

Databasestøttet Webpublicering, forår 2002

Forelæsning 12

Cookies og Autentificering

- Cookies
- Adgangskontrol i AOLserver
- Lognimekanisme
- Gennemgang af Eksamensopgaver E2000

Cookies

En cookie er en tekst-streng som en web-server sender til en browser og som browseren returnerer uændret når browseren igen besøger det samme site.

Se evt. http://www.netscape.com/newsref/std/cookie_spec.html

Cookies er nyttige til håndtering af simpel form for tilstand — session tracking:

- Brugerpersonalisering (Customization)
- Fokusering af banner ads — hvad var en bruger interesseret i sidst?
- Adgangskontrol — login mekanisme

I Netscape på Linux kan man se hvilke cookies der er installeret i filen .netscape/cookies:

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.
linuxlab.dk FALSE / FALSE 1262307600 ad_browser_id 13
linuxlab.dk FALSE / FALSE 1262307600 last_visit 988628269
linuxlab.dk FALSE / FALSE 1262307600 second_to_last_visit 988628263
linuxlab.dk FALSE / FALSE 1262307600 ad_user_login 60,4c6f674e6432373032
```

Filformatet er som følger:

Domain	?	Path	Secure	Expires	Name	Value
linuxlab.dk	FALSE	/	FALSE	1262307600	ad_browser_id	13

Problemer med Cookies

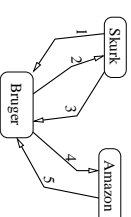
- Almindelige browsere understøtter kun omkring 20 cookies pr. site
- Almindelige browsere understøtter kun omkring 300 cookies totalt
- En cookie kan højst være 4 kilobytes stor
- Sikkerhedsproblemer med Cookies

Eksempel: Hvis et site benytter cookies til identification af en person kan personen blive udsat for et "trekants-attack".

– En skurk sætter en webside op der omdirigerer (redirects) personer til Amazon's bestillingsside for en bestemt bog (udenom alle forns)

– Herefter sender skurken en email til en "uskyldig person" som skurken ved køber ind på Amazon; skurken beder den "uskyldige person" om at "fange grisen" (trykke på et link)

– Når den uskyldige person fanger grisen bliver der bestilt en bog uden at personen kan afværge købet — Amazon får tilsendt en cookie og accepterer bestillingeni!



- 1: Email til bruger om at han skal "fange grisen"
- 2: Bruger "fanger grisen": dvs aktiverer link hos skurken
- 3: Skurken sender en redirect til Bruger om at aktivere link hos Amazon, som egentlig er at bestille en bog
- 4: Bruger bestiller bog hos Amazon
- 5: I det bruger også sender cookie til Amazon, så bestilles bogen helt uden at brugeren skal afgive flere informationer.

Løsning:

- Tilføj "Godkend-sider" til web-site

Cookies som en Trussel mod Privatlivet

Der er en grund til at nogle personer vælger at slå cookies fra i deres browser:

- Søgemaskiner viser ads for hvad man søgte efter sidste gang — problematisk hvis man bliver kigget over skulderen af arbejdsgiveren

Adgangskontrol i AOLserver

- Når et script i et underkatalog forespørges kan AOLserver sættes til at afvikle et Tcl-script (et filter) før siden returneres til brugeren.
- Tcl-scriptet kan kigge på en cookie — og dermed finde et kodeord gemt i cookien — og dermed verificere at brugeren har adgang til servicen.

- Sikkerhedsrisici — er dette en sikker strategi? Cookies sendes ukrypteret hvis ikke SSL (Secure Socket Layer) benyttes.

- Se <http://www.photo.net/wtr/thebook/>: Philip and Alex's Guide to Web Publishing, kapitel 16 (side 518-521) omkring authentication; og kapitel 15 (side 470) om hvorledes man sender en cookie til en browser:

```
# return a redirect with a cookie!
ns_write "HTTP/1.0 302 Found
Location: http://hug.it.edu:8077/Login/index.tcl
MIME-Version: 1.0
```

```
Set-Cookie: lg_user_id=expired;path=/Login; expires=Fri, 01-Jan-1990 01:00:00 GMT
Set-Cookie: lg_user_id=$user_id; path=/Login;
```

You should not be seeing this!

Loginmekanisme — Brugertabel (Login.sql)

Vi har brug for en brugertabel med login og password:

```
create table lg_user (
  user_id int primary key,
  password varchar(100) not null,
  login varchar(20) unique not null,
  name varchar(100) not null
);
```

USER_ID	PASSWORD	LOGIN	NAME
1	Niels	nh	Niels Hallemberg
2	Lise	lise	Lise Bemmedsen

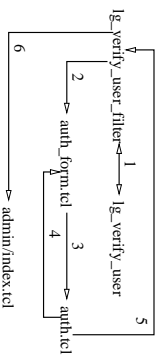
Demonstration af Systemet

- http://hug.it.edu:8077/Login/auth_form.tcl — Login-side
- <http://hug.it.edu:8077/Login/user/index.tcl> — Side der kan ses af alle
- <http://hug.it.edu:8077/Login/admin/index.tcl> — Side der kræver login

Loginmekanisme — Filerne

- `tcl/lg_verify_user.tcl` — Filter som køres når bruger besøger login-beskyttet side
- http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/lg_verify_user.tcl.txt
- `www/Login/auth_form.tcl` — Form til indlæsning af login og password
- http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/auth_form.tcl.txt
- `www/Login/auth.tcl` — Sætter cookie og sender bruger til `admin/index.tcl` med en "redirect"
- <http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/auth.tcl.txt>
- `www/Login/logout.tcl` — Fjerner cookies og sender bruger til login side
- <http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/logout.tcl.txt>
- `www/Login/admin/index.tcl` — Login-beskyttet side
- <http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/admin/index.tcl.txt>
- `www/Login/user/index.tcl` — Ikke login-beskyttet side
- <http://www.it.edu/courses/W2/F2002/S1ides/Eksempler/S112/user/index.tcl.txt>

Loginmekanisme — Overblik



- 1: cookie checkes i `lg_verify_user`
- 2: hvis login er forkert så returneres et loginbillede
- 3: indtastet login og password checkes ved at `auth.tcl` sætter en cookie med indtastet login og password, hvorefter der redirectes til `admin/index.tcl`, dvs. `lg_verify_user_filter` afvikles igen (5).
- 4: hvis login ikke findes i db, så sætter vi ikke en cookie men returnerer til loginbillede
- 6: login og password i cookie er godkendt og siden vises.

lg_verify_user.filter:

- Udføres for alle filer der hentes i `admin/`.
- Kaldet `lg_verify_user`
 - Hvis `user_id = 0`, så returneres `auth_form.tcl`.
 - Hvis `user_id ≠ 0`, så returneres fore-spurgte side.

lg_verify_user:

- Finder login og password i cookies
- Checker password og login med information i database
 - Returnerer `user_id` hvis login er ok
 - Returnerer 0 hvis login ikke er ok

Øvelse 11

Øvelse 11 er en "åben øvelse"

Hvis du har en ide til en lille web-service har du nu mulighed for at bygge den!

Du kan hente inspiration på løbesæddel 11:

- <http://www.it.edu/courses/W2/F2002/Lb/1b11.html>

Øvelseskrav

Se kursus hjemmesiden:

- <http://www.it.edu/courses/W2/F2002>

Vigtige datoer

- Eksamen: 10. juni 2002
- Spørgetime den 3. juni klokken 10 – 12. Lokale oplyses senere.