Scan Vulnerabilities Report

VTI3 NET LIMITED

June 07 2025

PREPARED BY:
SecurityMetrics
1275 W. 1600 N.
Orem, UT 84057

Executive Summary

Scan target: **app.turquoipay.com**	Maximum Score: **1.00**	Start: **2025-06-07 13:39:43**
Scan ID: **12735306**	Scan Expiration: **2025-09-07**	Finish: **2025-06-07 14:14:36**
Scan Compliance Status: **Passing**	TCP/IP Fingerprint PS Estimate: **Ubuntu 16.04 Linux Kernel 4.4**	Scan Length: **0:34:53**

Introduction

SecurityMetrics has determined that VTI3 NET limited is COMPLIANT with the PCI scan validation requirement for this target.
Congratulations, the target **passes** because no failing vulnerability was found.

Port Scan

Attackers use a port scan to find out what programs are running on your system. Most programs have known security weaknesses, so it is best practice to disable any unnecessary programs listed below.

Protocol	Port	Program
TCP	443	Amazon CloudFront httpd
TCP	80	Amazon CloudFront httpd

Scan Results

The following section lists all security vulnerabilities detected on your system. Vulnerabilities which cause you to fail PCI compliance have a score of 4.0 or higher and are listed in red.

Security Vulnerabilities

Protocol	Port	Service	Score	Summary
TCP	None	general	✓ 1.00	**Title:** OS Fingerprints Detected **Synopsis:** Multiple OS fingerprints were detected. **Impact:** Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here. **Resolution:** n/a **Data Received:** Following OS Fingerprints were found Remote operating system : Ubuntu 16.04 Linux Kernel 4.4 Confidence level : 56 Method : MLSinFP Type : unknown Fingerprint : unknown Remote operating system : Linux Kernel 2.x Confidence level : 54 Method : SinFP Type : general-purpose Fingerprint : SinFP: P1:B10113:F0x12:W65535:O0204ffff:M1440: P2:B10113:F0x12:W65535:O0204ffff0402080affffffff4445414401030309:M1440: P3:B00000:F0x00:W0:O0:M0 P4:190802_7_p=80R Following fingerprints could not be used to determine OS : HTTP:!:Server: CloudFront SSLcert:!:i/CN:Amazon RSA 2048 M03i/O:Amazons/CN:*.app.turquoipay.com 11b62f9b2644a2fd0584c65424559660b7f9b813

TCP	80	http_proxy	✓ 1.00	**Title:** Web Server No 404 Error Code Check **Synopsis:** The remote web server does not return 404 error codes. **Impact:** The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Resolution:** n/a **Data Received:** CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : http://app.turquoipay.com/ABbQPKni0OWp.html
TCP	80	http_proxy	✓ 1.00	**Title:** HyperText Transfer Protocol (HTTP) Redirect Information **Synopsis:** The remote web server redirects requests to the root directory. **Impact:** The remote web server issues an HTTP redirect when requesting the root directory of the web server. This plugin is informational only and does not denote a security problem. **Resolution:** Analyze the redirect(s) to verify that this is valid operation for your web server and/or application. **Data Received:** Request : http://app.turquoipay.com/ HTTP response : HTTP/1.1 301 Moved Permanently Redirect to : https://app.turquoipay.com/ Redirect type : 30x redirect Note that SecurityMetrics did not receive a 200 OK response from the last examined redirect.

TCP	443	http_proxy	✓ 1.00	**Title:** Web Server Crafted Request Vendor/Version Information Disclosure **Synopsis:** The remote host is running a web server that may be leaking information. **Impact:** The web server running on the remote host appears to be hiding its version or name, which is a good thing. However, using a specially crafted request, SecurityMetrics was able to discover the information. **Resolution:** No generic solution is known. Contact your vendor for a fix or a workaround. **Data Received:** After sending this request : HELP SecurityMetrics was able to gather the following information from the web server : CloudFront
TCP	443	http_proxy	✓ 1.00	**Title:** SSL / TLS Versions Supported **Synopsis:** The remote service encrypts communications. **Impact:** This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. **Resolution:** n/a **Data Received:** This port supports TLSv1.3/TLSv1.2.

TCP	443	http_proxy	✓ 1.00	**Title:** SSL Certificate Information **Synopsis:** This plugin displays the SSL certificate. **Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. **Resolution:** n/a **Data Received:** Subject Name: Common Name: *.app.turquoipay.com Issuer Name: Country: US Organization: Amazon Common Name: Amazon RSA 2048 M03 Serial Number: 07 E6 B3 B5 0C 67 9E 3F 74 8C 36 8A E0 0A 4F 01 Version: 3 Signature Algorithm: SHA-256 With RSA Encryption Not Valid Before: Mar 31 00:00:00 2025 GMT Not Valid After: Apr 30 23:59:59 2026 GMT Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 DA 96 FF A8 05 FA 35 A0 9F 67 61 A9 BC F5 FE DD CF DB B6 70 CD B3 25 E9 D3 52 66 1F FF D7 EA 13 F6 A3 B2 36 9C 25 09 19 19 A7 48 2F E7 B3 05 31 7B 60 8A B1 4A D7 60 03 E6 22 AE 18 4C DA 36 D6 9D 27 A3 F8 46 E9 69 AF 12 83 AB BA 9D E2 40 AC 08 27 49 C8 E7 2C A6 FE A8 C4 05 C8 D4 65 98 3A 8C EA 20 64 CA 91 9F 78 ED 32 29 A1 CE 85 06 29 F3 23 C5 BB 5F 9D B0 C2 70 99 5B B6 4B FB D2 62 52 CE C3 D7 FD C8 3A 85 7B 2C 41 CE B9 B6 CD 65 BA 27 C1 01 C5 2B F8 58 C2 3F D2 E2 4B C5 C5 D7 15 E8 AB A5 A1 60 31 6E D1 71 AA E2 0D A7 89 9B B0 06 CC BD 4B 85 63 09 35 25 EB 6A 83 BF 27 86 E5 D6 1C 01 44 76 F3 DF E3 1C 0F 73 15 6F 0E 8D 11 58 B4 7A 0A D5 4B F5 14 3D 52 AE 87 BD ED 23 25 3D 7B 60 AD B2 76 0F 53 50 29 36 13 AE C4 85 08 87 58 5F B0 0E 98 2C 6A 3F 7A 5E 58 FD 3A FB Exponent: 01 00 01 Signature Length: 256 bytes / 2048 bits Signature: 00 B3 EB 0E 50 C8 11 3B D7 B2 4F 34 F2 2B F3 54 41 4D 8C BE AF 65 94 38 CB A8 28 C1 46 FB 06 80 46 34 62 4A 5F AA 67 E6 6F 04 52 E0 2A 25 15 CB 3A A7 CF 00 6A A2 29 5B 65 B2 B5 F3 B7 26 3C 61 14 31 F5 9F C7 53 B2 4B 14 96 70 ED FC D2 7F 97 64 60 4B 2A 00 24 03 54 8B EF C5 15 87 AE 96 8D 1E 73 E0 65 6D 55 2D F4 1F 03 CC 8B 71 7E 29 E1 54 32 B0 4F E9 EF 63 72 40 FC 64 F7 0F 57 CB 71 58 4F CA D7 A8 54 3A 50 A7 E9 68 D9 C7 00 82 7B 5D 2A 83 F9 85 18 C9 BA 12 FB 99 BD 28 2C D9 67 A7 68 EB 49 A8 30 97 AD DB E9 2F 11 E4 CC 67 EA 86 0D 76 3C 39 F3 55 2A 17 F1 01 A5 DB 50 D2 C1 5D 16 9C A6 DA 46 DF C9 7B D3 93 05 F9 CF 9C E7 FE 83 0A 77 4A 07 98 C5 81 09 0E 09 0C 95 E6 B7 88 04 09 90 70 4D 36 D7 CC EA D1 6A BF D0 02 41 6D E0 98 A1 C5 5B 21 51 6C AC 11 75 56 58 2D 07 21 Extension: Authority Key Identifier (2.5.29.35) Critical: 0 Key Identifier: 55 D9 18 5F D2 1C CC 01 E1 58 B4 BE AB D9 55 42 01 D7 2E 02 Extension: Subject Key Identifier (2.5.29.14) Critical: 0 Subject Key Identifier: 3A 13 43 A3 F0 B5 C3 C9 4A CC 4E DF 2E 6C CF D7 DB 1E 54 72 Extension: Subject Alternative Name (2.5.29.17) Critical: 0 DNS: *.app.turquoipay.com DNS: app.turquoipay.com Extension: Policies (2.5.29.32) Critical: 0 Policy ID #1: 2.23.140.1.2.1 Extension: Key Usage (2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment Extension: Extended Key Usage (2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication

				(1.3.6.1.5.5.7.3.2) Extension: CRL Distribution Points (2.5.29.31) Critical: 0 URI: http://crl.r2m03.amazontrust.com/r2m03.crl Extension: Authority Information Access (1.3.6.1.5.5.7.1.1) Critical: 0 Method#1: Online Certificate Status Protocol URI: http://ocsp.r2m03.amazontrust.com Method#2: Certificate Authority Issuers URI: http://crt.r2m03.amazontrust.com/r2m03.cer Extension: Basic Constraints (2.5.29.19) Critical: 1 Extension: 1.3.6.1.4.1.11129.2.4.2 Critical: 0 Data: 04 82 01 6B 01 69 00 77 00 96 97 64 BF 55 58 97 AD F7 43 87 68 37 08 42 77 E9 F0 3A D5 F6 A4 F3 36 6E 46 A4 3F 0F CA A9 C6 00 00 01 95 E9 A4 69 74 00 00 04 03 00 48 30 46 02 21 00 C1 E2 F9 F8 49 A1 C1 35 79 AF C3 67 4E BB E7 28 B7 7C A3 92 1B 31 B1 FE 4C 08 03 97 89 C0 A4 34 02 21 00 EE E5 AB 41 5C EA 1E B9 88 19 CC 1C A4 0D BE 93 A4 D7 10 AD 9B 6F D3 6E 6C 43 A9 CE 4A BC 46 47 00 75 00 64 11 C4 6C A4 12 EC A7 89 1C A2 02 2E 00 BC AB 4F 28 07 D4 1E 35 27 AB EA FE D5 03 C9 7D CD F0 00 00 01 95 E9 A4 69 67 00 00 04 03 00 46 30 44 02 20 33 BC 32 53 AD 95 33 6E 23 89 C0 5C 08 58 70 EC E2 87 56 38 5A 66 29 88 82 F6 40 CB 49 F2 DE 4B 02 20 28 8A 01 C6 1C 10 02 3B FF 15 C6 B8 8B 58 B3 D3 87 CC 7A EB A3 AC 9A 41 38 1E 44 B4 1D 07 1F 55 00 77 00 49 9C 9B 69 DE 1D 7C EC FC 36 DE CD 87 64 A6 B8 5B AF 0A 87 80 19 D1 55 52 FB E9 EB 29 DD F8 C3 00 00 01 95 E9 A4 69 79 00 00 04 03 00 48 30 46 02 21 00 AA 5C A7 22 71 60 DF 39 FB AD 22 16 5A 19 85 BD 11 CE 6E FA D8 4B F4 D0 AC B7 A0 20 08 AC 98 C1 02 21 00 AB 13 23 9F 38 8B 32 45 35 70 72 8A E4 1E 86 61 BD E6 74 E3 20 BE 7E 76 65 BA 7C 64 B8 9E AE 4D Fingerprints : SHA-256 Fingerprint: 7C A7 8D 24 4C 09 CA 90 E9 E1 12 98 2F E0 38 79 DA 84 5C F2 27 7D CE 56 3E 80 6D 9F 4A 90 A6 64 SHA-1 Fingerprint: 11 B6 2F 9B 26 44 A2 FD 05 84 C6 54 24 55 96 60 B7 F9 B8 13 MD5 Fingerprint: 76 4E A0 28 DD E9 A5 E1 B4 C2 90 EF 9A F4 38 2B PEM certificate : -----BEGIN CERTIFICATE----- MIIF6TCCBNGgAwIBAgIQB+aztQxnnj90jDaK4ApPATANBgkqhkiG9w0BAQsFADA8MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRwwGgYDVQQDExNBbWF6b24gUlNBIDIwNDggTTAzMB4XDTI1MDMzMTAwMDAwMFoXDTI2MDQzMDIzNTk1OVowHzEdMBsGA1UEAwwUKi5hcHAudHVycXVvaXBheS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDalv+oBfo1oJ9nYam89f7dz9u2cM2zJenTUmYf/9fqE/ajsjacJQkZGadIL+ezBTF7YIqxStdgA+YirhhM2jbWnSej+Ebpaa8Sg6u6neJArAgnScjnLKb+qMQFyNRlmDqM6iBkypGfeO0yKaHOhQYp8yPFu1+dsMJwmVu2S/vSYlLOw9f9yDqFeyxBzrm2zWW6J8EBxSv4WMI/0uJLxcXXFeirpaFgMW7RcariDaeJm7AGzL1LhWMJNSXraoO/J4bl1hwBRHbz3+McD3MVbw6NEVi0egrVS/UUPVKuh73tIyU9e2CtsnYPU1ApNhOuxIUIh1hfsA6YLGo/el5Y/Tr7AgMBAAGjggMCMIIC/jAfBgNVHSMEGDAWgBRV2Rhf0hzMAeFYtL6r2VVCAdcuAjAdBgNVHQ4EFgQUOhNDo/C1w8lKzE7fLmzP19seVHIwMwYDVR0RBCwwKoIUKi5hcHAudHVycXVvaXBheS5jb22CEmFwcC50dXJxdW9pcGF5LmNvbTATBgNVHSAEDDAKMAgGBmeBDAECATAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwucjJtMDMuYW1hem9udHJ1c3QuY29tL3IybTAzLmNybDB1BggrBgEFBQcBAQRpMGcwLQYIKwYBBQUHMAGGIWh0dHA6Ly9vY3NwLnIybTAzLmFtYXpvbnRydXN0LmNvbTA2BggrBgEFBQcwAoYqaHR0cDovL2NydC5yMm0wMy5hbWF6b250cnVzdC5jb20vcjJtMDMuY2VyMAwGA1UdEwEB/wQCMAAwggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB3AJaXZL9VWJet90OHaDcIQnfp8DrV9qTzNm5GpD8PyqnGAAABlemkaXQAAAQDAEgwRgIhAMHi+fhJocE1ea/DZ0675yi3fKOSGzGx/kwIA5eJwKQ0AiEA7uWrQVzqHrmIGcwcpA2+k6TXEK2bb9NubEOpzkq8RkcAdQBkEcRspBLsp4kcogIuALyrTygH1B41J6vq/tUDyX3N8AAAAZXppGlnAAAEAwBGMEQCIDO8MlOtlTNuI4nAXAhYcOzih1Y4WmYpiIL2QMtJ8t5LAiAoigHGHBACO/8VxriLWLPTh8x666OsmkE4HkS0HQcfVQB3AEmcm2neHXzs/DbezYdkprhbrwqHgBnRVVL76esp3fjDAAABlemkaXkAAAQDAEgwRgIhAKpcpyJxYN85+60iFloZhb0Rzm762Ev00Ky3oCAIrJjBAiEAqxMjnziLMkU1cHKK5B6GYb3md

				OMgvn52Zbp8ZLierk0wDQYJKoZIhvcNAQELBQADggEBALPrDlDIETvXsk808ivzVEFNjL6vZZQ4y6gowUb7BoBGNGJKX6pn5m8EUuAqJRXLOqfPAGqiKVtlsrXztyY8YRQx9Z/HU7JLFJZw7fzSf5dkYEsqACQDVIvvxRWHrpaNHnPgZW1VLfQfA8yLcX4p4VQysE/p72NyQPxk9w9Xy3FYT8rXqFQ6UKfpaNnHAIJ7XSqD+YUYyboS+5m9KCzZZ6do60moMJet2+kvEeTMZ+qGDXY8OfNVKhfxAaXbUNLBXRacptpG38l705MF+c+c5/6DCndKB5jFgQkOCQyV5reIBAmQcE0218zq0Wq/0AJBbeCYocVbIVFsrBF1VlgtByE= -----END CERTIFICATE-----
TCP	443	http_proxy	✓ 1.00	**Title:** SSL Root Certification Authority Certificate Information **Synopsis:** A root Certification Authority certificate was found at the top of the certificate chain. **Impact:** The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. See also : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10) **Resolution:** Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. **Data Received:** The following root Certification Authority certificate was found : |-Subject : C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services Root Certificate Authority - G2 |-Issuer : C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services Root Certificate Authority - G2 |-Valid From : Sep 01 00:00:00 2009 GMT |-Valid To : Dec 31 23:59:59 2037 GMT |-Signature Algorithm : SHA-256 With RSA Encryption

TCP	443	http_proxy	✓ 1.00	**Title:** SSL Cipher Suites Supported **Synopsis:** The remote service encrypts communications using SSL. **Impact:** This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. See also : https://www.openssl.org/docs/man1.0.2/man1/ciphers.html http://www.nessus.org/u?e17ffced **Resolution:** n/a **Data Received:** Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv13 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------------------- ---------- --- ---- ---------------------- --- TLS_AES_128_GCM_SHA256 0x13, 0x01 - - AES-GCM(128) AEAD TLS_AES_256_GCM_SHA384 0x13, 0x02 - - AES-GCM(256) AEAD TLS_CHACHA20_POLY1305_SHA256 0x13, 0x03 - - ChaCha20-Poly1305(256) AEAD SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------------------- ---------- --- ---- ---------------------- --- ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8 ECDH RSA ChaCha20-Poly1305(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}

TCP	443	http_proxy	✓ 1.00	**Title:** TLS Version 1.3 Protocol Detection **Synopsis:** The remote service encrypts traffic using a version of TLS. **Impact:** The remote service accepts connections encrypted using TLS 1.3. See also : https://tools.ietf.org/html/rfc8446 **Resolution:** N/A **Data Received:** TLSv1.3 is enabled and the server supports at least one cipher.
TCP	443	http_proxy	✓ 1.00	**Title:** TLS Version 1.2 Protocol Detection **Synopsis:** The remote service encrypts traffic using a version of TLS. **Impact:** The remote service accepts connections encrypted using TLS 1.2. See also : https://tools.ietf.org/html/rfc5246 **Resolution:** N/A **Data Received:** TLSv1.2 is enabled and the server supports at least one cipher.

TCP	443	http_proxy	✓ 1.00	**Title:** TLS ALPN Supported Protocol Enumeration **Synopsis:** The remote host supports the TLS ALPN extension. **Impact:** The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports. See also : https://tools.ietf.org/html/rfc7301 **Resolution:** n/a **Data Received:** http/1.1 h2
TCP	443	http_proxy	✓ 1.00	**Title:** Web Server No 404 Error Code Check **Synopsis:** The remote web server does not return 404 error codes. **Impact:** The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Resolution:** n/a **Data Received:** The following title tag will be used : TurquoiPay

TCP	443	http_proxy	✓ 1.00	**Title:** HSTS Missing From HTTPS Server **Synopsis:** The remote web server is not enforcing HSTS. **Impact:** The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. See also : https://tools.ietf.org/html/rfc6797 **Resolution:** Configure the remote web server to use HSTS. For Nginx see: https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/ For Apache see: https://linux-audit.com/configure-hsts-http-strict-transport-security-apache-nginx/ Microsoft Azure/ISS: https://docs.microsoft.com/en-us/azure/frontdoor/front-door-security-headers https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts General: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://https.cio.gov/hsts/ **Data Received:** HTTP/1.1 400 Bad Request Server: CloudFront Date: Sat, 07 Jun 2025 19:48:09 GMT Content-Type: text/html Content-Length: 915 Connection: close X-Cache: Error from cloudfront Via: 1.1 f084fd1d3261276af092a09384ea9af4.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ORD56-P2 X-Amz-Cf-Id: t1ra0aq2mY_cH_Au0yGLWH8SH_IVlS90oPMUazN6ufJZQPw_dKMDpA== The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

TCP	443	http_proxy	✓ 1.00	**Title:** Web Application Sitemap **Synopsis:** The remote web server hosts linkable content that can be crawled by SecurityMetrics. **Impact:** The remote web server contains linkable content that can be used to gather information about a target. See also : http://www.nessus.org/u?5496c8d9 **Resolution:** n/a **Data Received:** The following sitemap was created from crawling linkable content on the target host : - https://app.turquoipay.com/ - https://app.turquoipay.com/assets/ - https://app.turquoipay.com/assets/index-Bqi9vLh_.css - https://app.turquoipay.com/logo.svg Attached is a copy of the sitemap file.
TCP	443	http_proxy	✓ 1.00	**Title:** Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header **Synopsis:** The remote web server does not take steps to mitigate a class of web application vulnerabilities. **Impact:** The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all. The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks. See also : http://www.nessus.org/u?55aa8f57 http://www.nessus.org/u?07cc2a06 https://content-security-policy.com/ https://www.w3.org/TR/CSP2/ **Resolution:** Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources. **Data Received:** The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy: - https://app.turquoipay.com/ - https://app.turquoipay.com/assets/

TCP	443	http_proxy	✓ 1.00	**Title:** Missing or Permissive X-Frame-Options HTTP Response Header **Synopsis:** The remote web server does not take steps to mitigate a class of web application vulnerabilities. **Impact:** The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all. The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors See also : https://en.wikipedia.org/wiki/Clickjacking http://www.nessus.org/u?399b1f56 **Resolution:** Set a properly configured X-Frame-Options header for all requested resources. **Data Received:** The following pages do not set a X-Frame-Options response header or set a permissive policy: - https://app.turquoipay.com/ - https://app.turquoipay.com/assets/
UDP	443	https?	✓ 1.00	**Title:** QUIC Service Detection **Synopsis:** The remote service(s) support the QUIC protocol. **Impact:** SecurityMetrics was able to detect that the remote service supports QUIC by sending a QUIC initial packet and receiving QUIC handshake messages in reply. **Resolution:** n/a **Data Received:** A QUIC server is running on this port.