Informace o testu	
Zadané URL serveru:	seznam.cz
Datum a čas testování:	2021-05-20 17:31:37

Legenda			
Dobře zabezpečený	A+ (100-95)	Částečně zabezpečený	B (79-50)
Zabezpečený	A (94-80)	Zranitelný	C (49-0)

Informace o certifikátu	
Subjekt	CN = www.seznam.cz
Vydavatel	C = US
	O = Let's Encrypt
	CN = R3
Secure Renegotiation	Bezpečné znovu vyjednávání nepodporuje
Komprese	NONE (žádná)
Veřejný klíč	RSA 4096 bitů
Podpis	sha256WithRSAEncryption
Platnost od	2021-04-11 14:01:11
Platnost do	2021-07-10 14:01:11
Certifikát je platný	

IP adresy
seznam.cz (77.75.75.176)
77.75.75.172
77.75.74.176
77.75.74.172
2a02:598:4444:1::1
2a02:598:3333:1::1
2a02:598:3333:1::2
2a02:598:4444:1::2

Známka	Skóre serveru
B	77

Porty
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp filtered domain
80/tcp open http
113/tcp filtered ident
443/tcp open https
3389/tcp filtered ms-wbt-server

Podpora HSTS
Ne

Podporované protokoly
TLSv1.3
TLSv1.2

Informace o serveru
whois-ip: Record found at whois.ripe.net
inetnum: 77.75.75.0 - 77.75.75.255
netname: SEZNAM-CZ
descr: Seznam.cz
country: CZ
role: Seznam.cz IT department
email: noc@firma.seznam.cz

OpenSSL 1.1.1d 10 Sep 2019 - Cipher suits (IANA)	
TLSv1.3	TLS_AES_256_GCM_SHA384
	TLS_CHACHA20_POLY1305_SHA256
	TLS_AES_128_GCM_SHA256
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Zranitelnosti	Doporučení
HTTP	Server má povolený nezabezpečený port 80. Hrozí potenciální odposlech spojení. Jak přesměrovat na HTTPS (Apache)
Renegotiation	Server nepodporuje bezpečné opětovné vyjednávání. Informace
HSTS	Nedetekováno - potenciální útok MITM. Konfigurace HSTS
LUCKY13	Byl použit mód CBC při šifrování. CVE-2013-0169 Detail (NIST)