SSL/TLS Security Scan Report

Domain: neoai.com.tr:443
Generated: 23.05.2026 11:57:40

Executive Summary

Security Grade: A+

Security Score: 95/100

Total Issues Found: 2

Critical/High Issues: 0

Security Headers Score: 20/100

Certificate Chain: 3 certificate(s)

Forward Secrecy: Enabled

Scan Duration: 0.01s

Certificate Information

Subject: neoai.com.tr
Issuer: R13
Valid: 19.05.2026 to 17.08.2026
Days Until Expiry: 86
Key Type: RSA
Key Size: 4096 bits
Signature Algorithm: Unknown
Extended Validation (EV): No
Wildcard: No
Certificate Transparency: Logged

Certificate Chain

Chain Status: Valid

1. [Server] neoai.com.tr
   Key: RSA 4096b | Issuer: R13
   Expires: 86 days
2. [Intermediate] R13
   Key: RSA 4096b | Issuer: ISRG Root X1
   Expires: 293 days
3. [Root CA] ISRG Root X1
   Key: RSA 8192b | Issuer: ISRG Root X1
   Expires: 3299 days

SecurityWall

Protocol & Cipher Support

Perfect Forward Secrecy: Enabled

Key Exchange: ECDHE, RSA, TLS 1.3 (ECDHE)

Supported Protocols:

[OK] TLSv1.2
[OK] TLSv1.3

Cipher Suite Analysis:

Total: 14 | Strong: 4 | Acceptable: 2 | Weak: 4

Cipher	KeyEx	Enc	Bits	PFS	Strength
TLS_AES_128_GCM_SHA256	TLS 1.3 (E	AES-128-GC	128	Yes	strong
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	AES-256-GC	256	Yes	strong
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	ChaCha20-P	256	Yes	acceptable
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	AES-128-GC	128	Yes	strong
ECDHE-RSA-AES128-SHA256	ECDHE	AES-128	128	Yes	acceptable
ECDHE-RSA-AES256-SHA	ECDHE	AES-256	256	Yes	weak
ECDHE-RSA-AES128-SHA	ECDHE	AES-128	128	Yes	weak
AES128-GCM-SHA256	RSA	AES-128-GC	128	No	strong
AES256-SHA	RSA	AES-256	256	No	weak
AES128-SHA	RSA	AES-128	128	No	weak

HTTP Security Headers

Score: 20/100

[OK] HSTS
[MISSING] Content-Security-Policy
[MISSING] X-Frame-Options
[MISSING] X-Content-Type-Options
[MISSING] Referrer-Policy
[MISSING] Permissions-Policy

Connection Details

Server IP: 185.199.111.153
ALPN Protocol: h2
Connection Time: 6ms
SNI Support: Yes
Session Resumption: Enabled
Session Tickets: Enabled
Secure Renegotiation: Yes

DNS CAA Records

Status: Not Found

SecurityWall

Compliance Mapping

' PCI DSS 4.0 - Score: 100%

Status: Compliant

[PASS] PCI-4.2.1: Strong cryptography protocols
[PASS] PCI-4.2.1-KEY: Minimum key size
[PASS] PCI-4.2.1-CIPHER: No weak cipher suites
[PASS] PCI-3.6.1: Valid certificate

' HIPAA - Score: 100%

Status: Compliant

[PASS] HIPAA-164.312(e)(1): Encryption in transit
[PASS] HIPAA-164.312(e)(2): Encryption mechanism
[PASS] HIPAA-164.312(d): Certificate authentication

' SOC 2 Type II - Score: 100%

Status: Compliant

[PASS] SOC2-CC6.1: Encryption of data in transit
[PASS] SOC2-CC6.7: Strong cryptographic keys
[PASS] SOC2-CC7.2: Security monitoring
[PASS] SOC2-CC8.1: Change management

' NIST CSF - Score: 67%

Status: Compliant

[PASS] NIST-PR.DS-2: Data-in-transit protection
[WARN] NIST-PR.DS-5: Protection against data leaks
[PASS] NIST-PR.IP-1: Baseline configuration

' GDPR - Score: 100%

Status: Compliant

[PASS] GDPR-32.1.a: Encryption of personal data
[PASS] GDPR-32.1.b: Confidentiality and integrity
[PASS] GDPR-32.2: Appropriate security level

Security Issues (2)

1. Missing Content-Security-Policy

Severity: LOW

Description: The server does not send a Content-Security-Policy header, which helps prevent XSS and injection attacks.
Recommendation: Implement a Content-Security-Policy header appropriate for your application.

2. Missing X-Frame-Options

Severity: LOW

Description: The server does not send X-Frame-Options header, which helps prevent clickjacking attacks.
Recommendation: Add X-Frame-Options: DENY or X-Frame-Options: SAMEORIGIN header.

SecurityWall

Security Recommendations

1. Implement Content-Security-Policy header
2. Add X-Frame-Options header (DENY or SAMEORIGIN) to prevent clickjacking attacks
3. Add DNS CAA records to control which CAs can issue certificates for your domain

SecurityWall