
Autentikointimenetelmät

- **Autentikoinnilla** tarkoitetaan niitä menetelmiä, joilla tiettyihin resursseihin valtuutetut (authorisoidut) käyttäjät voidaan **tunnistaa**.
- **Authorisointi** eli *valtuutuksien antaminen* on eri asia, vaikka liittyykin hyvin läheisesti autentikointiin.
- Tyypillisesti tämä tapahtuu kysymällä käyttäjiltä käyttäjätunnusta ja sitä vastaavaa salasanaa. Yksinkertaisin tapa autentikoinnin toteuttamiseen on HTTP-protokollan perusautentikointi (HTTP Basic Authentication), mutta sitä ei käsitellä tässä puutteidensa vuoksi (mm. hankala logout)
- HTTP on tilaton protokolla -> kerran hyväksytty autentikointi pitää pystyä säilyttämään voimassa ilman, että käyttäjä joutuu syöttämään tunnistetietonsa joka HTTP-pyynnölle uudelleen

Autentikointi ja sen voimassa pitäminen (istunto)

Tavallisin ratkaisu

- Käyttäjältä kysytään tunnus ja salasana web-lomakkeella
- Jos tunnistetiedot oikein, generoidaan sekä palvelimelle että evästeeksi istuntokohtainen tunniste
- Selain lähettää evästeen ja palvelinskripti tarkistaa onko ko. istunto alussa tehdyllä autentikoinnilla voimassa.

Esitetään ratkaisu, joka koostuu viidestä eri tiedostosta

- `main.php` on tavallinen web-sivu, jota voi katsella autentikoitumatta (kirjautumatta)
- `main-secure.php` on web-sivu, jonka katselu vaatii autentikoitumisen voimassa olemista
- `login.php` sisältää sekä kirjautumislomakkeen että varsinaisen autentikoinnin
- `logout.php` toteuttaa uloskirjautumisen
- `navbar.php` on upotettuna em. sivuihin navigointia varten

`main-secure.php` - autentikointi tarkistettava joka kerta

Jokaiselle autentikointia vaativalle sivulle vaaditaan määrätyn istuntomuuttujan olemassaolo ja tila

- jos vaadittu istuntomuuttuja \$_SESSION['app1_islogged'] ei ole asetettu, ohjataan autentikoitumaan (login.php)

```
1  <?php
2  // main-secure.php
3  session_start();
4
5  // Jos käyttäjä ei ole kirjautunut, ohjataan kirjautumissivulle
6  if (!isset($_SESSION['app1_islogged']) || $_SESSION['app1_islogged'] != 1) {
7      header("Location: http://" . $_SERVER['HTTP_HOST']
8              . dirname($_SERVER['PHP_SELF']) .
9              "login.php");
10
11     exit;
12 }
13
14 ?>
15 <title>Sovelluksen kirjautumista vaativa pääsivu</title>
16 <style>
17     * {background-color: #bbb;}
18 </style>
19
20 <?php include('navbar.php');?>
21
22 <p>
23 Terve <b><?php echo $_SESSION['uid'];?></b>!
24 Olet autentikoitunut tämän harmaapohjaisen sivun käyttäjäksi
25 </p>
```

login.php - varsinainen autentikointi ja istunnon asetus

- Tunnukset kysytään web-lomakkeella
- Jos tiedot oikein, asetetaan istunnon identifioiva istuntomuuttuja haluttuun tilaan
- Tässä tunnistautumistiedot kovakoodattuna (hard-coded) ohjelmakoodissa. Lisäksi salasana on selväkielisenä -> tuotantosovelluksissa ei voida toimia näin!

```
1  <?php
2  // login.php
3  session_start();
4
```

```

5  $errmsg = '';
6  if (isset($_POST['uid']) AND isset($_POST['passwd'])) {
7      // Kovakoodatut tunnus ja salasana
8      if ($_POST['uid'] === 'testi' AND $_POST['passwd'] === 's
9          // Kirjautuminen ok, merkitä sessiotauluun
10         $_SESSION['app1_islogged'] = true;
11         $_SESSION['uid'] = $_POST['uid']; // Tässä mukavuussy
12         header("Location: http://" . $_SERVER['HTTP_HOST']
13             . dirname($_SERVER['PHP_S
14             . "main-secure.php");
15         exit;
16     } else {
17         $errmsg = '<span style="background: yellow;">Tunnus/S
18     }
19 }
20 ?>
21
22 <title>Kirjautusmislomake</title>
23
24 <?php
25 if ($errmsg != '') echo $errmsg;
26 ?>
27
28 <form method="post" action="<?php echo $_SERVER['PHP_SELF'];?
29 style=color:#000;background-color:#eee>
30 Tunnus:<br><input type="text" name="uid" size="30"><br>
31 Salasana:<br><input type="text" name="passwd" size="30"><br>
32 <input type='submit' name='action' value='Kirjaudu'>
33 <br>
34 </form>

```

logout.php - istuntomuuttujan poistaminen

```

1  <?php
2  // logout.php
3  session_start();
4
5  if (isset($_SESSION['app1_islogged'])) {
6      unset($_SESSION['app1_islogged']);
7  }

```

```

8
9 header("Location: http://" . $_SERVER['HTTP_HOST']
10         . dirname($_SERVER['PHP_SELF']) .
11         . "main.php");
12 ?>

```

navbar.php - navigointivalikko

```

1 <?php
2
3 // Kirjautumattomat pääsevät kirjautumaan
4 if (!isset($_SESSION['app1_islogged']) || $_SESSION['app1_islogged'] == 0) {
5     echo "[Et ole kirjautunut] ";
6     echo "[ <a href='login.php'>Kirjaudu</a> ]";
7 } else { // ja kirjautuneet uloskirjautumaan
8     echo "[Kirjautunut: <span style='background: yellow;'>{$SESSION['app1_islogged']}</span>]";
9     echo "[<a href='logout.php'>Kirjaudu ulos</a>]";
10 }

```

main.php - pääsivu, joka ei vaadi kirjautumista

```

1 <?php
2 // main.php
3 session_start();
4
5 ?>
6 <title>Sovelluksen pääsivu</title>
7 <style>
8     * {background-color: #fff;}
9 </style>
10
11 <?php include('navbar.php');?>
12 <p>Tämä on sovelluksen pääsivu, tänne ei tarvitse kirjautua

```

Jätetty tarkoituksella tyhjäksi

