Přístup přes nedostatečně zabezpečený či chybně nakonfigurovaný protokol HTTPS

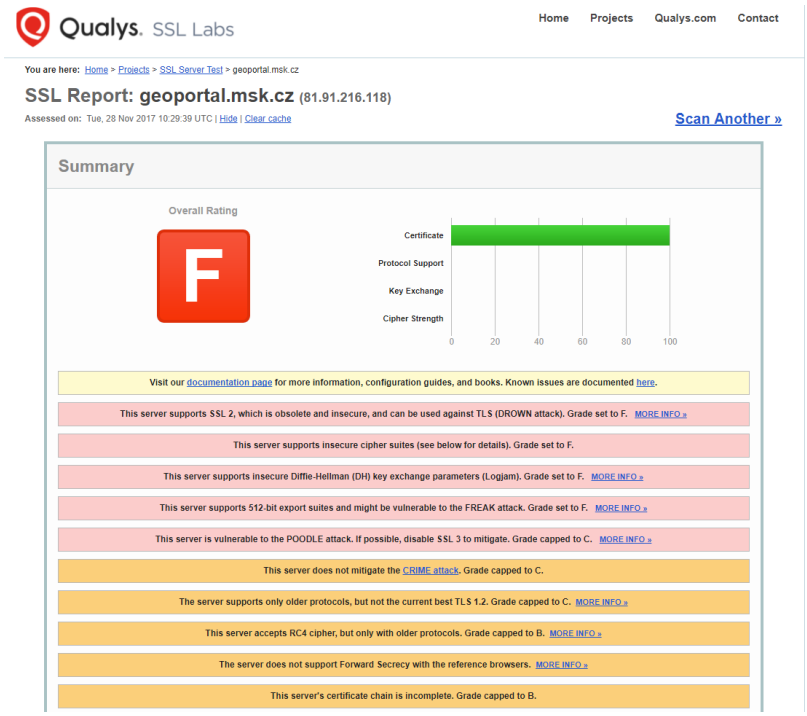
I přesto, že máte protokol HTTPS na vašem webovém serveru implementován a ve vašem oblíbeném prohlížeči při přístupu na vaše stránky či k otevřeným datům svítí v adresním řádku zelený zámeček, nemusí být vše v pořádku. Při nesprávné konfiguraci může být webový server používající protokol HTTPS náchylný k nejrůznějším zranitelnostem a nebo nemusí fungovat pro striktnější klienty. To se může projevovat například chybovými hláškami:

- unable to find valid certification path to requested target
- Invalid signature on ECDH server key exchange message
- ssl handshake failure

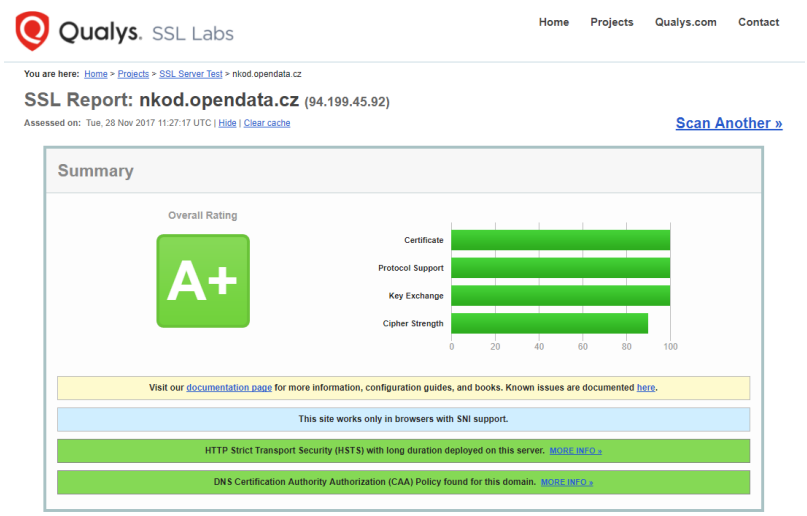
Jak zajistit správnou implementaci HTTPS

Správnou konfiguraci SSL na straně webového serveru můžete provést s pomocí nástroje Mozilla SSL Configuration Generator, který poskytuje vzorové konfigurace pro řadu webových serverů. Úroveň konfigurace volte na úrovni Modern. Pro kontrolu kvality implementace protokolu HTTPS na vašem serveru můžete použít například Qualys SSL Labs - stačí zadat vaši doménu. Snažte se dosáhnout hodnocení alespoň A, lépe však A+. Vyžadujte to případně po svých dodavatelích. Rozdíl mezi špatným a dobrým skóre je jasný:

Špatně



Dobře



Souběžná podpora HTTP a HTTPS

I při správné implementaci HTTPS je třeba rozhodnout o souběžné podpoře protokolu HTTP. Uživatel totiž typicky zadává do prohlížeče adresu bez protokolu, například `data.gov.cz`. Pak musí prohlížeč vědět, jak ke stránce přistoupit. Ve výchozím nastavení se prohlížeč pokusí nejprve připojit přes protokol HTTP (port 80). Toto lze řešit pouze dvěma způsoby Buďto protokol HTTP nebude podporován vůbec a doména bude zanesena to seznamu HSTS Preload, prohlížeč pak přímo použije HTTPS. Druhou možností je, že webserver bude nakonfigurován tak, že protokol HTTP bude sloužit pouze k přesměrování na protokol HTTPS.

Bez podpory HTTP, s registrací to seznamu HSTS

V této variantě webserver vůbec protokol HTTP na portu 80 nepodporuje. Pak je ale třeba doménu zanést do seznamu HSTS Preload, aby prohlížeč klienta při zadání adresy bez HTTPS věděl, že se má připojovat rovnou přes HTTPS, nikoliv HTTP, což by vedlo k chybě.

Přesměrování HTTP na HTTPS

V této variantě se libovolný požadavek na adresu přes protokol HTTP (port 80) pouze přesměruje na ekvivalentní HTTPS adresu (port 443) pomocí HTTP stavového kódu `301 Moved Permanently`.