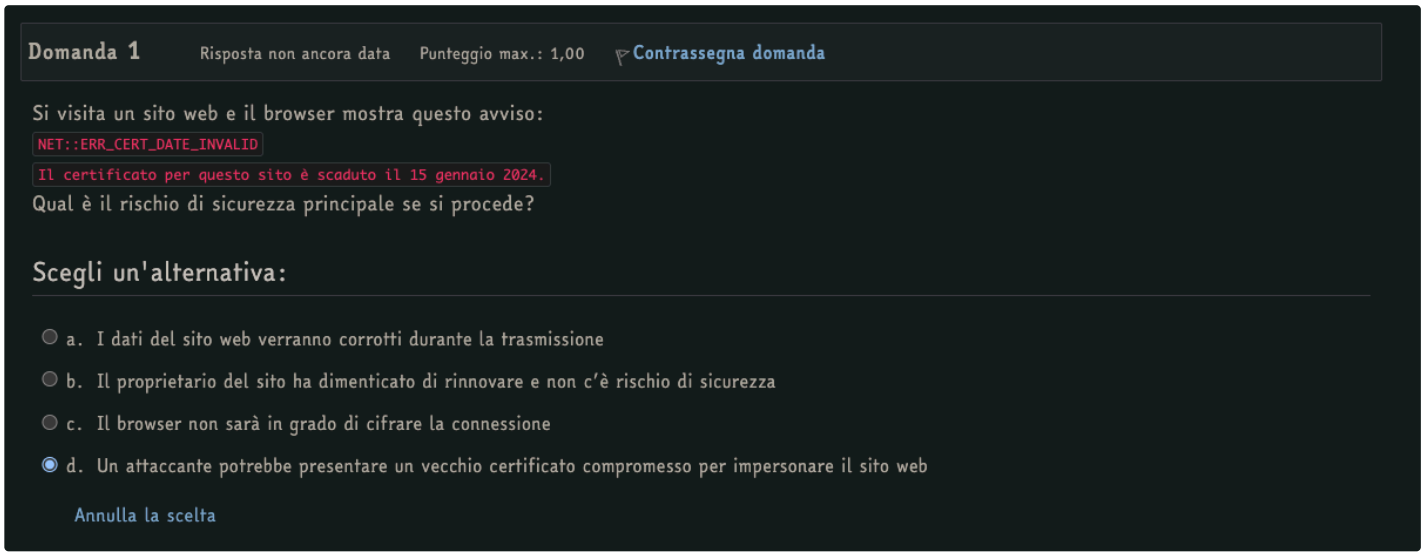
SIC - Quiz 05- PKI

Domanda 1



Domanda 1 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Si visita un sito web e il browser mostra questo avviso:

`NET::ERR_CERT_DATE_INVALID`

`Il certificato per questo sito è scaduto il 15 gennaio 2024.`

Qual è il rischio di sicurezza principale se si procede?

Scegli un'alternativa:

- a. I dati del sito web verranno corrotti durante la trasmissione
- b. Il proprietario del sito ha dimenticato di rinnovare e non c'è rischio di sicurezza
- c. Il browser non sarà in grado di cifrare la connessione
- d. Un attaccante potrebbe presentare un vecchio certificato compromesso per impersonare il sito web

Annulla la scelta

Domanda 2

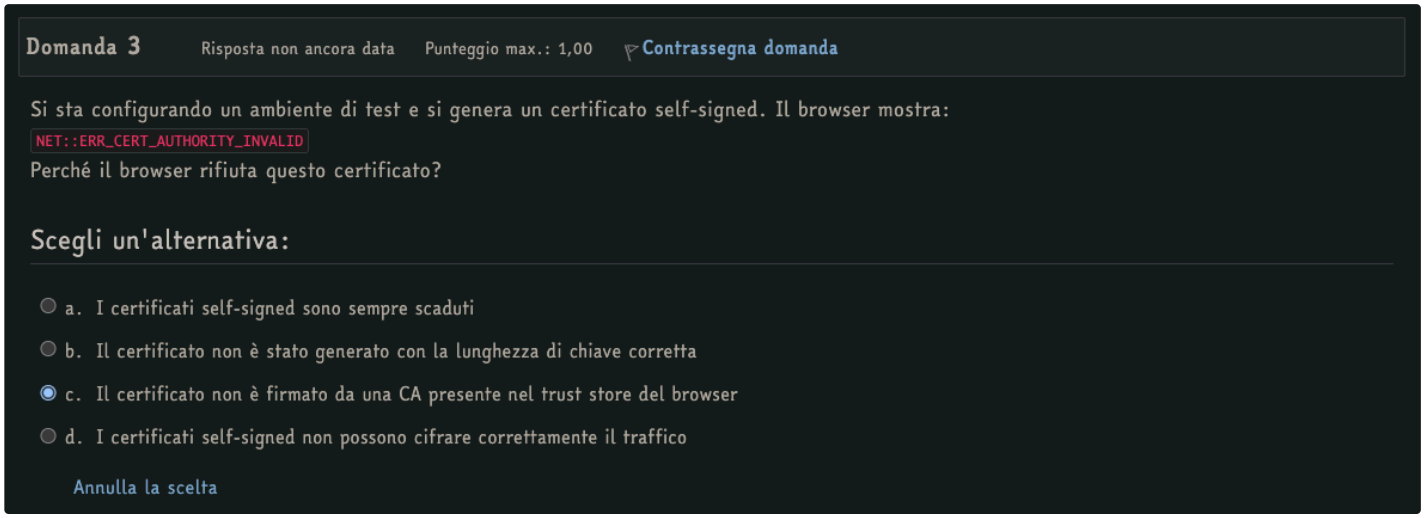
Domanda 2 Risposta salvata Punteggio max.: 1,00 Rimuovi contrassegno

Un browser moderno esegue diversi controlli quando valida un certificato HTTPS. Quale dei seguenti motivi può causare il fallimento della validazione del certificato? (Selezionare tutti quelli applicabili)

Scegli una o più alternative:

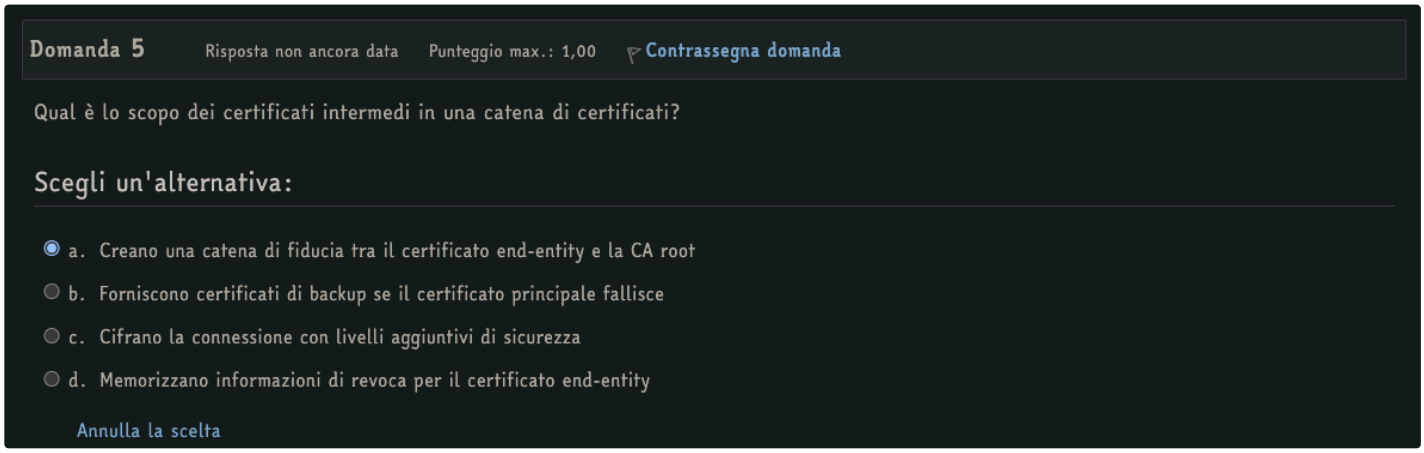
- [ ] a. La chiave pubblica del certificato è di 4096 bit invece di 2048 bit
- [x] b. La data corrente è successiva alla data "Not After" del certificato
- [x] c. La catena del certificato è incompleta (mancano certificati intermedi)
- [ ] d. Il certificato include Subject Alternative Names (SAN)
- [x] e. Il certificato è stato emesso da una Certificate Authority non presente nel trust store del browser
- [ ] f. Il certificato usa SHA-256 invece di SHA-1 per la firma
- [ ] g. Il Common Name (CN) del certificato è `example.com` (senza SAN) ma si sta visitando `www.example.com`

Domanda 3



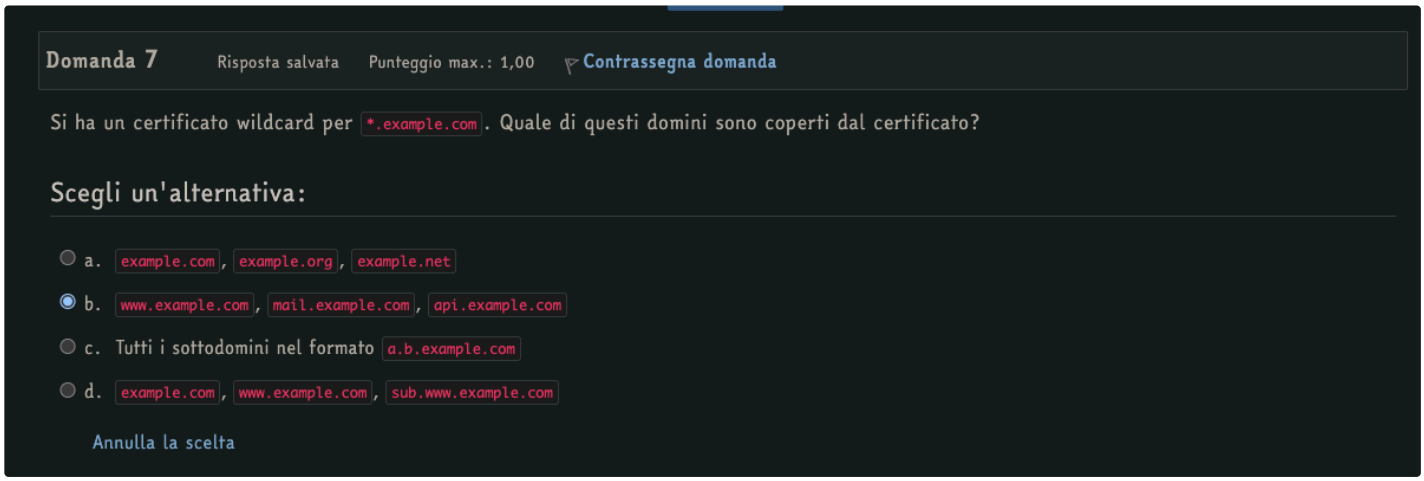
Domanda 4

Domanda 5

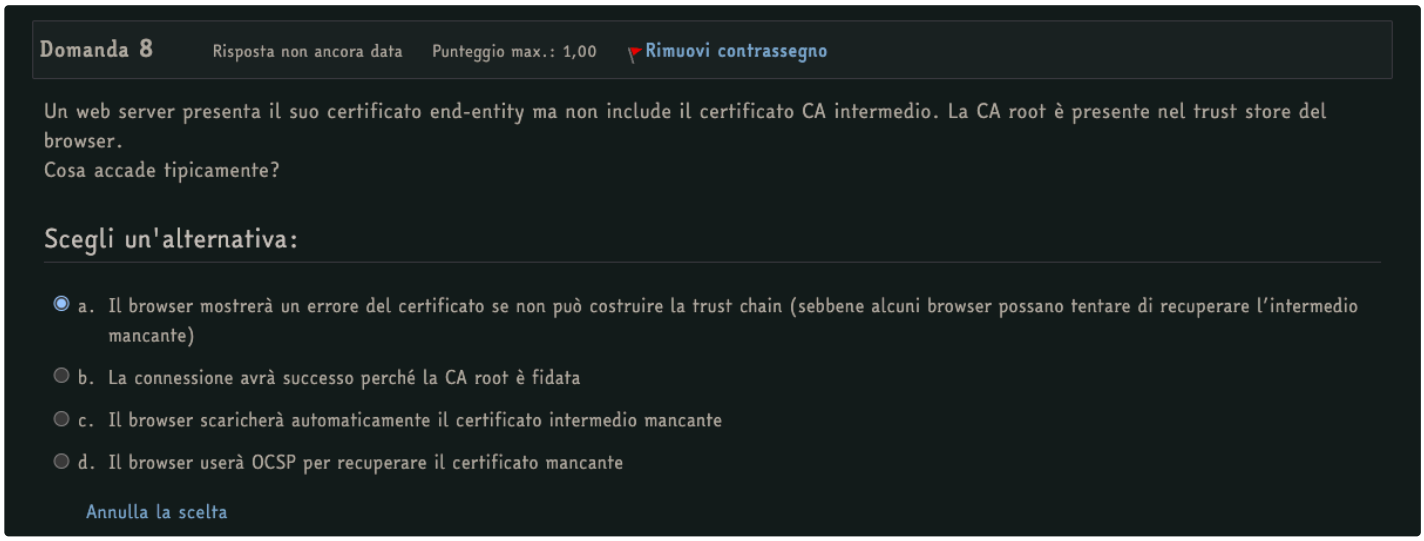


Domanda 6

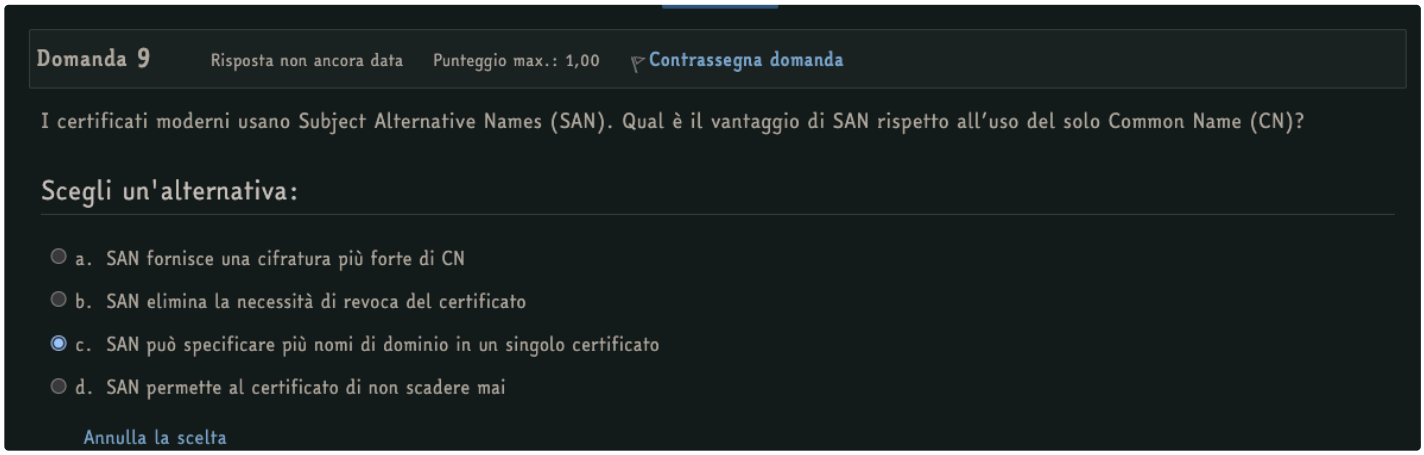
Domanda 7



Domanda 8



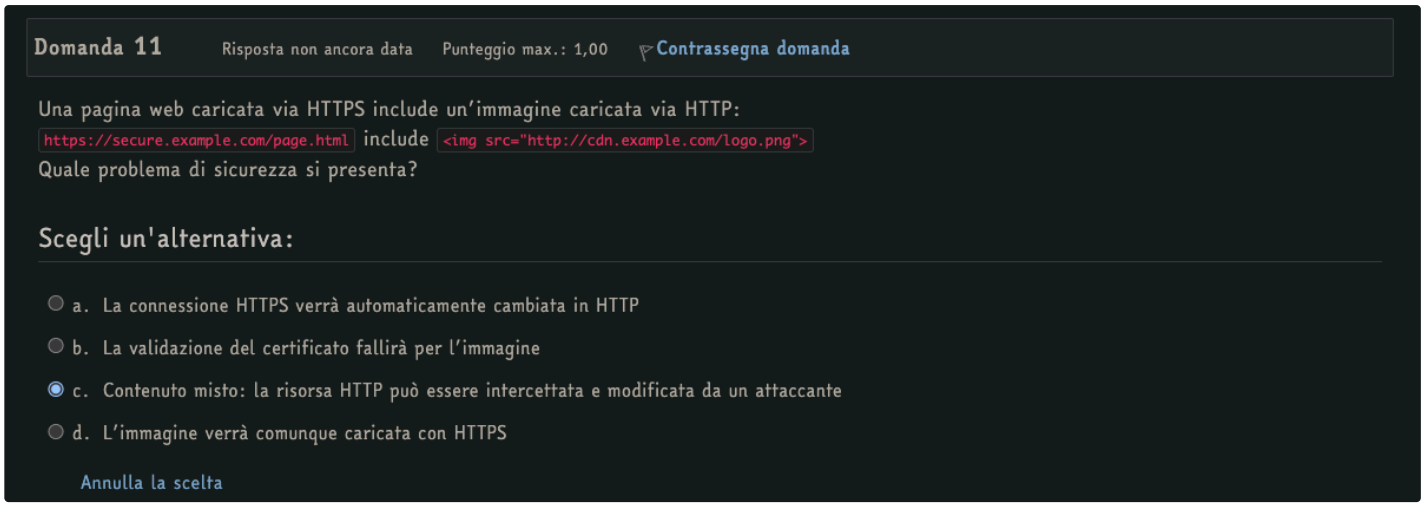
Domanda 9


Domanda 9
Risposta non ancora data
Punteggio max.: 1,00
Contrassegna domanda
I certificati moderni usano Subject Alternative Names (SAN). Qual è il vantaggio di SAN rispetto all'uso del solo Common Name (CN)?
Scegli un'alternativa:
a. SAN fornisce una cifratura più forte di CN
b. SAN elimina la necessità di revoca del certificato
c. SAN può specificare più nomi di dominio in un singolo certificato
d. SAN permette al certificato di non scadere mai
Annulla la scelta

Domanda 10


Domanda 10
Risposta non ancora data
Punteggio max.: 1,00
Contrassegna domanda
Si sta implementando HTTPS per shop.example.com. I requisiti sono:
Supportare shop.example.com e www.shop.example.com
I browser devono fidarsi del certificato per impostazione predefinita
Il certificato dovrebbe essere valido per almeno 1 anno
Deve usare algoritmi crittografici robusti
Cosa si dovrebbe fare? (Selezionare tutti quelli applicabili)
Scegli una o più alternative:
a. Ottenere un certificato da una Certificate Authority pubblicamente fidata
b. Includere sia shop.example.com che www.shop.example.com nei Subject Alternative Names
c. Usare almeno chiavi RSA 2048-bit o ECC 256-bit
d. Creare un certificato self-signed e distribuirlo a tutti gli utenti
e. Usare un certificato wildcard per *.example.com
f. Impostare il certificato per essere valido per 50 anni per semplificare il rinnovo

Domanda 11



Domanda 12

Domanda 13


Domanda 13
Risposta non ancora data
Punteggio max.: 1,00
Contrassegna domanda
Quali informazioni sono tipicamente incluse in un certificato X.509? (Selezionare tutti quelli applicabili)
Scegli una o più alternative:
a. Periodo di validità (date Not Before e Not After)
b. Cronologia del browser
c. Password degli utenti
d. Chiave pubblica e algoritmo di firma
e. Subject (a chi è rilasciato il certificato)
f. Indirizzo IP del server
g. Issuer (chi ha emesso il certificato)
h. Chiave privata