* czym jest certificate pinning? dlaczego sie go stosuje?

<http://security.stackexchange.com/questions/29988/what-is-certificate-pinning>

* czym jest Extended validation dla certyfikatów SSL?

<https://pl.wikipedia.org/wiki/EV_SSL>

* kto da sie nabrac na taki atak (kontekscie zadania 3)?
* czym sa CRL, OCSP?

<https://pl.wikipedia.org/wiki/Lista_uniewa%C5%BCnionych_certyfikat%C3%B3w> (CRL)

<https://pl.wikipedia.org/wiki/Online_Certificate_Status_Protocol>

* co sie stanie, gdy ktos pozna klucz tajny serwera www?

<http://security.stackexchange.com/questions/55525/how-can-an-attacker-use-a-leaked-private-key>

* co sie stanie, gdy ktos pozna klucz tajny CA, który podpisywał certyfikat serwera www?

<http://superuser.com/questions/140326/what-happens-if-the-private-key-of-a-certificate-authorityca-like-verisign-is>

* co sie stanie, gdy ktos pozna klucz tajny jakiegos CA?

Patrz wyżej

* co sie stanie, gdy pewne CA wydaje certyfikaty w oparciu o słabe funkcje haszujace np. MD5?

<https://www.win.tue.nl/hashclash/rogue-ca/>

* czym sa downgrade attacks na TLS?

<https://pl.wikipedia.org/wiki/Atak_downgrade>

* czym jest HTTP Strict Transport Security (HSTS)?

<https://pl.wikipedia.org/wiki/HTTP_Strict_Transport_Security>