

Payment Card Industry (PCI) Technical Report

11/21/2024

ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	Prymera Consulting Private Limited			Company:	Sectigo Limited		
Contact Name:	Dhruv Patel	Job Title:		Contact Name:	-	Job Title:	-
Telephone:		Email:	dhruv@remitso.com	Telephone:	-	Email:	-
Business Address:	Unit No 10, 16th Floor, Aurora Waterfront,			Business Address:	3rd Floor Building 26, Office Village Exchange Quay, Trafford Road		
City:	Kolkata	State/Province:		City:	Salford	State/Province:	None
ZIP/postal code:		Country:	India	ZIP/postal code:	M5 3EQ	Country:	United Kingdom
URL:				URL:	https://sectigo.com/		

A.3 Scan Status			
Date scan completed	11/21/2024	Scan expiration date (90 days from date scan completed)	02/19/2025
Compliance Status	PASS	Scan report type	Full scan
Number of unique in-scope components scanned			1
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

A.4 Scan Customer Attestation

Prymera Consulting Private Limited attests on 11/21/2024 at 18:50:28 GMT 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.

Prymera Consulting Private Limited 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 Sectigo Limited under certificate number 4172-01-17, according to internal processes that meet PCI DSS requirement 11.3.2 and the ASV Program Guide.

Sectigo Limited 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 N/A

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	Prymera Consulting Private Limited	ASV Company:	Sectigo Limited
Date scan was completed:	11/21/2024	Scan expiration date:	02/19/2025

Part 2. Component Compliance Summary

54.163.109.116, app.demo.remitso.com

PASS

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls <small>Noted by the ASV for this Vulnerability</small>
54.163.109.116, app.demo.remitso.com	38904 - OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent CVE-2023-38408	HIGH	9.8	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	42046 - OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion) CVE-2024-6387	HIGH	8.1	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38919 - OpenSSH Authentication Bypass Vulnerability CVE-2023-51767	HIGH	7	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38915 - OpenSSH OS Command Injection Vulnerability CVE-2023-51385	MED	6.5	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38928 - OpenSSH Incomplete Constrains Sensitive Information Disclosure Vulnerability CVE-2023-51384	MED	5.5	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38903 - OpenSSH Probable User Enumeration Vulnerability CVE-2016-20012	MED	5.3	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com port 22/tcp	38909 - SHA1 deprecated setting for SSH	LOW	3.7	PASS	The vulnerability is not included in the NVD. ASV Score = 3.7
54.163.109.116, app.demo.remitso.com	38900 - OpenSSH Public-Key Authentication Vulnerability CVE-2021-36368	LOW	3.7	PASS	

Part 3b. Special Notes to Scan Customer by Component

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

54.163.109.116	Embedded links or code from out-of-scope domains	150010 - External Links Discovered (Web Application: port 80/tcp)	<p>Yes - Actions Taken to Address Identified Risks Content Delivery Network (CDN):</p> <p>Verified the authenticity and security of cdnjs.cloudflare.com as a trusted source. Considered self-hosting critical external resources (e.g., animate.min.css) to eliminate dependency on third-party CDNs. Google reCAPTCHA:</p> <p>Evaluated the API key configuration to ensure it complies with data protection regulations. Restricted API usage to specific domains to prevent abuse. Documentation Links:</p> <p>Confirmed that links to documentation (cakephp.org) are for developer reference only and do not impact production security. Google Fonts:</p> <p>Evaluated the feasibility of self-hosting required fonts to reduce dependency on external services. General Safeguards:</p> <p>Implemented Subresource Integrity (SRI) for external scripts and styles where applicable. Enforced HTTPS for all external resources to ensure secure transmission. Reviewed and updated the Content Security Policy (CSP) to restrict access to trusted domains only.</p>
54.163.109.116	Embedded links or code from out-of-scope domains	150010 - External Links Discovered (Web Application: port 443/tcp)	<p>Yes - Actions Taken to Address Identified Risks Content Delivery Network (CDN):</p> <p>Verified the authenticity and security of cdnjs.cloudflare.com as a trusted source. Considered self-hosting critical external resources (e.g., animate.min.css) to eliminate dependency on third-party CDNs. Google reCAPTCHA:</p> <p>Evaluated the API key configuration to ensure it complies with data protection regulations. Restricted API usage to specific domains to prevent abuse. Documentation Links:</p> <p>Confirmed that links to documentation (cakephp.org) are for developer reference only and do not impact production security. Google Fonts:</p> <p>Evaluated the feasibility of self-hosting required fonts to reduce dependency on external services. General Safeguards:</p> <p>Implemented Subresource Integrity (SRI) for external scripts and styles where applicable. Enforced HTTPS for all external resources to ensure secure transmission. Reviewed and updated the Content Security Policy (CSP) to restrict access to trusted domains only.</p>
54.163.109.116	Remote Access	42017 - Remote Access or Management Service Detected (SSH:port 22/TCP)	<p>Yes - SSH access is now limited to specific IP addresses belonging to authorized system administrators.</p>

Part 3c. Special Notes Full Text

Note

Embedded links or code from out-of-scope domains

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

Remote Access

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

Part 4a. Scope Submitted by Scan Customer for Discovery

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

54.163.109.116

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

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

54.163.109.116, app.demo.remitso.com

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

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

Evaluation

IP Addresses/Ranges : - (not active) Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.

Evaluation

Report Summary

Company:	Prymera Consulting Private Limited
Hosts in Account:	1 IP
Hosts Active:	1
Hosts Scanned:	1
Scan Date:	11/21/2024 at 10:56:23 GMT
Report Date:	11/21/2024 at 18:50:27 GMT
Report Title:	PCI Scan
Template Title:	Payment Card Industry (PCI) Technical Report

Summary of Vulnerabilities

Vulnerabilities Total	53	Average Security Risk		2.0
-----------------------	----	-----------------------	---	-----

by Severity

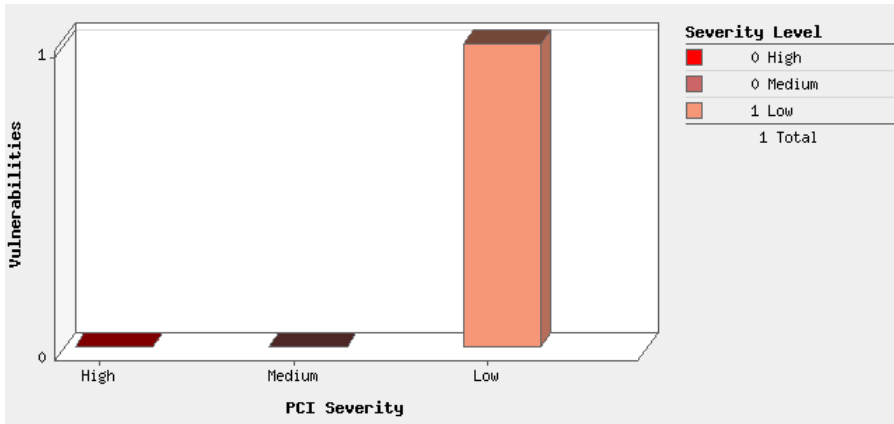
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	2	2
2	1	1	4	6
1	0	0	45	45
Total	1	1	51	53

by PCI Severity

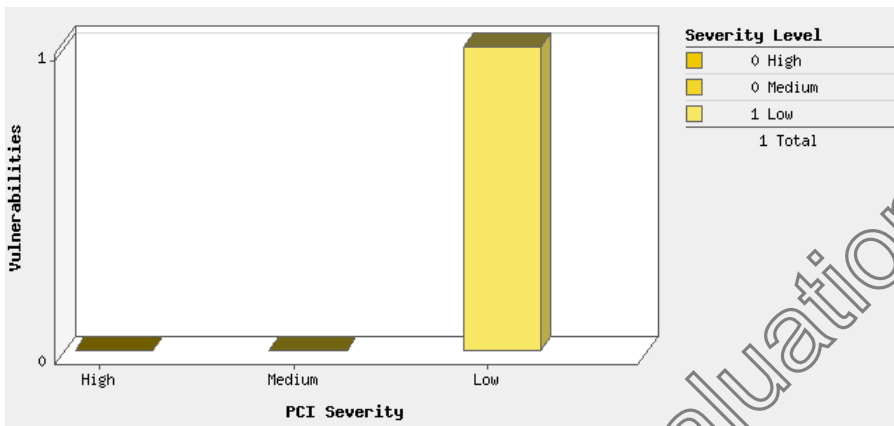
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	1	1	2
Total	1	1	2

Evaluation

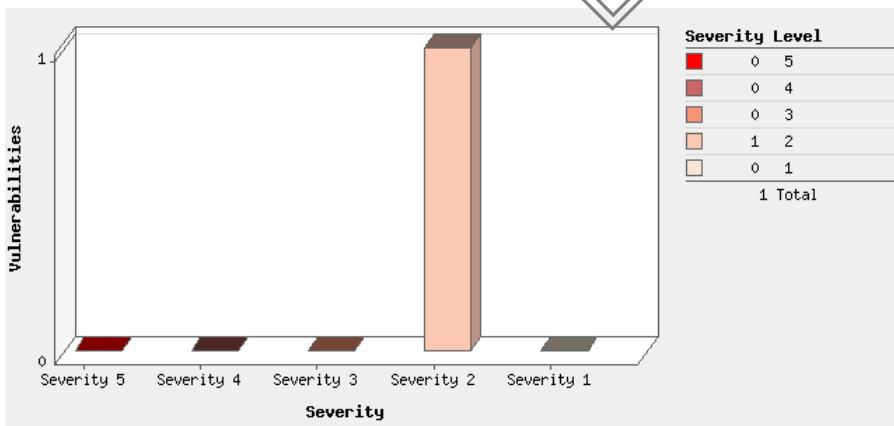
Vulnerabilities by PCI Severity



Potential Vulnerabilities by PCI Severity

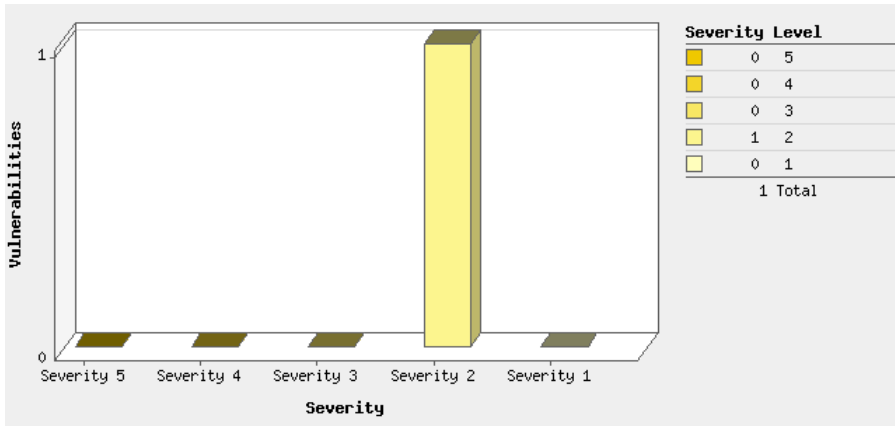


Vulnerabilities by Severity



Evaluation

Potential Vulnerabilities by Severity



Evaluation

Detailed Results

54.163.109.116 (app.demo.remitso.com,-)

Linux 2.6

Vulnerabilities Total

53

Security Risk

 2.0

Vulnerabilities (1)

SHA1 deprecated setting for SSH

port 22/tcp

PCI COMPLIANCE STATUS


PCI Severity:

 LOW

PASS

The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score: **3.7** AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS Temporal Score: **3.3** E:U/RL:W/RC:C
Severity: **2** 
QID: 38909
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/05/2024

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target is using deprecated SHA1 cryptographic settings to communicate.

IMPACT:

vulnerable to collision attacks, which are designed to fabricate the same hash value for different input data. each hash is supposedly unique.

SOLUTION:

Avoid using deprecated cryptographic settings.

Use best practices when configuring SSH.

Refer to NIST Retires SHA-1 Cryptographic Algorithm (SSH) (<https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm>) .

Other documents to refer

Deprecate settings listed for red hat (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.4_release_notes/chap-red_hat_enterprise_linux-7.4_release_notes-deprecated_functionality_in_rhel7)

Key exchange (<https://www.ietf.org/archive/id/draft-ietf-curdle-ssh-kex-sha2-13.html>)

CBC Cipher (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5161>)

SHA1 ietf reference (<https://datatracker.ietf.org/doc/html/rfc9142>)

Settings currently considered deprecated:

1.Key exchange algorithms:

diffie-hellman-group1-sha1, rsa1024sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, gss-gex-sha1-*, gss-group1-sha1-* and gss-group14-sha1-*

2.MAC:

hmac-sha1, hmac-sha1-96, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com

3.Host key:
ssh-rsa, ssh-dss, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com

RESULT:

Type	Name
MAC	hmac-sha1-etm@openssh.com
MAC	hmac-sha1

Potential Vulnerabilities (1)

OpenSSH Public-Key Authentication Vulnerability

PCI COMPLIANCE STATUS

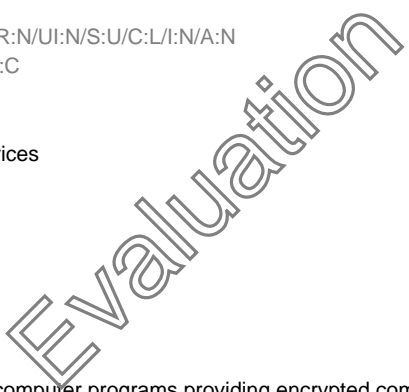
PCI Severity: LOW



The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score: **3.7** AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS Temporal Score: **3.2** E:U/RL:O/RC:C
Severity: **2**
QID: 38900
Category: General remote services
CVE ID: [CVE-2021-36368](#)
Vendor Reference: [OpenSSH 8.9](#)
Bugtraq ID: -
Last Update: 09/23/2024



THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH contains the following vulnerabilities:

CVE-2021-36368: If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf.

Affected Versions:
OpenSSH versions prior to 8.9

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows a remote attacker silently modify the server to support the None authentication option when a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose.

SOLUTION:

Customers are advised to upgrade to OpenSSH 8.9 (<https://www.openssh.com/>) or later to remediate these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 8.9 or later (<https://www.openssh.com/>)


Information Gathered (51)

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/04/2018

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
54.163.109.116	app.demo.remitso.com


Default Web Page (Follow HTTP Redirection)

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 13910
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/05/2020

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

SOLUTION:

Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (<https://www.qnap.com/en/security-advisory/nas-201911-01>)

RESULT:

GET / HTTP/1.1
Host: app.demo.remitso.com

Evaluation

Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">

<head>
  <!-- End Google Tag Manager -->
  <meta charset="utf-8"/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" />
  <link href="https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap" rel="stylesheet">
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css">
  <title>Send Money Abroad | International Money Transfer | DemoApp</title>

  <link rel="stylesheet" href="/css/style.css"/>
  <link rel="stylesheet" href="/vendors/iconfonts/mdi/font/css/materialdesignicons.min.css"/>
  <link rel="stylesheet" href="/vendors/iconfonts/flag-icon/css/flag-icon.min.css"/>
  <link rel="stylesheet" href="/vendors/gdpr/gdpr-cookie.css"/>
  <link rel="stylesheet" href="/assets/vendor/bootstrap/css/bootstrap.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/icofont/icofont.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/boxicons/css/boxicons.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/venobox/venobox.css"/>

  <script src="/vendors/js/vendor.bundle.base.js"></script>
</head>
<body itemtype="http://schema.org/WebPage">

  <link rel="stylesheet" href="/vendors/css/vendor.bundle.base.css"/>

  <header id="header">
    <div class="container d-flex align-items-center">
      <h1 class="logo"> (/)
      <nav class="nav-menu d-none d-lg-flex justify-content-between w-100">

        <li class="">
          Send Money (/send-money.html)

          <li class="">
            Login (/login.html)

          <li class="">
            Register (/register.html)

      </nav>
    </div>
  </header>
  <script>
    $(function () {
      setTimeout(function () {
        document.getElementById("top-header").classList.remove("hidden");
      }, 3000);
    });
  </script>

  <link rel="stylesheet" href="/css/paymentfont.min.css"/>

  <script src="/vendors/js/jquery.mask.min.js"></script>
  <style>
    #quoteForm .form-group.has-warning .form-control{
      border-color: #ffc21c;
      border-bottom-left-radius: 0;
    }
    #quoteForm .form-group.has-warning .input-group-append .input-group-text {
```

Evaluation

```

border-color: #ffc21c;
border-bottom-right-radius: 0;
}
#quoteForm .form-group.has-warning .feedback {
background-color: #ffc21c;
color: #fff;
}
#quoteForm p{
color: #121A41;
font-weight: 600;
}
/*#quoteForm .ui.dropdown .menu.left {*/
/* right: 0px !important;*/
/*}*/
#quoteForm .flag-icon.flag-icon-squared {
width: 1.4em;
line-height: 1.4em;
}
#quoteForm .search--input {
padding: 10px 18px;
}
#quoteForm .card-body {
padding: 2.25rem 2rem;
}

.send-money-list ul li {
line-height: 3;
}
.send-money-list ul li a {
font-weight: 600;
font-size: 1em;
display: flex;
align-items: center;
}
.send-money-list ul li a:hover
{
text-decoration: none;
}
.send-money-list ul li a i.bx{
font-size: 1.5rem;
}
.send-money-list .flag-icon.flag-icon-squared {
width: 1.5em;
line-height: 1.5em;
}
.country-nav-pills .nav-link.active, .country-nav-pills .show>.nav-link {
color: #007bff;
background-color: #fff;
border-bottom: 3px solid #007bff;
border-radius: 0;
border-top-left-radius: 5px;
border-top-right-radius: 5px;
}
.more-payout-country, .more-send-country {
display: none;
}

.nav-pills > li a
{
position: relative;
}
.nav-pills > li a.active:after {
position: absolute;
content: "";
width: 0;
height: 0;
border-left: 10px solid transparent;
border-right: 10px solid transparent;
border-top: 10px solid #000000;
left: 50%;
top: 100%;
margin-left: -10px;
}
.sending-heading
{
font-weight: 600;
font-size: 40px;
}

```

Evaluation

```

}
.pf.pf-credit-card.mr-1 {
  font-size: 1.50em;
  color: #9e9e9e;
  margin-top: 5px;
}
</style>
<section id="hero" class="d-flex align-items-center" style="margin-top: -1px">
  <div class="container">
    <div class="row align-items-center">
      <div class="hero-form-wrapper col-md-7 col-lg-6 col-xl-4">
        <h1 class="mob-visible">Spread joy this season with the gift everyone loves the gift of funds!
        <p class="py-4 mob-visible">Send money to family, friends, and cover bills affordablyanywhere, anytime.</p>
        <div class="header-banner">
          <form method="post" accept-charset="utf-8" id="quoteForm" action="/send-money.html"><div style="display:none;"><input type="hidden" name="_method"
value="POST"/><input type="hidden" name="_csrfToken" autocomplete="off"
value="f18ea8756849d7c46132f7a594e9e087e7cae18c2d6d593257a21f8edebefe677862d6695c5ca29bfc7e2a759e7dab2e7059c9fb530d779d3599d1b95cf2cc32"/></div>
<input type="hidden" name="payment_country_id" id="payment-country-id"/> <input type="hidden" name="payment_currency_id" id="payment-currency-id"/>
<input type="hidden" name="payout_country_id" id="payout-country-id" value="ad9a1212-2c72-4e50-b077-5cb3a1425692"/> <input
type="hidden" name="payout_currency_id" id="payout-currency-id"
value="efacdd7c-e346-4a0d-99fc-c05ba2b9e432"/> <div class="card shadow">
  <div class="card-body">
    <div class="alert alert-warning p-2 d-none"></div>
    <div class="form-group">
      <div class="input-group">
        <input type="text" name="send_amount" class="form-control border-right-0" placeholder="You send" id="send-amount" value="10000"/>
          <div class="input-group-append">
            <span class="input-group-text">
              <span class="flag-icon flag-icon-gb flag-icon-squared rounded-circle mr-2"></span>
              <span class="mr-4">GBP</span>
            </span>
          </div>
        </div>
      </div>
      <div class="fees cross-section form-group">
        <span class="text-theme float-right font-weight-bold">Transaction fees</span>
        <span class="ml-2">0.00</span>
      </div>
      <div class="convert cross-section form-group">
        <span class="text-theme float-right font-weight-bold">Converted amount</span>
        <span class="ml-2">100.00</span>
      </div>
      <div class="rate cross-section form-group">
        <span class="text-theme float-right font-weight-bold">Exchange rate</span>
        <span class="ml-2">20</span>
      </div>
    </div>
    <div class="input-group">
      <input type="text" name="payout_amount" class="form-control border-right-0" placeholder="Recipient gets" id="payout-amount"
value="200000"/>
      <div class="input-group-append">
        <span class="input-group-text">
          <span class="flag-icon flag-icon-gh flag-icon-squared rounded-circle mr-2"></span>
          <span class="mr-4">GHS</span>
        </span>
      </div>
    </div>
  </div>
  <div class="form-group">
    <button type="button" id="submitButton" class="btn btn-block btn-primary py-3">Get Started</button>
  </div>
  <p class="text-center text-theme">By clicking continue, you agree to our Terms and Conditions.</p>
  <div class="d-flex w-100 justify-content-center my-4 align-items-center">
    <span class="mx-1"><i class="pf pf-credit-card mr-1"> </span>
    <span class="mx-2"></span>
    <span class="mx-2"></span>
  </div>
  <p class="text-center text-theme">We are Authorised and Regulated by the Financial Conduct Authority (FCA).</p>
</div>
</div>
  </form> </div>
</div>
<div class="col-md-5 col-lg-6 pr-md-5 col-xl-6 offset-xl-1">
  Spread joy this season with the gift everyone loves the gift of funds!
  <p class="py-4">Send money to family, friends, and cover bills affordablyanywhere, anytime.</p>
  <div class="d-flex align-items-center">
     (javascript:)
  </div>

```

```

         (javascript:)
    </div>
</div>
</div>
</section>

```

```

<script type="text/javascript">

```

```

$(function(){
    $('.more-payout-button').click(function(event) {
        event.preventDefault();
        $('.more-payout-country').slideToggle();
        if ($(this).hasClass('expanded')) {
            $('.more-payout-country').removeClass("d-flex");
            $(this).removeClass('expanded');
            $(this).text('View More Options');
        } else {
            $(this).addClass('expanded');
            $(this).text('View Fewer Options');
            $('.more-payout-country').addClass("d-flex");
        }
    });
    $('.more-send-button').click(function(event) {
        event.preventDefault();
        $('.more-send-country').slideToggle();
        if ($(this).hasClass('expanded')) {
            $('.more-send-country').removeClass("d-flex");
            $(this).removeClass('expanded');
            $(this).text('View More Options');
        } else {
            $(this).addClass('expanded');
            $(this).text('View Fewer Options');
            $('.more-send-country').addClass("d-flex");
        }
    });
});

function getQuote(direction)
{
    let $url = '/orders/get-quote';
    $url += '?payment_country_id='+$("#payment-country-id").val();
    $url += '&payment_currency_id='+$("#payment-currency-id").val();
    $url += '&payout_country_id='+$("#payout-country-id").val();
    $url += '&payout_currency_id='+$("#payout-currency-id").val();
    if ( direction === "sending" ) {
        $url += '&send_amount='+$("#send-amount").val();
        $url += '&direction=sending';
    } else {
        $url += '&payout_amount='+$("#payout-amount").val();
        $url += '&direction=receiving';
    }
    $("#submitButton").addClass("disabled").attr("disabled", "disabled").text("Processing...");
    let $alert = $("#quoteForm").find(".alert").eq(0);
    $alert.addClass("d-none");
    $.ajax($url, {
        accepts: {
            json: 'application/json'
        },
        method: 'GET',
        cache: false,
        success: function (response) {
            // if ( response.messages.length > 0 ) {
            //     $alert
            //         .removeClass("d-none")
            //         .html('<div class="small mb-0 text-justify">'+response.messages[0]+'</div>');
            // }
            // }
            if ( response.resolved_issues.length > 0 ) {
                $.each(response.resolved_issues, function(item){
                    let $parameter = $("#quoteForm").find("[name='"+$(this).attr("param")+"'").eq(0);
                    if (typeof $parameter != 'undefined') {
                        $parameter.parents('.form-group').eq(0).addClass("has-warning");
                        let $errorContainer = $('<p />').addClass("mt-0 mb-0 p-3 feedback text-white").text($(this).attr("message"));
                        $parameter.parents('.form-group').append($errorContainer);
                    }
                });
            }
        }
    });
}

```

```

    });
  }
  $("#send-amount").val(response.send_amount);
  $("#payout-amount").val(response.payout_amount);

$("#quoteForm").find(".fees.cross-section").eq(0).find("span:last").html(response.total_cost_nice);
$("#quoteForm").find(".convert.cross-section").eq(0).find("span:last").html(response.send_amount_nice);
$("#quoteForm").find(".rate.cross-section").eq(0).find("span:last").html(response.sell_rate);
},
error: function(xhr, status, error) {
  if ( xhr.status === 400 ) {
  } else if ( xhr.status === 401 ) {
    window.location.href = '/';
  } else if ( xhr.status === 403 ) {
  } else if ( xhr.status === 404 ) {
  } else {
  }
},
complete: function(xhr, status) {
  $("#submitButton").removeClass("disabled").removeAttr("disabled").text("Get Started");
}
});
}(function(){
  $("#submitButton").on("click", function(e){
    e.preventDefault();
    e.stopPropagation();
    $("#submitButton").addClass("disabled").attr("disabled", "disabled").text("Processing...");
    window.location.href = $("#quoteForm").attr("action");
  });
  $("#send-amount").mask("000,000,000,000,000,000.00", {reverse: true});
  $("#send-amount").on("change", function(e){
    getQuote("sending");
  });
  $("#payout-amount").mask("000,000,000,000,000,000.00", {reverse: true});
  $("#payout-amount").on("change", function(e){
    getQuote("receiving");
  });
  $("#sourceDropdown").dropdown({
    fullTextSearch: "exact",
    onShow: function(){
      $elem = $(this);
      $inputGroup = $elem.parents(".input-group").eq(0);
      $elem.children(".menu").css("max-width", $inputGroup.width()+ 'px');
      $elem.children(".menu").css("min-width", $inputGroup.width()+ 'px');
      $elem.children(".menu").css("width", $inputGro
up.width()+ 'px');
    },
    onChange: function(value, text, choice){
      $icon = $('<i />')
        .addClass("flag-icon rounded-circle mr-2 flag-icon-squared")
        .addClass("flag-icon-"+$(choice).attr("data-country-iso").toLowerCase());
      $(choice).parents(".menu").eq(0).parents(".menu").eq(0).prev().prev().text("")
        .html($icon)
        .append($(choice).attr("data-currency-iso"));
      $("#payment-country-id").val($(choice).attr("data-country-id"));
      $("#payment-currency-id").val($(choice).attr("data-currency-id"));
      getQuote("sending");
    },
    selectOnKeydown: false,
    match: 'text',
    message: {
      noResults: 'No Results Found.'
    }
  });
  $("#sourceDropdown").dropdown("set selected", "5a44aa9e-a3d6-411e-9534-859cd4fa09ec_13e006a6-b459-4932-815d-ef289999ae45");
  $("#destinationDropdown").dropdown({
    fullTextSearch: "exact",
    onShow: function(){
      $elem = $(this);
      $inputGroup = $elem.parents(".input-group").eq(0);
      $elem.children(".menu").css("max-width", $inputGroup.width()+ 'px');
      $elem.children(".menu").css("min-width", $inputGroup.width()+ 'px');
      $elem.children(".menu").css("width", $inputGroup.width()+ 'px');
    },
    onChange: function(value, text, choice){
      $icon = $('<i />')

```



```

        .addClass("flag-icon rounded-circle mr-2 flag-icon-squared")
        .addClass("flag-icon-" + $(choice).attr("data-country-iso").toLowerCase());
    $(choice).parents(".menu").eq(0).parents(".menu").eq(0).prev().prev(".text")
        .html($icon)
        .append($(choice).attr("data-currency-iso"));
    $("#payout-country-id").val($(choice).attr("data-country-
id"));
    $("#payout-currency-id").val($(choice).attr("data-currency-id"));
    getQuote("sending");
    },
    selectOnKeydown: false,
    match: 'text',
    message: {
        noResults: 'No Results Found.'
    }
    });
    $('#destinationDropdown').dropdown("set selected", "ad9a1212-2c72-4e50-b077-5cb3a1425692_efacdd7c-e346-4a0d-99fc-c05ba2b9e432");
    });
</script>

```

```


<script src="/vendors/gdpr/gdpr-cookie.js"></script>
<script src="/assets/js/main.js"></script>
<script src="/assets/vendor/venobox/venobox.js"></script>
<script type="text/javascript">
    $(function(){
        $.gdprcookie.init({
            title: "",
            subtitle: "",
            message: "This website uses cookies to ensure you get the best experience on our website. Cookies Policy.",
            delay: 2000,
            expires: 30,
            cookieName: "cookieControlPrefs",
            acceptReload: false,
            acceptBtnLabel: "Got it!",
            advancedBtnLabel: "Customize cookies",
            customShowMessage: undefined,
            customHideMessage: undefined,
            customShowChecks: undefined,
            cookieTypes: [
                {
                    type: "Essential",
                    value: "essential",
                    description: "These are cookies that are essential for the website to work correctly."
                },
                {
                    type: "Site Preferences",
                    value: "preferences",
                    description: "These are cookies that are related to your site preferences, e.g. remembering your username, site colours, etc."
                },
                {
                    type: "Analytics",
                    value: "analytics",
                    description: "Cookies related to site visits, browser types, etc."
                },
                {
                    type:
"Marketing",
                    value: "marketing",
                    description: "Cookies related to marketing, e.g. newsletters, social media, etc"
                }
            ],
        });
    });
</script>
</body>
</html>
-CR-

```

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 12230

Category: CGI

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 03/16/2019

THREAT:

The Result section displays the default Web page for the Web server.

RESULT:

GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">

<head>
  <!-- End Google Tag Manager -->
  <meta charset="utf-8"/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" />
  <link href="https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap" rel="stylesheet">
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css">
  <title>Send Money Abroad | International Money Transfer | DemoApp</title>

  <link rel="stylesheet" href="/css/style.css"/>
  <link rel="stylesheet" href="/vendors/iconfonts/mdi/font/css/materialdesignicons.min.css"/>
  <link rel="stylesheet" href="/vendors/iconfonts/flag-icon/css/flag-icon.min.css"/>
  <link rel="stylesheet" href="/vendors/gdpr/gdpr-cookie.css"/>
  <link rel="stylesheet" href="/assets/vendor/bootstrap/css/bootstrap.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/icofont/icofont.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/boxicons/css/boxicons.min.css"/>
  <link rel="stylesheet" href="/assets/vendor/venobox/venobox.css"/>

  <script src="/vendors/js/vendor.bundle.base.js"></script>
</head>
<body itemtype="http://schema.org/WebPage">

  <link rel="stylesheet" href="/vendors/css/vendor.bundle.base.css"/>

  <header id="header">
    <div class="container d-flex align-items-center">
      <h1 class="logo"> (/)
      <nav class="nav-menu d-none d-lg-flex justify-content-between w-100">
```

```

        <li class="">
            Send Money (/send-money.html)

            <li class="">
                Login (/login
.html)

            <li class="">
                Register (/register.html)

        </nav>
    </div>
</header>
<script>
    $(function () {
        setTimeout(function () {
            document.getElementById("top-header").classList.remove("hidden");
        }, 3000);
    });
</script>

<link rel="stylesheet" href="/css/paymentfont.min.css"/>

<script src="/vendors/js/jquery.mask.min.js"></script>
<style>
    #quoteForm .form-group.has-warning .form-control{
        border-color: #ffc21c;
        border-bottom-left-radius: 0;
    }
    #quoteForm .form-group.has-warning .input-group-append .input-group-text {
        border-color: #ffc21c;
        border-bottom-right-radius: 0;
    }
    #quoteForm .form-group.has-warning .feedback {
        background-color: #ffc21c;
        color: #fff;
    }
    #quoteForm p{
        color: #121A41;
        font-weight: 600;
    }
    /*#quoteForm .ui.dropdown .menu.left {*/
    /* right: 0px !important;*/
    /*}*/
    #quoteForm .flag-icon.flag-icon-squared {
        width: 1.4em;
        line-height: 1.4em;
    }
    #quoteForm .search--input {
        padding: 10px 18px;
    }
    #quoteForm .card-body {
        padding: 2.25rem 2rem;
    }

    .send-money-list ul li {
        line-height: 3;
    }
    .send-money-list ul li a {
        font-weight: 600;
        font-size: 1em;
        display: flex;
        align-items: center;
    }
    .send-money-list ul li a:hover
    {
        text-decoration: none;
    }
    .send-money-list ul li a i.bx{
        font-size: 1.5rem;
    }
    .send-money-list .flag-icon.flag-icon-squared {
        width: 1.5em;
        line-height: 1.5em;
    }
}

```

Evaluation

```

.country-nav-pills .nav-link.active, .country-nav-pills .show>.nav-link {
  color: #007bff;
  background-color: #fff;
  border-bottom: 3px solid #007bff;
  border-radius: 0;
  border-top-left-radius: 5px;
  border-top-right-radius: 5px;
}
.more-payout-country, .more-send-country {
  display: none;
}

.nav-pills > li a
{
  position: relative;
}
.nav-pills > li a.active:after {
  position: absolute;
  content: "";
  width: 0;
  height: 0;
  border-left: 10px solid transparent;
  border-right: 10px solid transparent;
  border-top: 10px solid #000000;
  left: 50%;
  top: 100%;
  margin-left: -10px;
}
.sending-heading
{
  font-weight: 600;
  font-size: 40px;
}
.pf.pf-credit-card.mr-1 {
  font-size: 1.50em;
  color: #9e9e9e;
  margin-top: 5px;
}
</style>
<section id="hero" class="d-flex align-items-center" style="margin-top: 1px">
  <div class="container">
    <div class="row align-items-center">
      <div class="hero-form-wrapper col-md-7 col-lg-6 col-xl-4">
        <h1 class="mob-visible">Spread joy this season with the gift everyone loves the gift of funds!
        <p class="py-4 mob-visible">Send money to family, friends, and cover bills affordablyanywhere, anytime.</p>
        <div class="header-banner">
          <form method="post" accept-charset="utf-8" id="quoteForm" action="/send-money.html"><div style="display:none;"><input type="hidden" name="_method"
value="POST"/><input type="hidden" name="_csrfToken" autocomplete="off"
value="3b31be7424c01a0a2f53a1eb8962de203c14a41436d75370e5f5592492a6f75916375b81909c82021a40714db1461b83d9290a90ee65f3c5f1f848934366c745"/></div>
<input type="hidden" name="payment_country_id" id="payment-country-id"/> <input type="hidden" name="payment_currency_id" id="payment-currency-id"/>
<input type="hidden" name="payout_country_id" id="payout-country-id" value="ad9a1212-2c72-4e50-b077-5cb3a1425692"/> <input
type="hidden" name="payout_currency_id" id="payout-currency-id"
value="efacdd7c-e346-4a0d-99fc-c05ba2b9e432"/> <div class="card shadow">
  <div class="card-body">
    <div class="alert alert-warning p-2 d-none"></div>
    <div class="form-group">
      <div class="input-group">
        <input type="text" name="send_amount" class="form-control border-right-0" placeholder="You send" id="send-amount" value="10000"/>
        <div class="input-group-append">
          <span class="input-group-text">
            <span class="flag-icon flag-icon-gb flag-icon-squared rounded-circle mr-2"></span>
            <span class="mr-4">GBP</span>
          </span>
        </div>
      </div>
    </div>
    <div class="fees cross-section form-group">
      <span class="text-theme float-right font-weight-bold">Transaction fees</span>
      <span class="ml-2">0.00</span>
    </div>
    <div class="convert cross-section form-group">
      <span class="text-theme float-right font-weight-bold">Converted amount</span>
      <span class="ml-2">100.00</span>
    </div>
    <div class="rate cross-section form-group">
      <span class="text-theme float-right font-weight-bold">Exchange rate</span>
      <span class="ml-2">20</span>
    </div>
  </div>
</div>

```

```

        </div>
        <div class="form-group">
            <div class="input-group">
                <input type="text" name="payout_amount" class="form-control border-right-0" placeholder="Recipient gets" id="payout-amount"
value="200000"/>
                <div class="input-group-append">
                    <span class="input-group-text">
                        <span class="flag-icon flag-icon-gh flag-icon-squared rounded-circle mr-2"></span>
                        <span class="mr-4">GHS</span>
                    </span>
                </div>
            </div>
        </div>
        <div class="form-group">
            <button type="button" id="submitButton" class="btn btn-block btn-primary py-3">Get Started</button>
        </div>
        <p class="text-center text-theme">By clicking continue, you agree to our Terms and Conditions.</p>
        <div class="d-flex w-100 justify-content-center my-4 align-items-center">
            <span class="mx-1"><i class="pf pf-credit-card mr-1"> </span>
            <span class="mx-2"></span>
            <span class="mx-2"></span>
        </div>
        <p class="text-center text-theme">We are Authorised and Regulated by the Financial Conduct Authority (FCA).</p>
    </div>
</div>
</form>
</div>
</div>
<div class="col-md-5 col-lg-6 pr-md-5 col-xl-6 offset-xl-1">
    Spread joy this season with the gift everyone loves the gift of funds!
    <p class="py-4">Send money to family, friends, and cover bills affordablyanywhere, anytime.</p>
    <div class="d-flex align-items-center">
         (javascript:)
         (javascript:)
    </div>
</div>
</div>
</div>
</section>

```

```

<script type="text/javascript">
$(function(){
    $(' .more-payout-button').click(function(event) {
        event.preventDefault();
        $(' .more-payout-country').slideToggle();
        if ($(this).hasClass('expanded')) {
            $(' .more-payout-country').removeClass("d-flex");
            $(this).removeClass('expanded');
            $(this).text('View More Options');
        } else {
            $(this).addClass('expanded');
            $(this).text('View Fewer Options');
            $(' .more-payout-country').addClass("d-flex");
        }
    });
    $(' .more-send-button').click(function(event) {
        event.preventDefault();
        $(' .more-send-country').slideToggle();
        if ($(this).hasClass('expanded')) {
            $(' .more-send-country').removeClass("d-flex");
            $(this).removeClass('expanded');
            $(this).text('View More Options');
        } else {
            $(this).addClass('expanded');
            $(this).text('View Fewer Options');
            $(' .more-send-country').addClass("d-flex");
        }
    });
});

function getQuote(direction)
{
    let $url = '/orders/get-quote';
    $url += "?payment_country_id="+$("#payment-country-id"
).val();
    $url += "&payment_currency_id="+$("#payment-currency-id").val();
}

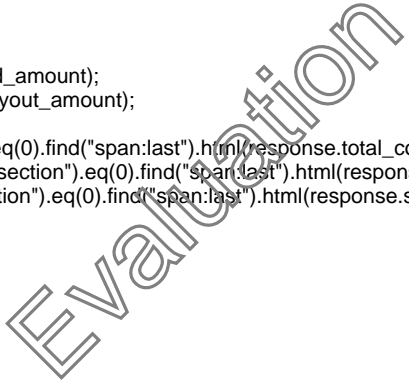
```

Evaluation

```

$url += '&payout_country_id='+$("#payout-country-id").val();
$url += '&payout_currency_id='+$("#payout-currency-id").val();
if ( direction === "sending" ) {
    $url += '&send_amount='+$("#send-amount").val();
    $url += '&direction=sending';
} else {
    $url += '&payout_amount='+$("#payout-amount").val();
    $url += '&direction=receiving';
}
$("#submitButton").addClass("disabled").attr("disabled", "disabled").text("Processing...");
let $alert = $("#quoteForm").find(".alert").eq(0);
$alert.addClass("d-none");
$.ajax($url, {
    accepts: {
        json: 'application/json'
    },
    method: 'GET',
    cache: false,
    success: function (response) {
        // if ( response.messages.length > 0 ) {
        //     $alert
        //         .removeClass("d-none")
        //         .html('<div class="small mb-0 text-justify">'+response.messages[0]+'</div>');
        // }
        // }
        if ( response.resolved_issues.length > 0 ) {
            $.each(response.resolved_issues, function(item){
                let $parameter = $("#quoteForm").find("[name='"+$(this).attr("param")+"'").eq(0);
                if (typeof $parameter != 'undefined') {
                    $parameter.parents('.form-group').eq(0).addClass("has-warning");
                    let $errorContainer = $('<p />').addClass("mt-0 mb-0 p-3 feedback text-white").text($(this).attr("message"));
                    $parameter.parents('.form-group').append($errorContainer);
                }
            });
        }
        $("#send-amount").val(response.send_amount);
        $("#payout-amount").val(response.payout_amount);
    },
    error: function(xhr, status, error) {
        if ( xhr.status === 400 ) {
        } else if ( xhr.status === 401 ) {
            window.location.href = '/';
        } else if ( xhr.status === 403 ) {
        } else if ( xhr.status === 404 ) {
        } else {
        }
    },
    complete: function(xhr, status) {
        $("#submitButton").removeClass("disabled").removeAttr("disabled").text("Get Started");
    }
});
}
$(function(){
    $("#submitButton").on("click", function(e){
        e.preventDefault();
        e.stopPropagation();
        $("#submitButton").addClass("disabled").attr("disabled", "disabled").text("Processing...");
        window.location.href = $("#quoteForm").attr("action");
    });
    $("#send-amount").mask("000,000,000,000,000,000.00", {reverse: true});
    $("#send-amount").on("change", function(e){
        getQuote("sending");
    });
    $("#payout-amount").mask("000,000,000,000,000,000.00", {reverse: true});
    $("#payout-amount").on("change", function(e){
        getQuote("receiving");
    });
    $("#sourceDropdown").dropdown({
        fullTextSearch: "exact",
        onShow: function(){
            $elem = $(this);
            $inputGroup = $elem.parents(".input-group").eq(0);
            $elem.children(".menu").css("max-width", $inputGroup.width()+10+'px');
        }
    });
}

```



```

        $elem.children(".menu").css("min-width", $inputGroup.width()+ 'px');
        $elem.children(".menu").css("width", $inputGro
up.width()+ 'px');
    },
    onChange: function(value, text, choice){
        $icon = $('<i />')
            .addClass("flag-icon rounded-circle mr-2 flag-icon-squared")
            .addClass("flag-icon-"+$(choice).attr("data-country-iso").toLowerCase());
        $(choice).parents(".menu").eq(0).parents(".menu").eq(0).prev().prev(".text")
            .html($icon)
            .append($(choice).attr("data-currency-iso"));
        $("#payment-country-id").val($(choice).attr("data-country-id"));
        $("#payment-currency-id").val($(choice).attr("data-currency-id"));
        getQuote("sending");
    },
    selectOnKeydown: false,
    match: 'text',
    message: {
        noResults: 'No Results Found.'
    }
}
});
$("#sourceDropdown").dropdown("set selected", "5a44aa9e-a3d6-411e-9534-859cd4fa09ec_13e006a6-b459-4932-815d-ef289999ae45");
$("#destinationDropdown").dropdown({
    fullTextSearch: "exact",
    onShow: function(){
        $elem = $(this);
        $inputGroup = $elem.parents(".input-group").eq(0);
        $elem.children(".menu").css("max-width", $inputGroup.width()+ 'px');
        $elem.children(".menu").css("min-width", $inputGroup.width()+ 'px');
        $elem.children(".menu").css("width", $inputGroup.width()+ 'px');
    },
    onChange: function(value, text, choice){
        $icon = $('<i />')
            .addClass("flag-icon rounded-circle mr-2 flag-icon-squared")
            .addClass("flag-icon-"+$(choice).attr("data-country-iso").toLowerCase());
        $(choice).parents(".menu").eq(0).parents(".menu").eq(0).prev().prev(".text")
            .html($icon)
            .append($(choice).attr("data-currency-iso"));
        $("#payout-country-id").val($(choice).attr("data-country-
id"));
        $("#payout-currency-id").val($(choice).attr("data-currency-id"));
        getQuote("sending");
    },
    selectOnKeydown: false,
    match: 'text',
    message: {
        noResults: 'No Results Found.'
    }
}
});
$("#destinationDropdown").dropdown("set selected", "ad9a1212-2c72-4e50-b077-5cb3a1425692_efacdd7c-e346-4a0d-99fc-c05ba2b9e432");
});
</script>

```

```

<script src="/vendors/gdpr/gdpr-cookie.js"></script>
<script src="/assets/js/main.js"></script>
<script src="/assets/vendor/venobox/venobox.js"></script>
<script type="text/javascript">
$(function(){
    $.gdprcookie.init({
        title: "",
        subtitle: "",
        message: "This website uses cookies to ensure you get the best experience on our website. Cookies Policy.",
        delay: 2000,
        expires: 30,
        cookieName: "cookieControlPrefs",
        acceptReload: false,
        acceptBtnLabel: "Got it!",
    });
});

```

```

advancedBtnLabel: "Customize cookies",
customShowMessage: undefined,
customHideMessage: undefined,
customShowChecks: undefined,
cookieTypes: [
  {
    type: "Essential",
    value: "essential",
    description: "These are cookies that are essential for the website to work correctly."
  },
  {
    type: "Site Preferences",
    value: "preferences",
    description: "These are cookies that are related to your site preferences, e.g. remembering your username, site colours, etc."
  },
  {
    type: "Analytics",
    value: "analytics",
    description: "Cookies related to site visits, browser types, etc."
  },
  {
    type:
"Marketing",
    value: "marketing",
    description: "Cookies related to marketing, e.g. newsletters, social media, etc"
  }
],
});
</script>
</body>
</html>
-CR-

```

SSL Certificate - Information

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID: 86002

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 03/07/2020

THREAT:

SSL certificate information is provided in the Results section.

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	04:d1:c6:b1:9a:eb:1b:70:a2:42:67:d0:01:98:2a:f9:18:d6
(0)Signature Algorithm	ecdsa-with-SHA384
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E5
(0)SUBJECT NAME	
commonName	app.demo.remitso.com

(0)Valid From	Oct 15 21:11:20 2024 GMT
(0)Valid Till	Jan 13 21:11:19 2025 GMT
(0)Public Key Algorithm	id-ecPublicKey
(0)EC Public Key	
(0)	Public-Key: (256 bit)
(0)	pub:
(0)	04:c3:0e:d2:92:ae:23:82:2f:67:b4:97:1d:fe:d2:
(0)	50:2b:c8:6f:85:23:98:78:43:4f:24:e0:71:60:83:
(0)	47:51:3d:e9:75:23:09:41:d5:a0:a3:80:ac:ab:ec:
(0)	90:e3:6a:0d:5b:34:b4:b5:77:8b:f4:20:a2:41:78:
(0)	d0:0d:70:c5:bd
(0)	ASN1 OID: prime256v1
(0)	NIST CURVE: P-256
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	AA:40:14:AE:C1:CE:15:42:39:0E:1C:A7:E1:AE:76:7D:1F:72:9F:43
(0)X509v3 Authority Key Identifier	keyid:9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D
(0)Authority Information Access	OCSP - URI:http://e5.o.lencr.org
(0)	CA Issuers - URI:http://e5.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:app.demo.remitso.com
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)CT Precertificate SCTs	Signed Certificate Timestamp
(0)	Version : v1 (0x0)
(0)	Log ID : E0:92:B3:FC:0C:1D:C8:E7:68:36:1F:DE:61:B9:96:4D:
(0)	0A:52:78:19:8A:72:D6:72:C4:B0:4D:A5:6D:6F:54:04
(0)	Timestamp : Oct 15 22:09:50.589 2024 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D1:A6:66:F5:74:C8:86:5B:25:02:06:
(0)	8D:89:D2:53:83:2C:D0:23:8E:FD:E4:C3:72:DA:26:2E:
(0)	DB:A0:95:13:39:02:20:04:48:7E:49:AA:34:2A:D3:D2:
(0)	79:55:6C:06:1F:41:10:D3:21:05:E9:0B:DF:C5:2A:5B:
(0)	A3:47:02:99:40:F8:49
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : CF:11:56:EE:D5:2E:7C:AF:F3:87:5B:D9:69:2E:9B:E9:
(0)	1A:71:67:4A:B0:17:EC:AC:01:D2:5B:77:CE:CC:3B:08
(0)	Timestamp : Oct 15 22:09:50.632 2024 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:B9:3F:8E:10:B6:5C:E1:D4:AB:41:90:
(0)	71:F9:FD:F5:4F:5C:A4:34:15:BB:FA:81:2B:C9:E6:EE:
(0)	D0:CA:A3:94:D6:02:21:00:EF:2B:90:E3:EA:E8:9F:27:
(0)	18:E0:85:0B:BE:6F:E9:AB:AD:BE:BD:94:29:D8:7C:FE:
(0)	F2:C9:B9:D5:1C:B7:20:43
(0)Signature	(104 octets)
(0)	30:66:02:31:00:cf:5a:e0:88:a5:64:68:35:35:8e:9b
(0)	da:67:21:8c:40:cd:3a:39:66:f3:e7:01:1f:e8:ed:bb
(0)	89:06:9d:5f:95:7b:da:bf:07:ff:13:58:28:a9:36:24
(0)	9d:ec:f9:96:8a:02:31:00:f3:5e:a3:90:ad:b3:27:dc
(0)	41:41:78:75:d0:65:65:eb:d5:39:42:1c:80:27:02:82

(0)	f6:50:74:cd:db:96:98:f8:68:0f:a8:10:a5:c9:f9:d0
(0)	dd:90:b4:da:02:9b:87:bf:70
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	83:8f:6c:63:ce:b1:39:8c:62:06:62:83:15:c9:fd:de
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E5
(1)Valid From	Mar 13 00:00:00 2024 GMT
(1)Valid Till	Mar 12 23:59:59 2027 GMT
(1)Public Key Algorithm	id-ecPublicKey
(1)EC Public Key	
(1)	Public-Key: (384 bit)
(1)	pub:
(1)	04:0d:0b:3a:8a:6b:61:8e:b6:ef:dc:5f:58:e7:c6:
(1)	42:45:54:ab:63:f6:66:61:48:0a:2e:59:75:b4:81:
(1)	02:37:50:b7:3f:16:79:dc:98:ec:a1:28:97:72:20:
(1)	1c:2c:cf:d5:7c:52:20:4e:54:78:5b:84:14:6b:c0:
(1)	90:ae:85:ec:c0:51:41:3c:5a:87:7f:06:4d:d4:fe:
(1)	60:d1:fa:6c:2d:e1:7d:95:10:88:a2:08:54:0f:99:
(1)	1a:4c:e6:ea:0a:ac:de
(1)	ASN1 OID: secp384r1
(1)	NIST CURVE: P-384
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:70:8B:D2:D7:0D
(1)X509v3 Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)Signature	(512 octets)
(1)	1f:72:9d:34:45:42:41:da:a4:d0:b2:b2:b8:d2:26:4c
(1)	a7:51:25:8d:42:da:ec:36:48:96:a3:ba:1a:a4:c8:63
(1)	d8:f0:2f:b3:ce:cb:9f:67:e9:a0:9e:19:ea:d4:0d:8a
(1)	55:03:92:ca:43:84:9d:46:f1:d5:cc:ba:df:ba:c1:02
(1)	28:71:f7:ba:fe:6d:cc:1b:64:ce:ac:4c:32:1a:12:b8
(1)	91:fc:f2:e4:e8:b2:ac:f4:17:b4:ba:85:71:80:e2:83
(1)	72:91:bd:b2:f0:f7:dc:9f:86:f4:b7:1f:bf:52:bd:96
(1)	e0:e6:49:38:06:e9:73:45:20:de:6f:7c:8e:60:b3:f9
(1)	4c:3f:2a:23:10:c7:48:cc:af:5b:95:c9:76:ff:5b:ca
(1)	c4:ef:16:18:27:23:be:c4:35:9c:9f:cf:c2:df:0b:41
(1)	90:5f:38:5c:95:5c:ff:2e:6c:0a:7f:6a:ed:dd:73:81
(1)	0a:58:6f:4c:3b:9c:dc:c7:5a:93:f7:e3:57:44:67:55

(1)	5b:11:af:98:11:51:01:a8:dc:88:c7:d7:30:4d:59:b8
(1)	69:a4:df:f1:8e:92:80:0c:ed:99:23:66:69:5e:ca:89
(1)	0f:d4:b1:b3:99:f2:5c:51:df:6c:ed:e7:ae:d7:ff:7f
(1)	7a:0e:57:95:77:7f:e7:91:ad:62:30:0c:f8:2e:03:1b
(1)	98:bb:79:a3:6a:72:6d:85:fb:2c:58:20:fb:7a:71:b6
(1)	ed:61:53:49:08:67:c7:5a:a1:c4:43:81:58:4a:d5:32
(1)	16:7b:fc:b2:3c:aa:53:cc:a9:81:96:8d:27:d6:95:71
(1)	64:88:08:b3:88:13:5f:d0:bf:fe:e8:2a:c9:d9:09:62
(1)	7d:db:ac:14:e9:1a:86:d4:e6:0f:18:e8:b5:ce:e0:01
(1)	84:bc:3a:d5:cb:8f:54:34:f6:f2:74:12:fd:ee:b3:f7
(1)	97:09:5e:ad:1e:2b:50:5c:68:9e:9f:25:9b:26:6e:34
(1)	60:0f:9a:77:9a:f1:1f:e6:f7:50:33:b3:02:12:f5:34
(1)	b4:76:ec:c7:62:39:98:71:c9:a0:00:47:6f:c2:95:06
(1)	05:a9:fe:57:17:19:68:96:69:e3:b2:07:b4:4f:f8:e7
(1)	c3:b6:f8:b6:3a:c6:a9:c5:78:95:ee:f3:55:b3:b7:cc
(1)	96:b4:63:63:58:e8:29:aa:a6:9b:27:27:06:f0:2a:d7
(1)	80:04:6e:dc:8b:b1:57:ce:4b:ae:81:f1:aa:64:78:55
(1)	f6:35:8e:17:3c:46:15:e1:94:82:7b:c5:47:3e:b7:6b
(1)	11:19:36:c0:82:c6:dd:3f:c4:1a:64:88:90:26:15:50
(1)	c4:a7:8e:62:5d:55:00:fd:17:a3:5a:ff:ec:e6:5c:27


Web Server Supports HTTP Request Pipelining

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86565

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 02/23/2005

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker, it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

RESULT:

GET / HTTP/1.1
Host:54.163.109.116:443


GET /Q_Evasive/ HTTP/1.1
Host:54.163.109.116:443

Evaluation

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38718

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 06/08/2021

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

RESULT:


Source	Validated	Name	URL	ID	Time
Certificate #0		CN=app.demo.remits o.com			
Certificate	no	(unknown)	(unknown)	e092b3fc0c1dc8e768361fde61b9964d0a527 8193a72d672c4b04da56d6f5404	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	cf1456eed52e7caff3875bd9692e9be91a716 74ab017ecac01d25b77cecc3b08	Thu 01 Jan 1970 12:00:00 AM GMT

SSL Certificate will expire within next six months

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38600

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 11/14/2024

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:

Certificate #0 CN=app.demo.remitso.com The certificate will expire within six months: Jan 13 21:11:19 2025 GMT


Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38706

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 06/09/2021

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the `extended_master_secret` extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Encrypt Then MAC: indicates whether the `encrypt_then_mac` extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Heartbeat: indicates whether the `heartbeat` extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the `truncated_hmac` extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID: 38704

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 02/01/2023

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

RESULT:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLSv1.3						
TLS13-AES-128-GCM-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe8192	8192	yes	202	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe3072	3072	yes	132	low

TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-128-CCM-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-128-CCM-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-128-CCM-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-128-CCM-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-128-CCM-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-128-CCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-CCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-CCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-CCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-CCM-SHA256	ECDHE	secp384r1	384	yes	192	low


SSL Server Information Retrieval

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38116

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/24/2016

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only

through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

RESULT:


CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-ECDSA-AES128-GCM-SHA256	ECDH	ECDSA		AEAD AESGCM(128)	MEDIUM
ECDHE-ECDSA-AES256-GCM-SHA384	ECDH	ECDSA		AEAD AESGCM(256)	HIGH
ECDHE-ECDSA-CHACHA20-POLY1305	ECDH	ECDSA		AEAD CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A		AEAD AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A		AEAD AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A		AEAD CHACHA20/POLY1305(256)	HIGH
TLS13-AES-128-CCM-SHA256	N/A	N/A		AEAD AESCCM(128)	MEDIUM

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38597

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 07/12/2021

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

RESULT:


my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 42350
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/21/2016

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

RESULT:

TLS Secure Renegotiation Extension Status: supported.


SSL Session Caching Information

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38291
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/19/2020

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

RESULT:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

Evaluation


Nginx Web Server Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45433
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/15/2024

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

QID Detection Logic:(authenticated)

This QID checks for the version from the nginx binary, the path is extracted via running processes.

QID Detection Logic:(unauthenticated)

This QID checks for the nginx web server by sending a GET / request and checking the response header.

RESULT:

Nginx Web Server Detected on 443 over TCP.
Server: nginx


HTTP Response Method and Header Information Collected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48118
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/20/2020

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Server: nginx
Date: Thu, 21 Nov 2024 11:26:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: csrfToken=3b31be7424c01a0a2f53a1eb8962de203c14a41436d75370e5f5592492a6f75916375b81909c82021a40714db1461b83d9290a90ee65f3c5f1f848934366c745; path=/; secure; HttpOnly
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade

HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48002
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/12/2021

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

RESULT:

HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive

Evaluation

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86137
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/08/2015

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

RESULT:

Strict-Transport-Security: max-age=31536000; includeSubDomains

List of Web Directories

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86672
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/10/2004

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

Table with 2 columns: Directory, Source. Lists directories like /img/, /assets/, /orders/, etc. and their source as brute force.

Evaluation

/css/	web page
/vendors/	web page
/vendors/js/	web page
/assets/	web page
/assets/img/	web page
/vendors/gdpr/	web page
/assets/vendor/	web page
/assets/vendor/venobox/	web page


Cookies Collected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 02/19/2020

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 2

Device=Q2FrZQ%3D%3D.NWY4ZWYzNGU2MzFiNTIjNGUyOWRiZWQwNGE0MzBiYmQyNTA1M2UxZjhZDRiNTk0ZDI2ZTYyMjUwMDE1MWU3OaxA8afuoK8%2FELFtEa9f2f635jSEC4fEHVIHBcmhWVbqBaAHxDpbGZndq5kQD7AVPBHnUh0tBhFeluuT%2Baf%2Bm9i5jVfRiWlx5LCGNAXbbW6M; expires=Fri Nov 21 11:15:04 2025; path=/; domain=app.demo.remitso.com; max-age=31535980; secure; httponly

csrfToken=715abe758abcd8d1370428e81008603f43c593fa6df2c822a50d31414082c4de6f8e12070b5a14eb8ac66052acb208bc2cd7e9bf5aac3a29e2878b5b7efb; path=/; domain=app.demo.remitso.com; secure; httponly


Links Crawled

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2020

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 29.00
Number of links: 6
(This number excludes form requests and links re-requested during authentication.)

<https://app.demo.remitso.com/>
<https://app.demo.remitso.com/favicon.ico>
<https://app.demo.remitso.com/forgot-password.html>
<https://app.demo.remitso.com/login.html>
<https://app.demo.remitso.com/register.html>
<https://app.demo.remitso.com/send-money.html>

External Links Discovered


port 443/tcp

PCI COMPLIANCE STATUS

PASS

Evaluation

VULNERABILITY DETAILS

Severity: 1 
QID: 150010
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/19/2020

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

RESULT:

Number of links: 5
<https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css>
<https://www.google.com/recaptcha/api.js?render=6LdzjGIqAAAAAARYet0bwdeFSHr0bhyEXsJfktxj>
<https://book.cakephp.org/3.0/>
<https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap>
<https://api.cakephp.org/>


Scan Diagnostics

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <https://app.demo.remitso.com/> fetched. Status code:200, Content-Type:text/html, load time:1678 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 7 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 24 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 5) + directories:(9 x 3) + paths:(0 x 8) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 8 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 2 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (59 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 59 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Blind SQL manipulation - have 0 URI parameters,5 form fields - no tests enabled.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
WebCgiOobTests: no test enabled
Potential LDAP Login Bypass no tests enabled.
Insufficient Authentication token validation no tests enabled.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 6 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 6 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 2 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 448 requests, 254 seconds. Completed 448 requests of 448 estimated requests (100%). XSS optimization removed 58 links. All tests completed.
Batch #4 Header manipulation: estimated time < 10 minutes (47 tests, 6 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 726 requests, 738 seconds. Completed 726 requests of 780 estimated requests (93.0769%). XSS optimization removed 348 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 6 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 6 requests, 8 seconds. Completed 6 requests of 6 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
 Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
 httpoxy no tests enabled.
 Static Session ID no tests enabled.
 Login Brute Force no tests enabled.
 Login Brute Force manipulation estimated time: no tests enabled
 Insecurely Served Credential Forms no tests enabled.
 Cookies Without Consent no tests enabled.
 Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
 Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
 Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 5) + directories:(4 x 3) + paths:(11 x 8) = total (100)
 Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 8 inputs)
 Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 99 requests, 34 seconds. Completed 99 requests of 100 estimated requests (99%). All tests completed.
 Tomcat
 t Vuln manipulation no tests enabled.
 Time based path manipulation no tests enabled.
 Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(4 x 5) + directories:(94 x 3) + paths:(5 x 8) = total (342)
 Batch #5 Path manipulation: estimated time < 10 minutes (103 tests, 8 inputs)
 Batch #5 Path manipulation: 103 vulnsigs tests, completed 336 requests, 30 seconds. Completed 336 requests of 342 estimated requests (98.2456%). All tests completed.
 WebCgiHrsTests: no test enabled
 Batch #5 WebCgiGeneric: estimated time < 2 hours (824 tests, 1 inputs)
 Batch #5 WebCgiGeneric: 824 vulnsigs tests, completed 10 requests, 8 seconds. Completed 10 requests of 9640 estimated requests (0.103734%). All tests completed.
 Duration of Crawl Time: 29.00 (seconds)
 Duration of Test Phase: 1074.00 (seconds)
 Total Scan Time: 1103.00 (seconds)

Total requests made: 1743
 Average server response time: 3.73 seconds

Average browser load time: 3.93 seconds
 Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.
 HTML form authentication unavailable, no WEBAPP entry found

Links Rejected By Crawl Scope or Exclusion List port 443/tcp

PCI COMPLIANCE STATUS



Evaluation

VULNERABILITY DETAILS

Severity: 1

QID: 150020
 Category: Web Application
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 02/07/2022

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css
 https://www.google.com/recaptcha/api.js?render=6LdzjGIqAAAAAARYet0bwdeFSHr0bhyEXsJfktxj
 https://book.cakephp.org/3.0/
 https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap
 https://api.cakephp.org/

IP based excluded links:


Referrer-Policy HTTP Security Header Not Detected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 48131
 Category: Information gathering
 CVE ID: -
 Vendor Reference: [Referrer-Policy](#)
 Bugtraq ID: -
 Last Update: 01/18/2023

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

RESULT:

Referrer-Policy HTTP Header missing on 80 port.
GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive


Nginx Web Server Detected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45433
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/15/2024

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache.

QID Detection Logic:(authenticated)

This QID checks for the version from the nginx binary, the path is extracted via running processes.

QID Detection Logic:(unauthenticated)

This QID checks for the nginx web server by sending a GET request and checking the response header.

RESULT:

Nginx Web Server Detected on 80 over TCP.
Server: nginx


HTTP Response Method and Header Information Collected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48118
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/20/2020

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single

HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Thu, 21 Nov 2024 11:03:05 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://app.demo.remitso.com/


Default Web Page

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/16/2019

THREAT:

The Result section displays the default Web page for the Web server.

RESULT:

GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Thu, 21 Nov 2024 11:03:05 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://app.demo.remitso.com/

Evaluation

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center> 301 Moved Permanently </center>
<center>nginx</center>
</body>
</html>
```


Cookies Collected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150028
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/19/2020

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 2
Device=Q2FrZQ%3D%3D.Yjk2ZGQ4NmNkn2JhOTU5YzA0ODRIYTIhMGZjYmMwY2FkYjc1NTk5Y2NmMDExNTUzYzYzM2M2JiMzYzZjgwYTViMFlvXSWl%2FS0x2od%2FwISonwPxOOKqoibCypNawzYqF7M9aV7qJsD0cPEFKP9%2BvOS%2FM8akSoCWPHKYosTpDmreSvEF7rhOCzRS6i9%2F1EtYlm%2F; expires=Fri Nov 21 11:01:34 2025; path=/; domain=app.demo.remitso.com; max-age=31535984; secure; httponly
csrfToken=ad2153b55a603a2766bd6baf26f92622dd7e8bb632f52afd1a68575b98aa128b46d7d992fc143fef4e02f301f11f7ecccd1cf97333c2236a559b324d2c0775c; path=/; domain=app.demo.remitso.com; secure; httponly


Links Crawled

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -

Bugtraq ID: -
Last Update: 07/27/2020

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 28.00
Number of links: 8
(This number excludes form requests and links re-requested during authentication.)

https://app.demo.remitso.com/
https://app.demo.remitso.com/.
https://app.demo.remitso.com/favicon.ico
https://app.demo.remitso.com/forgot-password.html
https://app.demo.remitso.com/login.html
https://app.demo.remitso.com/register.html
https://app.demo.remitso.com/send-money.html
http://app.demo.remitso.com/


External Links Discovered

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150010
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/19/2020

Evaluation

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

RESULT:

Number of links: 5
https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css
https://www.google.com/recaptcha/api.js?render=6LdzjGIqAAAAAARYet0bwdeFSHr0bhyEXsJfktxj
https://book.cakephp.org/3.0/
https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap
https://api.cakephp.org/


Scan Diagnostics

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <http://app.demo.remitso.com/> fetched. Status code:301, Content-Type:text/html, load time:151 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 26 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 5) + directories:(9 x 5) + paths:(0 x 10) = total (45)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 10 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 36 requests, 2 seconds. Completed 36 requests of 45 estimated requests (80%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (59 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 59 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Blind SQL manipulation - have 0 URI parameters, 5 form fields - no tests enabled.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
WebCgiOobTests: no test enabled
Potential LDAP Login Bypass no tests enabled.
Insufficient Authentication token validation no tests enabled.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 8 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 8 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 2 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 484 requests, 258 seconds. Completed 484 requests of 484 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 10 minutes (47 tests, 8 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 1089 requests, 478 seconds. Completed 1089 requests of 1040 estimated requests (104.712%). XSS optimization removed 464 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 8 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 9 requests, 5 seconds. Completed 9 requests of 8 estimated requests (112.5%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httproxy no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.
 Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
 Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
 Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 5) + directories:(4 x 5) + paths:(11 x 10) = total (130)
 Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 10 inputs)
 Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 124 requests, 17 seconds. Completed 124 requests of 130 estimated requests (95.3846%). All tests completed.
 Tomcat Vuln manipulation no tests enabled.
 Time based path manipulation no tests enabled.
 Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(4 x 5) + directories:(94 x 5) + paths:(5 x 10) = total (540)
 Batch #5 Path manipulation: estimated time < 10 minutes (103 tests, 10 inputs)
 Batch #5 Path manipulation: 103 vulnsigs tests, completed 438 requests, 19 seconds. Completed 438 requests of 540 estimated requests (81.1111%). All tests completed.
 WebCgiHrsTests: no test enabled
 Batch #5 WebCgiGeneric: estimated time < 1 hours (824 tests, 1 inputs)
 Batch #5 WebCgiGeneric: 824 vulnsigs tests, completed 12 requests, 3 seconds. Completed 12 requests of 12050 estimated requests (0.0995851%). All tests completed.
 Duration of Crawl Time: 28.00 (seconds)
 Duration of Test Phase: 782.00 (seconds)
 Total Scan Time: 810.00 (seconds)

Total requests made: 2389
 Average server response time: 1.99 seconds

Average browser load time: 2.06 seconds
 Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.
 HTML form authentication unavailable, no WEBAPP entry found


Links Rejected By Crawl Scope or Exclusion List

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 150020
 Category: Web Application
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 02/07/2022

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
<https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css>
<https://www.google.com/recaptcha/api.js?render=6LdzjG1qAAAAAARYet0bwdefFSHr0bhyEXsJfktxj>
<https://book.cakephp.org/3.0/>
<https://fonts.googleapis.com/css2?family=Inter:wght@100;300;400;500;600;700&display=swap>
<https://api.cakephp.org/>

IP based excluded links:


SSH Banner

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38050
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/30/2020

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:

The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

SSH-2.0-OpenSSH_8.7


SSH daemon information retrieving

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38047
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Evaluation

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

Supported ciphers suites reported in this qid are in server-preferred order.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentication methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,
rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr	
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,
rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr	
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96	
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96	
Supported authentication methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

RESULT:


SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, kex-strict-s-v00@openssh.com
Supported host key algorithms for SSH2	rsa-sha2-512, rsa-sha2-256, ecdsa-sha2-nistp256, ssh-ed25519
Supported decryption ciphers for SSH2	aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes256-ctr, aes128-gcm@openssh.com, aes128-ctr
Supported encryption ciphers for SSH2	aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes256-ctr, aes128-gcm@openssh.com, aes128-ctr
Supported decryption macs for SSH2	hmac-sha2-256-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha1, umac-128@openssh.com, hmac-sha2-512
Supported encryption macs for SSH2	hmac-sha2-256-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha1, umac-128@openssh.com, hmac-sha2-512
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, gssapi-keyex, gssapi-with-mic

Open TCP Services List

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2024

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

RESULT:


Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

RESULT:


Average change between subsequent TCP initial sequence numbers is 1136344965 with a standard deviation of 630213552. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5079 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82046
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2006

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

RESULT:


IP ID changes observed (network order) for port 22: 0
Duration: 30 milli seconds

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 04/22/2019

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 111, 135, 445, 1, 7.

Listed below are the ports filtered by the firewall.


No response has been received when any of these ports are probed.
1-21,23-79,81-442,444-6128,6130-65535

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45426
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/24/2020

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

RESULT:


Protocol	Port	Time
TCP	22	0:03:05
TCP	80	2:57:39
TCP	443	6:54:49

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/15/2022

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 4320 seconds

Evaluation

Start time: Thu, Nov 21 2024, 10:57:46 GMT


End time: Thu, Nov 21 2024, 12:09:46 GMT

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:


Hops	IP	Round Trip Time	Probe	Port
1	64.39.111.4	0.18ms	ICMP	
2	*.*.*	0.00ms	Other	80
3	154.24.94.217	1.08ms	ICMP	
4	154.54.31.109	1.06ms	ICMP	
5	154.54.31.189	12.97ms	ICMP	
6	154.54.44.85	24.67ms	ICMP	
7	154.54.166.69	33.67ms	ICMP	
8	154.54.165.25	44.89ms	ICMP	
9	154.54.47.214	45.33ms	ICMP	
10	*.*.*	0.00ms	Other	80
11	*.*.*	0.00ms	Other	80
12	*.*.*	0.00ms	Other	80
13	*.*.*	0.00ms	Other	80
14	*.*.*	0.00ms	Other	80
15	54.163.109.116	76.64ms	TCP	80

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45004
Category: Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/15/2013

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

RESULT:


The network handle is: AMAZON
Network description:
Amazon Technologies Inc.

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/27/2013

Evaluation

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

RESULT:


The ISP network handle is: COGENT-154-54-16
ISP Network description:
PSINet, Inc.

SSH Algorithms ChaCha20-Poly1305 or CBC-EtM Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48259
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/03/2024

THREAT:

The ChaCha20-Poly1305 algorithm and the CBC-EtM algorithm are known to be vulnerable to the SSH Prefix Truncation Vulnerability (Terrapin).

QID Detection Logic (Unauthenticated):

This detection attempts to start the SSH key exchange process and examines whether either of the vulnerable ChaCha20-Poly1305 Algorithm or CBC-EtM Algorithm is active. Please note that this is an Information Gathering QID and does not check if a target is vulnerable, as this does not checks for Strict Key Exchange. Customers are advised to refer to QID 38913 to detect vulnerable assets.

IMPACT:

The algorithms are known to be vulnerable to the SSH Prefix Truncation Vulnerability (Terrapin). Successful exploitation of the vulnerability may allow an attacker to downgrade the security of an SSH connection when using SSH extension negotiation. The impact in practice heavily depends on the supported extensions. Most commonly, this will impact the security of client authentication when using an RSA public key.

RESULT:


SSH Algorithms ChaCha20-Poly1305 or CBC-EtM detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/27/2020

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:


Host Name	Source
app.demo.remitso.com	FQDN

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/18/2024

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

RESULT:

Operating System	Technique	ID
Linux 2.6	TCP/IP Fingerprint	U6930:22


Web Server HTTP Protocol Versions

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/02/2024

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

RESULT:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1


Web Server HTTP Protocol Versions

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/02/2024

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

RESULT:


Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 82063
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:


Based on TCP timestamps obtained via port 22, the host's uptime is 36 days, 5 hours, and 36 minutes. The TCP timestamps from the host are in units of 1 milliseconds.

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 
QID: 42017
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/20/2024

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: SSH on TCP port 22.


Content-Security-Policy HTTP Security Header Not Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 
QID: 48001
Category: Information gathering
CVE ID: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Last Update: 03/11/2019

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

RESULT:

Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: app.demo.remitso.com
Connection: Keep-Alive

Appendices

Approved False Positive Details

Following is a list of all vulnerabilities that were approved as false positives on the hosts included in this report. Any approvals for vulnerabilities not detected by the latest host scans are not included.

OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion)

QID: 42046 CVSS base: 8.1

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

OpenSSH Authentication Bypass Vulnerability

QID: 38919 CVSS base: 7

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

OpenSSH Incomplete Constrains Sensitive Information Disclosure Vulnerability

QID: 38928 CVSS base: 5.5

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

OpenSSH OS Command Injection Vulnerability

QID: 38915 CVSS base: 6.5

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent

QID: 38904 CVSS base: 9.8

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

OpenSSH Probable User Enumeration Vulnerability

QID: 38903

CVSS base: 5.3

IP Address	Protocol	Port	SSL	Approved Date
54.163.109.116			NO	11/21/2024

Hosts Scanned

54.163.109.116

Option Profile

Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.


A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
----------	-------	-------------

 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
---	---------	--

	2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels




A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description	
	1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Evaluation