**Oppgave 1**

1. Mitt kandidatnummer er 15850 og hash verdien jeg får er c78dc58a8699beca99f260869104e6e0030181d01018e04380892c8bb826de9a

Jeg har brukt SHA256 kalkulator fra denne nettsiden <https://xorbin.com/tools/sha256-hash-calculator>

1. Vi forventer forskjellige svar fordi alle elever har forskjellige kandidatnummer og derfor vil hash verdi være forskjellig til hver enkel student.
2. Nei det kan vi ikke, fordi en av funksjonene til hash er at det skal være enveis, det betyr at det skal være umulig å finne meldingen M selv om vi har hash verdien Hash(M).
3. Først konverterer jeg b verdi fra heksadesimalt tall til desimaltall, 9a blir 154   
   (var usikker om vi skal konvertere hele hash-verdien eller bare to siste tall men her antar jeg at det gjelder bare de to siste)

Da får jeg a = 50 b= 154 g=2 og p=1000  
først regner jeg ga mod p = 250 mod 1000 = 624

Også regner jeg gb mod p = 2154 mod 1000 = 984

Nå vil alice sende sin delnøkkel til bob og får bob sin delnøkkel

Da må alice regne ut hemmelig gab = (gb)a mod p = 98450 mod 1000 = 376

Og bob regner gab = (ga)b mod p = 624154 mod 1000 = 376

Nå har alice og bob utvekslet anonym hemmelig nøkkel 376

1. M her er mitt kandidatnummer, altså M = 15850 og C er nøkkelen 376  
   fra oppgaveteksten har vi at MAC(M,C) = HASH(append(M,C))

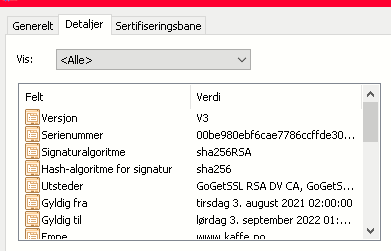
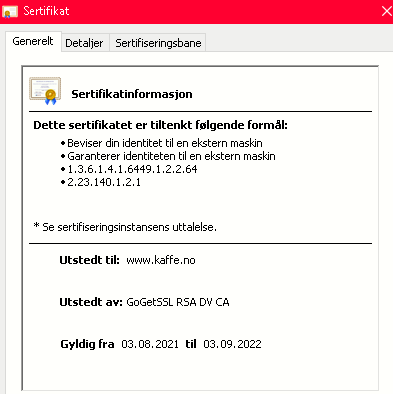
Append(M,C) gir oss 15850376

Altså MAC(15850, 376) = HASH(15850376)

Fra nettsiden jeg brukte i oppgave 1a så får jeg HASH(15850376) lik e7e047aeb54f45ba1345e313d835d441e7c4462e4e6a7e0e7b84592420d02c39

Jeg ser at hash verdien jeg fikk nå er ikke det samme som det jeg fikk i oppgave a og det gir mening siden forskjellige meldinger gir forskjellige hash verdier, selv om det første 5 tall er det samme, men hash verdien må bytte alt for mer sikkerhet.

**Oppgave 2**

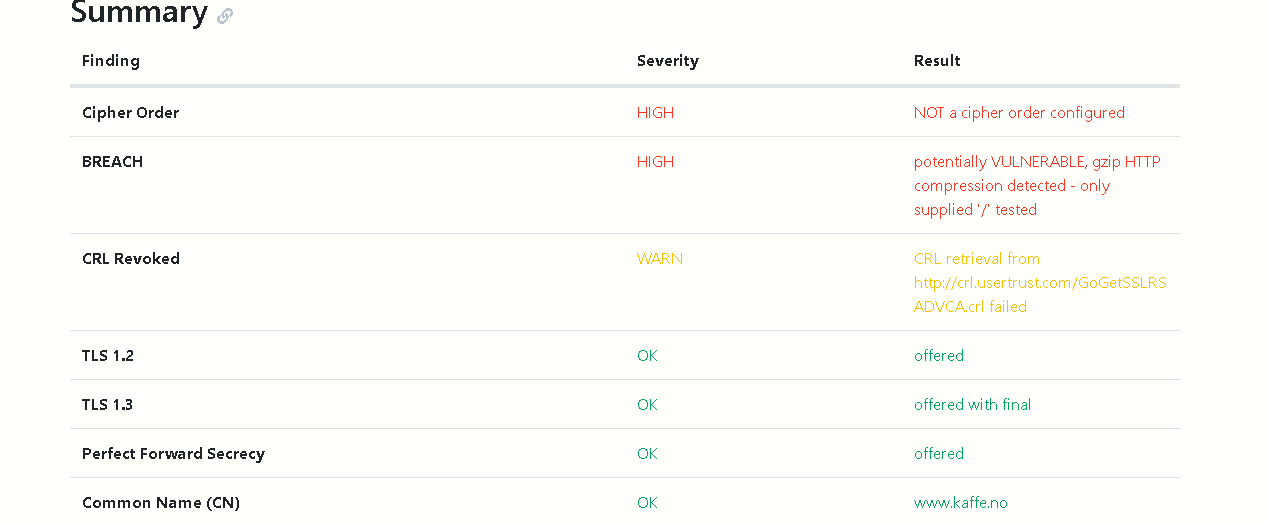
1. Jeg skal bruke domenenavnet kaffe.no, nettleseren har hengelås og det betyr at HTTPS brukes, i tillegg til kan vi sjekke URL av nettsiden, hvis det står https så betyr det at nettsiden brukes https.
2. Sertifikatet i kaffe.no er GoGetSSL RSA DV CA som utstedt det. Gyldigheten er fra 03.08.2021 til 03.09.2022. Hash algoritme som brukes er SHA256  
   
3. For å finne IP-adressen brukte jeg ping i webtjenesten <https://viewdns.info> da fikk jeg at IP-adressen til domenenavnet kaffe.no er 193.93.255.134 i Norge. For å finne når domenet ble registrert og hvem eier det brukte jeg nettsiden <https://www.norid.no> og da fikk jeg at det ble registret i 14-11-1999 og eieren er Norsk Kaffeinformasjon.

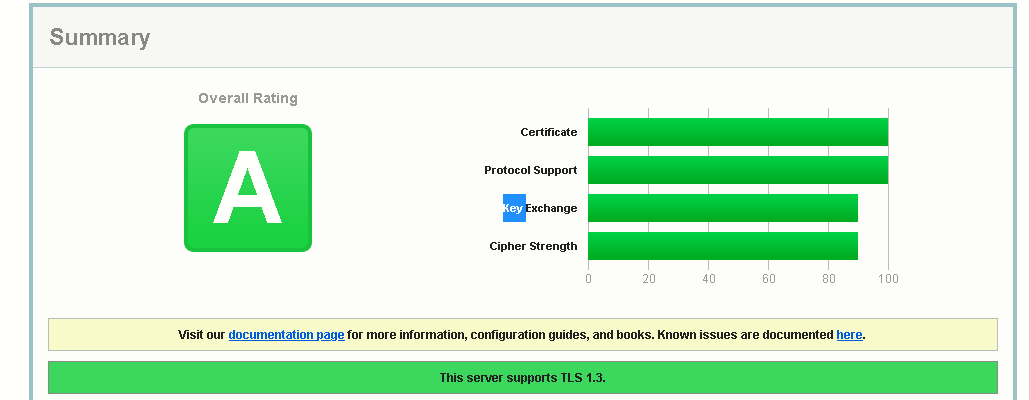
Et bilde som inneholder bord

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

1. De problemene som jeg funnet her er at cipher order er ikke konfigurert og breach er høy og det øker risikoen for angrep.   
   

Jeg har også brukt den andre nettsiden for å se om jeg finner flere problemer, her står det at serveren brukes TLS 1.3, ved TLS 1.3 vil foroversikkerhet oppnås ved bruk av Diffie-Hellman og her er key-exchange ikke høyt nok som også kan være et problem.   


1. Kommandoen for å akseptere alle IP-pakker er iptables -A FORWARD -s 193.93.255.134 -j ACCEPT der iptables er en linux pakkefilter kommando og forward tillater en admin til å kontrollere hvor pakkene skal til og accept gjør at pakkene blir akseptert.
2. alert tcp $EXTERNAL\_NET any -> 193.93.255.134 443 (msg «Uautorisert tilgang til IP- adresse 193.93.255.134»)   
   alert forteller snort til å reportere slik oppførsel som en uautorisert tilgang, tcp betyr at rollen skal skje i TCP, og external\_net har noe å gjøre med området til IP-adressen og msg er bare en melding som jeg velger selv. 443 er porten.

**Oppgave 3**

Det var ikke lurt å logge seg inn i en lenke som ble send via epost, særlig at man må være sikker at det er egentlig forelesere som har sendt denne meldingen. Studentene ved UiO må vite at alle informasjon om eksamen blir lagt i emnesiden og man vanligvis får ikke slike meldinger, derfor må man tenke før man åpner slike meldinger særlig at lenken ble utgitt som «her» og da blir det vanskelig å vite hva lenken egentlig er.

Det som er mistenkelig med meldingen er eposten som meldingen ble sendt fra, alle epostene må endes opp med uio.no mens denne e-posten ender med .ru og det er ikke sikkert å trykke på fordi det inneholder skade hvis man oppgir sensitive informasjon. I tillegg til er det uvanlig for å ende meldingen med «foreleserne», det er mer vanlig å oppgi et navn, for eksempel faglærer, men det var manglet i denne meldingen.

Denne type angrep er phishing-angrep som er en type sosial manipulering og vanligvis skjer ved å sende epost eller sms til mottagere, denne typen angrep prøver å lure personer til å besøke false nettsider for å oppgi sensitive informasjon som angriperen kan bruke i ekte nettsiden. I dette tilfelle er det spyd-phishing da målgruppen er bestemte personer, altså studentene som tar emnet IN2120.

Vi kan unngå phishing ved å øke og spre kunnskap rundt denne type angrep og ikke trykke på lenker man ikke er sikker på. Konsekvensene kan være mange, for eksempel bryting på konfidensialitet fordi angriperen vil få tilgang til informasjon selv om at angriperen er uautorisert.

**Oppgave 4**

Den første e-posten bruker jeg for lenger tid og for mange ting enn den andre.





Kilder:

* xorbin.com, (2008-2019) <https://xorbin.com/tools/sha256-hash-calculator>
* Notater fra forelesninger
* <https://viewdns.info>
* <https://www.norid.no>
* <https://testtls.com/>
* ssllabs, (2009-2021) <https://www.ssllabs.com/ssltest>
* <https://haveibeenpwned.com/>