ASV Scan Report Summary

tenable PCI ASV

Part 1. Scan Information - New Attestation

Scan Customer Company:	GeniusSSL	ASV Company:	Tenable Network Security
Date scan was completed:	03/18/2026	Scan expiration date:	06/16/2026

Part 2. Component Compliance Summary

Component: 172.67.193.245	payments.geniusssl.com	PASS

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, Controls
172.67.193.245:443	Missing HTTP Strict Transport Security Policy (98056)	Medium	6.5	PASS	Per Scan Customer: cdn-cgi endpoints do not have an HSTS setting because the endpoint is managed by cloudflare. https://developers.cloudflare.com/fundamentals/reference/cdn-cgi-endpoin The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP Address:

No additional corrections required for this IP address to achieve a passing scan.

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed
172.67.193.245:0	Insecure Services / industry deprecated protocols	Insecure Services Detected, SMTP Cleartext Login Permitted, Unencrypted Telnet Server, Web Server Transmits Cleartext Credentials, Web Server Uses Basic Authentication without HTTPS	
	The following cookie does not set the secure cookie flag : Name : Genius-Payments		

ASV Scan Report Summary

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed
	Path : / Value : W3 Domain : Version : Expires : Comment : Secure : false Httponly : false Port :		

Part 3c. Special Notes - Full Text

Insecure Services / industry deprecated protocols

Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Address	FQDN
172.67.193.245	payments.geniusssl.com

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

IP Address	FQDN
172.67.193.245	payments.geniusssl.com

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

IP Address	FQDN