://69.167.163.100:80/_ScriptLibrary/ URL: http://69.167.163.100:80/_scripts/ URL: http://69.167.163.100:80/_sharedtemplates/ URL: http://69.167.163.100:80/_tests/ URL: http://69.167.163.100:80/_themes/ URL: http://69.167.163.100:80/_vti_bin/ URL: http://69.167.163.100:80/_vti_bot/ URL: http://69.167.163.100:80/_vti_log/ URL: http://69.167.163.100:80/_vti_pvt/ URL: http://69.167.163.100:80/_vti_shm/ URL: http://69.167.163.100:80/_vti_txt/ URL: http://69.167.163.100:80/Admin/ URL: http://69.167.163.100:80/css/ URL: http://69.167.163.100:80/datafiles/ URL: http://69.167.163.100:80/db/ URL: http://69.167.163.100:80/graphics/

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://69.167.163.100:80/images/ URL: http://69.167.163.100:80/includes/ URL: http://69.167.163.100:80/stylesheets/ URL: http://69.167.163.100:80/temp/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
17		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100/Admin/stylesheets/about.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
18		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack.

69.167.163.100						
#	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://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100/Admin/stylesheets/association_events.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
19		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100/Admin/stylesheets/bible_school.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
20		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta'

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100/Admin/stylesheets/camp_registration.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
21		HTTP Responses Missing	0.00	Info	Pass	**Port:** tcp/80

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Character Encoding				During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100/Admin/stylesheets/charity_events.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						encoding.
22		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://69.167.163.100:80/Admin/

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
23		Non-HttpOnly Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/80 The website software running on this server appears to be setting session cookies without the HttpOnly flag set. This means the session identifier information in these cookies is susceptible to attacks such as Cross-site Scripting which may allow attackers to read this cookie's data. **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly.aspx https://www.owasp.org/index.php/HttpOnly **Evidence:** URL: http://69.167.163.100/Admin/ Cookie Name: ASPSESSIONIDCARABSSA Cookie Value: BLJKKNDCFJKDPLMCCNEPNEAH Cookie HttpOnly Flag: false

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Contact the vendor of this web application and request the HttpOnly flag be set on session cookies.
24		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/443 It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired. Please note the port associated

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
25		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/443 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Hostnames provided to scanner: 69.167.163.100 Subject Name: www.planetreg.com Subject Alternative Name: www.planetreg.com Subject Alternative Name: planetreg.com **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure that the domain name is properly mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
26		No Hostname Entered For This Web Server	0.00	Info	Pass	**Port:** tcp/443 This host is running a web server and does not have a fully-qualified domain name (i.e. www.example.com) associated with it. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** If your organization owns a domain name that corresponds to this web server, add it to the scan parameters from within the TrustKeeper portal.
27	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/443 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
28		Enumerated SSL/TLS Cipher	0.00	Info	Pass	**Port:** tcp/443

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Suites				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 **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 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : AES128-SHA 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-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.
29		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: false Today: 2018-02-02 13:37:30 -0600 Start date: 2015-11-26 16:53:38 UTC End date: 2018-11-26 16:53:38 UTC

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Expired: false Fingerprint: 77:E9:BA:86:FD:E6:98:05:85:97:53:58:E7:EC:AF:EB Subject: /OU=Domain Control Validated/CN=www.planetreg.com Common name: www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Signature Algorithm: sha256WithRSAEncryption Version: 2
30		.htr ISAPI Mappings	0.00	Info	Pass	**Port:** tcp/443 Microsoft HTR extensions are known to have numerous serious security vulnerabilities. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Request: GET /trustkeeper12345.htr HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: 69.167.163.100 Content-Type: text/html Content-Length: 0 Response: HTTP/1.1 200 OK Cache-Control: private

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Content-Length: 7358 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDCARABSSA=EFJLKNDCBGBHEAHPDPPMCGPJ; path=/ X-Powered-By: ASP.NET Date: Fri, 02 Feb 2018 18:50:11 GMT Status code: equals '200' **Remediation:** Unmap all unnecessary ISAPI extensions. Install all current IIS security patches in order to reduce risk associated with required ISAPI extensions.
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:iis URI: / Version: 7.5 **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
32		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:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
33		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:**

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						No remediation is required.
34		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.
35		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://69.167.163.100:443/admin/ HTTP Response Code: 200 URL: https://69.167.163.100:443/_utils/ HTTP Response Code: 302 URL: https://69.167.163.100:443/api/soap/?wsdl

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://69.167.163.100:443/_archive/ URL: https://69.167.163.100:443/_backup/ URL: https://69.167.163.100:443/_cti_pvt/ URL: https://69.167.163.100:443/_derived/ URL: https://69.167.163.100:443/_errors/ URL: https://69.167.163.100:443/_fpclass/ URL: https://69.167.163.100:443/_mem_bin/ URL: https://69.167.163.100:443/_notes/ URL: https://69.167.163.100:443/_objects/ URL: https://69.167.163.100:443/_old/ URL: https://69.167.163.100:443/_pages/ URL: https://69.167.163.100:443/_passwords/ URL: https://69.167.163.100:443/_private/ URL: https://69.167.163.100:443/_ScriptLibrary/ URL: https://69.167.163.100:443/_scripts/ URL: https://69.167.163.100:443/_sharedtemplates/ URL: https://69.167.163.100:443/_tests/ URL: https://69.167.163.100:443/_themes/ URL: https://69.167.163.100:443/_vti_bin/ URL: https://69.167.163.100:443/_vti_bot/ URL: https://69.167.163.100:443/_vti_log/ URL: https://69.167.163.100:443/_vti_pvt/ URL: https://69.167.163.100:443/_vti_shm/ URL: https://69.167.163.100:443/_vti_txt/ URL: https://69.167.163.100:443/Admin/ URL: https://69.167.163.100:443/css/ URL: https://69.167.163.100:443/datafiles/ URL: https://69.167.163.100:443/db/ URL: https://69.167.163.100:443/graphics/

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://69.167.163.100:443/images/ URL: https://69.167.163.100:443/includes/ URL: https://69.167.163.100:443/stylesheets/ URL: https://69.167.163.100:443/temp/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
36		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100/Admin/stylesheets/about.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
37		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack.

69.167.163.100						
#	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://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100/Admin/stylesheets/association_events.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
38		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100/Admin/stylesheets/bible_school.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
39		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta'

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100/Admin/stylesheets/camp_registration.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
40		HTTP Responses Missing	0.00	Info	Pass	**Port:** tcp/443

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Character Encoding				During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100/Admin/stylesheets/charity_events.asp **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						encoding.
41		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://69.167.163.100:443/Admin/

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
42		Non-HttpOnly Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/443 The website software running on this server appears to be setting session cookies without the HttpOnly flag set. This means the session identifier information in these cookies is susceptible to attacks such as Cross-site Scripting which may allow attackers to read this cookie's data. **CVSSv2:** AV:N/AC:H/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly.aspx https://www.owasp.org/index.php/HttpOnly **Evidence:** URL: https://69.167.163.100/Admin/ Cookie Name: ASPSESSIONIDCARABSSA Cookie Value: PHPKKNDCCPGNFJBCPAJAKIJD Cookie HttpOnly Flag: false

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Contact the vendor of this web application and request the HttpOnly flag be set on session cookies.
43		Non-Secure Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/443 The website software running on this server appears to be setting session cookies without the Secure flag set over HTTPS connections. This means the session identifier information in these cookies would be transmitted even over unencrypted HTTP connections, which might make them susceptible to interception and tampering. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** https://www.owasp.org/index.php/SecureFlag **Evidence:** URL: https://69.167.163.100/ Cookie Name: ASPSESSIONIDCARABSSA Cookie Value: EBCLKNDCMPCAJFFOLIKFCOPJ Cookie Secure Flag: false **Remediation:** Contact the vendor of this web application and request the Secure flag be set on session cookies transmitted over HTTPS.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
44		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/3389 It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
45		SSL Certificate Common	0.00	Info	Pass	**Port:** tcp/3389

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Name Does Not Validate				This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Evidence:** Subject: /OU=Domain Control Validated/CN=www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Hostnames provided to scanner: 69.167.163.100 Subject Name: www.planetreg.com Subject Alternative Name: www.planetreg.com Subject Alternative Name: planetreg.com **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure that the domain name is properly mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
46	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/3389 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2,

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
47		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/3389 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 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:**

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA 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-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-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.
48		SSL-TLS Certificate Information	0.00	Info	Pass	**Port:** tcp/3389 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:** generic_ssl

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Verified: false Today: 2018-02-02 13:37:41 -0600 Start date: 2015-11-26 16:53:38 UTC End date: 2018-11-26 16:53:38 UTC Expired: false Fingerprint: 77:E9:BA:86:FD:E6:98:05:85:97:53:58:E7:EC:AF:EB Subject: /OU=Domain Control Validated/CN=www.planetreg.com Common name: www.planetreg.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Signature Algorithm: sha256WithRSAEncryption Version: 2
49		Enumerated Hostnames	0.00	Info	Pass	This list contains all hostnames discovered during the scan that are believed to belong to this host. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Hostname: www.planetreg.com, Source: SSL Certificate Subject Common Name Hostname: www.planetreg.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: planetreg.com, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.

ASV Scan Report Vulnerability Details

69.167.163.100						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
50		Unknown services found	0.00	Info	Pass	The finding reports all ports and protocols that couldn't be remotely identified. Particular items may indicate uncommon but safe protocols or in-house application that uses custom and/or proprietary protocol. However they can as well indicate malicious activity (backdoors, rootkits, any other types of malware). This finding is purely informational. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Unknown Service: transport protocol: tcp, port: 3389, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 49154, ssl: false, banner: (N/A) **Remediation:** Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

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:	