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 jasenet VALUES(NULL,".$\_SESSION['ruokakunta\_ruokakunta\_id'].",:jasen)");

$stmt->bindParam(':jasen',$uusi\_jasen);

$stmt->execute();

------------------------------------------------------------------------------

$query\_str = "DELETE FROM jasenet WHERE jasen\_id=".$\_POST['jasenet'];

$kysely=$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);

------------------------------------------------------------------------------

1. **ruokakunta\_form.php**

------------------------------------------------------------------------------

$query\_str="SELECT jasen\_id,jasen FROM jasenet WHERE ruokakunta\_id=".$\_SESSION['ruokakunta\_ruokakunta\_id'];

$kysely=$db->query($query\_str);

------------------------------------------------------------------------------

1. **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='proteiinit'";

$kysely=$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);

------------------------------------------------------------------------------

1. **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;

------------------------------------------------------------------------------

$query\_str = "UPDATE reseptin\_aineet SET kaytto\_maara=".$taulun\_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";

------------------------------------------------------------------------------

1. **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'];

------------------------------------------------------------------------------

$query\_str = "SELECT ruoka\_aineet.ruoka\_aine,reseptin\_aineet.kaytto\_maara\*ruoka\_aineet.paino\_kaytto\_yks AS paino, sisalto\_hiilih,sisalto\_protei,sisalto\_rasva FROM ruoka\_aineet JOIN reseptin\_aineet ON reseptin\_aineet.ruoka\_aine\_id=ruoka\_aineet.ruoka\_aine\_id WHERE reseptin\_aineet.resepti\_id=".$\_SESSION['resepti\_id'];

------------------------------------------------------------------------------

$query\_str = "SELECT annoskoko FROM reseptit WHERE resepti\_id=".$\_SESSION['resepti\_id'];

------------------------------------------------------------------------------

1. **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";

------------------------------------------------------------------------------

1. **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();

$kysely = $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();

$kysely = $stmt->fetchAll(PDO::FETCH\_ASSOC);

------------------------------------------------------------------------------

$query\_str = "INSERT INTO energia\_sisallot VALUES(NULL,'hiilihydraatit',17,".$\_SESSION['user\_id'].")";

$kysely=$db->query($query\_str);

$query\_str = "INSERT INTO energia\_sisallot VALUES(NULL,'proteiinit',17,".$\_SESSION['user\_id'].")";

$kysely=$db->query($query\_str);

$query\_str = "INSERT INTO energia\_sisallot VALUES(NULL,'rasvat',38,".$\_SESSION['user\_id'].")";

$kysely=$db->query($query\_str);

------------------------------------------------------------------------------

1. **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=".$hiilih.", sisalto\_protei=".$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'];

------------------------------------------------------------------------------

1. **ruokakalenteri.php**

------------------------------------------------------------------------------

$query\_str\_resepti = "SELECT \* FROM reseptit WHERE ruokakunta\_id=".$\_SESSION['kalenteri\_ruokakunta'];

------------------------------------------------------------------------------

$query\_str\_resepti = "SELECT \* FROM reseptit WHERE resepti LIKE '%".$rajaa."%' 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";

------------------------------------------------------------------------------

1. **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]."'";

------------------------------------------------------------------------------

1. **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'];

------------------------------------------------------------------------------