- Hvad er kryptering? Hvordan virker det?

Man kan kryptere filer, tekster og enheder for at beskytte data. Man “oversætter”, lad os sige en tekst, til et unikt sprog, som ikke kan læses og forstås. Den eneste måde man kan læse den krypteret tekst er ved at igen “oversæt” teksten til dens originale form. Det gør man via en nøgle (Password, et sæt af ord eller en anden metode).

- Hvor kan man med fordel bruge kryptering i en virksomhed?

Jeg kan forestille mig at virksomheder kryptere data som er hemmeligt (nye ideer og etc). Online cloud filer er også man nok gerne ville kryptere, da det er nemmere for en hacker at få adgang til en cloud en det er at få adgang til local serveren.

- Hvad er et DoS angreb?

DoS står Denial of Service og er et angreb som målretter sig for at benægte service fra en IP Adresse. Angriberen sender en masse requests (request at opdatere en side eller request adgang). Modtageren kan kun håndtere en bestemt mængde requests. (Hardware eller båndbredde har en begrænsning)

- Find et eksempel på et DoS angreb.

Mafiaboy.
En af det første DoS angreb som nåde nyhederne den 7. Feb, 2000 var en dreng på 16 år som gik med navnet Mafiaboy lancerede en af de største DoS angreb i den tid. Mafiaboy benægtede adgang til store sider som CNN.com, Amazon.com, eBay og Yahoo. Angrebet foregik i en uge og det meste af tiden kunne man ikke få adgang til de sider. FBI var ind over det, og Mafiaboy blev arresteret April 2000, da han råbte højt på Online medier.

- Hvad er XSS?

XSS står for Cross Site Scripting og er en injection type angreb. Angriberen kan inject malware scripts ind i pålidelige websteder. På den måde kan angriberen manipulere hjemmesiden (kan ændre i HTML koden). Et eksempel kan være at en angriber bruger laver et thread på en forum. Han laver en clickbait title og skriver en HTML code i message boxen, som indeholder et malware script. Når andre brugere så klikker på denne post, kører de scripted og giver angriberen adgang til dine informationer.

- Hvad er SQL Injection?

SQL Injection er når man skriver SQL kode i et input felt. På den måde kan man få adgang til f.eks database som man ikke burde have adgang til. På den måde kan angriberen ændre i kontoer eller måske oprette en konto, så han kan få adgang til hjemmesiden, hvis det er det han vil.

Et eksempel kunne være et simpelt (dårlig kodet) login. Lad os sige at vi kender et username, men ikke passwordet.
Vi ved at username er “Allthings12”. Vi skriver Allthings12 ind i username inputtet og vi kan derefter inject SQL kode i password inputtet for at snyde, hvor man f.eks skriver “whatever’ OR 1 = 1”

Når det bliver læst og bliver kørt igennem SQL vil der være fejl når den læser whatever fordi det er det forkerte password, men efterfulgt læser den 1 = 1, som jo er sandt og derfor vil vi få adgang.

Det der sker er:
SELECT FROM Users WHERE
username =’Allthings12’ AND
password =’whatever’ or 1 = 1-’;