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 `$ _SESSIO['app1_islogged'` ei ole asetettu, ohjataan autentikoitumaan (login.php)

```
<?php
// main-secure.php
session_start();

// Jos käyttäjä ei ole kirjautunut, ohjataan kirjautumissisvu
if (!isset($_SESSION['app1_islogged']) || $_SESSION['app1_isl
header("Location: http://" . $_SERVER['HTTP_HOST']
                           . dirname($_SERVER['PHP_SELF']) .
                           . "login.php");

exit;
}

?>
<title>Sovelluksen kirjatumista vaativa pääsivu</title>
<style>
    * {background-color: #bbb;}
</style>

<?php include('navbar.php');?>

<p>
Terve <b><?php echo $_SESSION['uid']?></b>!
Olet autentikoitunut tämän harmaapohjaisen sivun käyttäjäksi
</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!

```
<?php
// login.php
session_start();

```

```php
$errmsg = '';
if (isset($_POST['uid']) AND isset($_POST['passwd'])) {
    // Kovakoodatut tunnus ja salasana
    if ($_POST['uid'] === 'testi' AND $_POST['passwd'] === 's
        // Kirjautuminen ok, merkintä sessiotauluun
        $_SESSION['app1_islogged'] = true;
        $_SESSION['uid'] = $_POST['uid']; // Tässä mukavuussy
         header("Location: http://" . $_SERVER['HTTP_HOST']
                                    . dirname($_SERVER['PHP_S
                                    . "main-secure.php");
        exit;
    } else {
        $errmsg = '<span style="background: yellow;">Tunnus/S
    }
}
?>

<title>Kirjautusmislomake</title>

<?php
if ($errmsg != '') echo $errmsg;
?>

<form method="post" action="<?php echo $_SERVER['PHP_SELF'];?
style=color:#000;background-color:#eee>
Tunnus:<br><input type="text" name="uid" size="30"><br>
Salasana:<br><input type="text" name="passwd" size="30"><br>
<input type='submit' name='action' value='Kirjaudu'>
<br>
</form>
```

logout.php - istuntomuuttujan poistaminen

```php
<?php
// logout.php
session_start();

if (isset($_SESSION['app1_islogged'])) {
    unset($_SESSION['app1_islogged']);
}
```

```
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']) || $_SESSION['app1_isl
5     echo "[Et ole kirjautunut] ";
6     echo "[ <a href='login.php'>Kirjaudu</a> ]";
7  } else { // ja kirjautuneet uloskirjautumaan
8     echo "[Kirjautunut: <span style='background: yellow;'>{$_S
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 sovellluksen pääsivu, tänne ei tarvitse kirjautua
```

> Jätetty tarkoituksella tyhjäksi

```
© #AriRantala
```