TK2100

T-05

**Nettleser- og www-sikkerhet**

Notater:

* Aldri bruke stream cipher (eksamens relatert)
* Forskjellen på Asymmetrisk og symmetrisk kryptering (eksamen)
* Hvis nettsiden er kryptert ser ikke forsvarsetteretningen dataen til brukeren på nettsiden , men kan se hvem du snakker med via ip-adressen. PST og forsvaret ser nettverkstrafikken utenom dette.

1. **Hvilke metoder finnes under HTTP/1.1**

Hvis brukeren trykker på en usikker nettside og fortsetter å bruke tjenesten , inklusivt oppgi passord , og siden webapplikasjoner kommuniserer med hverandre er det ingen bruker som kan passe på , det er årsaken til at HTTPS krever at brukeren er observant ved bruk av nettsidene.

HSTS er en metode som får klienten til å huske sertifikatet, slik at angriperen ikke har mulighet til å redigere til en annen side.

1. **Nevn noen grunner til å bruke «cookies»**

Mange nettsider benytter seg av cookies

Og den består av fire hoved-elementer:

* Cookie header linje i http-responsen
* Cookie header linje i http-forespørselen
* Cookie fil som ligger hos klienten (som kan ha ulik varighet fra sesjon til evig)
* Database over cookies hos tjeneren

Gode grunner til å benytte seg av cookies:

1. Den bevarer tilstanden til nettsiden du var på
2. Den husker autorisasjonene , login , innstillingene(settings) som eks hva du søkte på eller lo i handlekurven på en bestillingsvare

Problemet med dette er at det kan stjeles av angriperen, spoofes eller gjettes.

1. **Hva er «session hijacking» (sniffing)?**

Session hijacking eller sniffing som det også kalles er en metode som lar angriperen stjele (session) cookie fremdriftene til brukeren. Siden cookie er serverens «state» kan man kopiere cookie til en annen maskin som manipulerer serveren til å tro at det er den opprinnelige maskinen. Dette er en vanlig sårbarhet i webaplikasjoner.

1. **Hva er et serfikat?**

Sertifikater benyttes av nettsider som indentifiserer den som ekte og ikke falske. Dette skaper et trygt miljø for besøkende og forsikrer seg om at all data mellom nettleseren og webserveren er krypterte. Sertifikater forhindrer i at personlig data (cookies) og informasjon havner hos angriperen hvis nettsiden blir angrepet. Uten dette ville en ondsinnet aktør kunne ha stjålet info om brukeren på en vellykket måte. De fleste nettsider bruker SSL-sertifikater for å sikre nettsidene sine.

1. **Hva er «Cross Site Scripting» (XSS)?**

Javakoden ligger i en sandbox

Dette ligger interpretert i browseren og ligger typisk innenfor <script> … <script> dette kan man sjekke ved for eksempel inspisere en nettside. Den injiserer script på webserver i andres webaplikasjoner

Truslene som XSS utsettes for er:

Phishing, hijacking, endre brukerinnstillingene , stjele cookie , tyveri , forgiftning , og falsk reklame er eksempler på truslene XSS utsettes for.

1. **Hva er «Cross Site Request Forgery» (CSRF)**

CSRF satser på at Webserveren stoler på brukeren

Dette er et nyere type angrep og det motsatte av XSS og utnytter en site’s tillitt til en site’n

Et eksempel er :

Brukeren er pålogget i en nettbank samtidig som den besøker et slemt nettsted

1. **Hva er «SQL-injection»?**

Site’n benytter seg av en (relasjons)database

Og i et sql- injection angrep utnyttes usikker oppbygging av SQL-statements slik a

angriper har mulighet til å injecte andre sql-kommandoer. Dette finnes også i varianter som Code Injection angrep hvor angriper har utført kommandoer i shell på serveren

1. **Hva er “phishing”?**

Phishing er en metode for å manipulere brukere til å oppgi personlig informasjon og kommer i form av epost , meldinger eller falske telefonsamtaler. Det er typisk at eposten utgjør seg for å være en bank eller en nettside, som f.eks. facebook, paypal osv. Slike phishing meldinger vil innholde en url som har i hensikt å få personen til å klikke på den. Det finnes mange ulike varianter, men den vanligste er å be om brukernavn og passord. Forsvaret og ansatte i en bedrift har fått i opplæring i hvordan man skal unngå phishing, men uheldigvis så er det fremdeles mange ansatte som blir utsatt for dette f.eks klikke på en epostlink og deretter mister rettighetene til å ha en epost. Det sendes tester til alle ansatte i en bedrift f.eks som læring og hvordan man skal kontrollere disse, men ansatte gjør allikevel denne feilen.

Phishing metoder for å unngå å bli oppdaget er:

* En liten feilstaving på nettsiden
* En falsk eller fjern url felt i browseren

URL obfuskering

• I forrige slide så det ut som

paypal.com

• Det var en Kryllisk «a», som

har et annet Unicode-punkt enn

latinsk «a» (Punycode)

• http://www.xn--pypal-4ve.com

Phishing er så effektivt at ekte hackere ofte ikke bruker

andre teknikker for å komme på innsiden av et selskap

• To varianter er:

• Voice Phishing (vishing) – å ringe opp og utgi seg for å

være IT avdelingen, bank eller politi (enten for direkte

svindel, for å infisere deg med malware, eller for å få

brukernavn og passord)

• SMS Phishing (smishing) – samme som via epost, men

via sms – moderne smarttelefoner kan åpne URL linker

direkte fra tekstmeldinger (obs, avsender av sms kan

forfalskes!)