

Käytetyt SQL-kysely php koodina. Kyselyiden suuresta määrästä johtuen niitä ei esitetä käytettävänä SQL-kyselynä. Osa lyselyistä on SQL-injektiosuojattuja, mutta jälleen määrästä johtuen kaikkiin riskin alaisiin kyselyihin sitä ei ole tehty.

1. ruokakunta.php

```
$stmt=$db->prepare("INSERT INTO jasetet
VALUES(NULL,".$_SESSION['ruokakunta_ruokakunta_id'].",:jasetet");

$stmt->bindParam(':jasetet',$uusi_jasetet);

$stmt->execute();
```

```
$query_str = "DELETE FROM jasetet WHERE jasetet_id=".$_POST['jasetet'];

$kysely=$db->query($query_str);
```

```
$stmt=$db->prepare("INSERT INTO ruokakunnat VALUES(NULL,".$_SESSION['user_id'].":uusi_nimi");

$stmt->bindParam(':uusi_nimi',$_POST['ruokakunta']);

$stmt->execute();
```

```
$query_str = "DELETE FROM ruokakunnat WHERE ruokakunta_id=".$_POST['ruokakunnat'];

$kysely=$db->query($query_str);
```

```
$query_str_ruokakunta="SELECT ruokakunta_id,ruokakunta FROM ruokakunnat WHERE
kayttaja_id=".$_SESSION['user_id'];

$kysely=$db->query($query_str_ruokakunta);
```

2. ruokakunta_form.php

```
$query_str="SELECT jasetet_id,jasetet FROM jasetet WHERE
ruokakunta_id=".$_SESSION['ruokakunta_ruokakunta_id'];

$kysely=$db->query($query_str);
```

3. yllapito.php

```
$query_str = "UPDATE energia_sisallot SET kj_g=".$._SESSION['e_hiili']." WHERE  
kayttaja_id=".$._SESSION['user_id']." AND ravintoaine='hiilihydraatit';
```

```
$kysely=$db->query($query_str);
```

```
$query_str = "UPDATE energia_sisallot SET kj_g=".$._SESSION['e_prote']." WHERE  
kayttaja_id=".$._SESSION['user_id']." AND ravintoaine='proteiini';
```

```
$kysely=$db->query($query_str);
```

```
$query_str = "UPDATE energia_sisallot SET kj_g=".$._SESSION['e_rasva']." WHERE  
kayttaja_id=".$._SESSION['user_id']." AND ravintoaine='rasvat';
```

```
$kysely=$db->query($query_str);
```

```
-----  
$stmt=$db->prepare("INSERT INTO yksikot VALUES(NULL,:uusi, ".$._SESSION['user_id'].")");
```

```
$stmt->bindParam(':uusi',$_POST['uusi_yksikko']);
```

```
$stmt->execute();
```

```
-----  
$query_str = "DELETE FROM yksikot WHERE yksikko_id=".$_POST['yksikot'];
```

```
$kysely=$db->query($query_str);
```

```
-----  
$query_str = "SELECT * FROM yksikot WHERE kayttaja_id=".$_SESSION['user_id'];
```

```
$kysely=$db->query($query_str);
```

4. reseptit.php

```
-----  
$query_str_resepti = "SELECT * FROM reseptit WHERE  
ruokakunta_id=".$_SESSION['resepti_ruokakunta_id'];
```

```
-----  
$query_str_resepti = "SELECT * FROM reseptit WHERE resepti LIKE '%".$_POST['resepti_haku']."' AND  
ruokakunta_id=".$_SESSION['resepti_ruokakunta_id'];
```

```
-----  
$query_str_aine = "SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet WHERE ruoka_aine LIKE  
'%".$_POST['ruoka-aine_haku']."' AND kayttaja_id=".$_SESSION['user_id']."' ORDER BY ruoka_aine";
```

```
-----  
$query_str_resepti = "SELECT * FROM reseptit WHERE resepti_id=".$_valittu_resepti_id;
```

```
$query_str = "UPDATE reseptin_aineet SET kaytto_maara=".$staulun_arvo." WHERE id=".$resepti_id;
```

```
-----  
$ruoka_aine_id = $_POST['reseptin_aineet'];
```

```
$query_str = "INSERT INTO reseptin_aineet  
VALUES(NULL,".$_SESSION['resepti_id'].",".$ruoka_aine_id.",1)";
```

```
$kysely=$db->query($query_str);
```

```
-----  
$query_str = "DELETE FROM reseptin_aineet WHERE id=".$_POST['poista'];
```

```
$kysely=$db->query($query_str);
```

```
-----  
$query_str = "INSERT INTO reseptit  
VALUES(NULL,".$_SESSION['resepti_ruokakunta_id'].",".$_POST['resepti_haku'].",100)";
```

```
$kysely=$db->query($query_str);
```

```
-----  
$query_str = "DELETE FROM reseptit WHERE resepti_id=".$resepti_id;
```

```
$kysely=$db->query($query_str);
```

```
-----  
$stmt=$db->prepare("UPDATE reseptit SET annoskoko=:annos WHERE  
resepti_id=".$_SESSION['resepti_id']);
```

```
$stmt->bindParam(':annos',$_POST['annos_koko']);
```

```
$stmt->execute();
```

```
-----  
$query_str = "SELECT * FROM ruokakunnat WHERE kayttaja_id=".$_SESSION['user_id']." ORDER BY  
ruokakunta";
```

5. reseptit_aineet.php

```
-----  
$query_str = "SELECT  
ruoka_aineet.ruoka_aine_id,ruoka_aine,reseptin_aineet.kaytto_maara,yksikot.yksikko,reseptin_aineet.id  
FROM ruoka_aineet JOIN reseptin_aineet ON ruoka_aineet.ruoka_aine_id = reseptin_aineet.ruoka_aine_id  
JOIN yksikot ON ruoka_aineet.kaytto_yks_id=yksikot.yksikko_id WHERE  
reseptin_aineet.resepti_id=".$_SESSION['resepti_id']." ORDER BY ruoka_aineet.ruoka_aine";
```

```
$query_str_hinta = "SELECT  
AVG(hinta_hankinta_yks),ruoka_aineet.paino_kaytto_yks,ruoka_aineet.paino_hankinta_yks FROM  
ostokset JOIN ruoka_aineet ON ruoka_aineet.ruoka_aine_id=ostokset.ruoka_aine_id WHERE  
ostokset.ruoka_aine_id=".$row['ruoka_aine_id'];
```

```
-----  
$query_str = "SELECT  
ruoka_aineet.ruoka_aine,reseptin_aineet.kaytto_maara*ruoka_aineet.paino_kaytto_yks AS paino,  
sisalto_hiilihi,sisalto_protei,sisalto_rasva FROM ruoka_aineet JOIN reseptin_aineet ON  
reseptin_aineet.ruoka_aine_id=ruoka_aineet.ruoka_aine_id WHERE  
reseptin_aineet.resepti_id=".$_SESSION['resepti_id'];
```

```
-----  
$query_str = "SELECT annoskoko FROM reseptit WHERE resepti_id=".$_SESSION['resepti_id'];
```

6. ostoslista.php

```
-----  
$query_str = "SELECT * FROM ruokakunnat WHERE kayttaja_id=".$_SESSION['user_id']." ORDER BY  
ruokakunta";
```

```
-----  
$query_str = "SELECT count(id) FROM ruokakalenteri WHERE ruokailu='".$ruokailut[$q]."' AND  
pvm>='".$query_start."' AND pvm <='".$query_end."'";
```

```
-----  
$query_str = "SELECT ruokakalenteri.ruokailu,reseptit.resepti,COUNT(ruokakalenteri.resepti_id) AS lkm  
FROM ruokakalenteri JOIN reseptit ON reseptit.resepti_id=ruokakalenteri.resepti_id WHERE  
ruokakalenteri.ruokakunta_id=".$_SESSION['ostoslista_ruokakunta_id']."' AND  
ruokakalenteri.pvm>='".$query_start."' AND ruokakalenteri.pvm<='".$query_end."' AND  
ruokakalenteri.ruokailu='".$ruokailut[$x]."' GROUP BY ruokakalenteri.resepti_id";
```

```
-----  
$query_str = "select  
ruoka_aineet.ruoka_aine,reseptin_aineet.kaytto_maara*count(ruokakalenteri.resepti_id) AS  
lkm,AVG(ostokset.hinta_hankinta_yks) AS  
hinta,ruoka_aineet.paino_kaytto_yks,ruoka_aineet.paino_hankinta_yks,yksikot.yksikko FROM  
ruoka_aineet JOIN reseptin_aineet ON reseptin_aineet.ruoka_aine_id=ruoka_aineet.ruoka_aine_id JOIN  
reseptit ON reseptit.resepti_id=reseptin_aineet.resepti_id JOIN ruokakalenteri ON  
ruokakalenteri.resepti_id=reseptit.resepti_id JOIN ostokset ON  
ostokset.ruoka_aine_id=ruoka_aineet.ruoka_aine_id JOIN yksikot ON  
yksikot.yksikko_id=ruoka_aineet.hankinta_yks_id WHERE  
ruokakalenteri.ruokakunta_id=".$_SESSION['ostoslista_ruokakunta_id']."' AND  
ruokakalenteri.pvm>='".$query_start."' AND ruokakalenteri.pvm<='".$query_end."' GROUP BY  
ruoka_aineet.ruoka_aine_id";
```

7. login.php

```
$query_str = "SELECT * FROM energia_sisallot WHERE kayttaja_id='".$$_SESSION['user_id']."' ORDER BY
ravintoaine LIMIT 3";
```

```
$stmt=$db->prepare("SELECT COUNT(kayttaja_id) FROM kayttajat WHERE kayttaja=:username");
$stmt->bindParam(':username',$kayttaja);
$stmt->execute();
$skysely = $stmt->fetch(PDO::FETCH_COLUMN);
```

```
$koodattu_salasana = password_hash($_POST['salasana'],PASSWORD_DEFAULT);
$stmt=$db->prepare("INSERT INTO kayttajat VALUES(NULL,:username,:password)");
$stmt->bindParam(':username',$kayttaja);
$stmt->bindParam(':password',$koodattu_salasana);
$stmt->execute();
```

```
$stmt=$db->prepare("SELECT kayttaja_id FROM kayttajat WHERE kayttaja=:username");
$stmt->bindParam(':username',$kayttaja);
$stmt->execute();
$skysely = $stmt->fetchAll(PDO::FETCH_ASSOC);
```

```
$query_str = "INSERT INTO energia_sisallot VALUES(NULL,'hiilihydraatit',17,".$_SESSION['user_id'].")";
$skysely=$db->query($query_str);
$query_str = "INSERT INTO energia_sisallot VALUES(NULL,'proteiinit',17,".$_SESSION['user_id'].")";
$skysely=$db->query($query_str);
$query_str = "INSERT INTO energia_sisallot VALUES(NULL,'rasvat',38,".$_SESSION['user_id'].")";
$skysely=$db->query($query_str);
```

8. ruoka-aineet.php

```
$query_str = 'SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet WHERE
kayttaja_id="'.$_SESSION['user_id'].'';
```

```
-----  
$query_str = "SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet WHERE ruoka_aine LIKE  
'%".$_POST['ruoka_aine']."%'";
```

```
-----  
$query_str = "SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet WHERE  
ruoka_aine_id=".$_POST['ruoka-aineet'];
```

```
-----  
$query_str = "CALL lisaa_ruoka_aine('".$_SESSION['user_id']."','".$_POST['ruoka_aine']."'");
```

```
    $kysely=$db->query($query_str);
```

```
    $query_str = 'SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet';
```

```
-----  
$query_str = "DELETE FROM ruoka_aineet WHERE ruoka_aine_id=".$_POST['ruoka_aine_id'];
```

```
    $kysely=$db->query($query_str);
```

```
    $query_str = 'SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet';
```

```
-----  
$query_str = "UPDATE ruoka_aineet SET ruoka_aine='".$_ruoka_aine_nimi."',  
kaytto_yks_id=".$_kaytto_yks_id.", paino_kaytto_yks=".$_kaytto_paino.",  
hankinta_yks_id=".$_hankinta_yks_id.", paino_hankinta_yks=".$_hankinta_paino.", sisalto_hiilih=".$_shiilih.",  
sisalto_protei=".$_proteiinit.", sisalto_rasva=".$_rasvat." WHERE ruoka_aine_id=".$_ruoka_aine_id;
```

```
-----  
$query_str = "SELECT hankinta_yks_id FROM ruoka_aineet where ruoka_aine_id=".$_SESSION['ruoka-  
aine_id'];
```

```
-----  
$query_str = "SELECT yksikko_id,yksikko FROM yksikot WHERE kayttaja_id=".$_SESSION['user_id'];
```

```
-----  
$query_str = "SELECT kaytto_yks_id FROM ruoka_aineet where ruoka_aine_id=".$_SESSION['ruoka-  
aine_id'];
```

```
-----  
$query_str = "SELECT paino_hankinta_yks FROM ruoka_aineet WHERE ruoka_aine_id=".$_SESSION['ruoka-  
aine_id'];
```

```
-----  
$query_str = "SELECT yksikko_id,yksikko FROM yksikot WHERE kayttaja_id=".$_SESSION['user_id'];
```

```
-----
```

```
$query_str = "SELECT paino_kaytto_yks FROM ruoka_aineet WHERE ruoka_aine_id=" . $_SESSION['ruoka-aine_id'];
```

```
$query_str = "SELECT sisalto_hiilih,sisalto_protei,sisalto_rasva FROM ruoka_aineet WHERE ruoka_aine_id=" . $_SESSION['ruoka-aine_id'];
```

9. ruokakalenteri.php

```
$query_str_resepti = "SELECT * FROM reseptit WHERE ruokakunta_id=" . $_SESSION['kalenteri_ruokakunta'];
```

```
$query_str_resepti = "SELECT * FROM reseptit WHERE resepti LIKE '%" . $raja . "%' AND ruokakunta_id=" . $_SESSION['kalenteri_ruokakunta'];
```

```
$query_str = "INSERT INTO ruokakalenteri VALUES(NULL,'" . $lisaa_pvm . "','" . $lisaa_ruokailu . "','" . $lisaa_ruokakunta . "','" . $lisaa_resepti_id . "')";
```

```
$query_str = "DELETE FROM ruokakalenteri WHERE id=" . $_POST['poista_kalenteri'];
```

```
$query_str = "SELECT * FROM ruokakunnat WHERE kayttaja_id=" . $_SESSION['user_id'] . " ORDER BY ruokakunta";
```

10. ruokakalenteri_kalenteri.php

```
$query_str = "SELECT ruokakalenteri.id, ruokakalenteri.resepti_id, reseptit.resepti FROM ruokakalenteri JOIN reseptit ON reseptit.resepti_id=ruokakalenteri.resepti_id WHERE ruokakalenteri.ruokakunta_id=1 AND ruokakalenteri.pvm='" . $query_date . "' AND ruokakalenteri.ruokailu='" . $ruokailu[$x] . "'";
```

11. ostokset.php

```
$query_str = 'SELECT ruoka_aine_id, ruoka_aine FROM ruoka_aineet';
```

```
$query_str = "SELECT ruoka_aine_id, ruoka_aine FROM ruoka_aineet WHERE ruoka_aine LIKE '%" . $_POST['ruoka_aine'] . "%'";
```

\$query_str = "SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet WHERE
ruoka_aine_id=".\$\$_POST['ruoka-aine'];

\$query_str = "INSERT INTO ostokset
VALUES(NULL,".\$ruokakunta_id.",",".\$pvm.",",".\$ruoka_aine_id.",",".\$hinta.",",".\$maara.")";

query_str = 'SELECT ruoka_aine_id,ruoka_aine FROM ruoka_aineet';

\$query_str2 = "SELECT * FROM ruokakunnat WHERE kayttaja_id=".\$\$_SESSION['user_id']." ORDER BY
ruokakunta";

\$query_str = "SELECT yksikko FROM yksikot JOIN ruoka_aineet ON
ruoka_aineet.hankinta_yks_id=yksikot.yksikko_id WHERE
ruoka_aineet.ruoka_aine_id=".\$\$_SESSION['ostos_id'];
