

Forum:[Hack Forums](#)

Thread: [PHP Warning: mysqli::query\(\): Empty query in](#)

Villezzai - June 14, 2017, 1:15 pm

Need a little help with my website.

Error:

Code PHP Warning: mysqli::query(): Empty query in /home/psctrade/public_html/test/process.php on line 24:

Code:

Code <?php

```
$koodi = $_POST['koodi'];
```

```
$arvo = $_POST['arvo'];
```

```
$currency = $_POST['currency'];
```

```
$purse_type = $_POST['purse_type'];
```

```
$purse_currency = $_POST['purse_currency'];
```

```
$osoite = $_POST['osoite'];
```

```
$sahkoposti = $_POST['sahkoposti'];
```

```
$servername = "localhost";
```

```
$username = "censored";
```

```
$password = "censored";
```

```
$dbname = "censored";
```

```
$conn = new mysqli($servername, $username, $password, $dbname);
```

```
if ($conn->connect_error) {
```

```
    die("Connection failed: " . $conn->connect_error);
```

```
}
```

```
if ($action === "record"){
```

```
$sql = "INSERT INTO `psctrade_homo`.`koodit` (`ID`, `koodi`, `arvo`, `currency`, `purse_type`, `purse_currency`, `osoite`, `sahkoposti`);
```

```
VALUES
```

```
(NULL, $koodi, $arvo, $currency, $purse_type, $purse_currency, $osoite, $sahkoposti);";
```

```
}
```

```
if ($conn->query($sql) === TRUE) {
```

```
    echo "New record created successfully";
```

```
} else {
```

```
    echo "Error: " . $sql . "<br>" . $conn->error;
```

```
}
```

```
$conn->close();
```

```
?>
```

Line 24:

```
Code if ($conn->query($sql) === TRUE) {
```

Water Aura - June 14, 2017, 1:20 pm

well what happens if action isn't "record"...the variable sql is empty

```
Code <?php
$koodi = $_POST['koodi'];
$arvo = $_POST['arvo'];
$currency = $_POST['currency'];
$purse_type = $_POST['purse_type'];
$purse_currency = $_POST['purse_currency'];
$osoite = $_POST['osoite'];
$sahkoposti = $_POST['sahkoposti'];

$servername = "localhost";
$username = "censored";
$password = "censored";
$dbname = "censored";

$conn = new mysqli($servername, $username, $password, $dbname);
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
if ($action === "record"){
    $sql = "INSERT INTO `psctrade_homo`.`koodit` (`ID`, `koodi`, `arvo`, `currency`, `purse_type`,
`purse_currency`, `osoite`, `sahkoposti`);
VALUES
(NULL, $koodi, $arvo, $currency, $purse_type, $purse_currency, $osoite, $sahkoposti)";
    if ($conn->query($sql) === TRUE) {
        echo "New record created successfully";
    } else {
        echo "Error: " . $sql . "<br>" . $conn->error;
    }
}

$conn->close();

?>
```

Another solution as I guess you're adding more "actions" is to check if the variable "sql" is empty before executing the query.

Also seems like the variable "action" isn't even defined.

Villezzai - June 14, 2017, 1:26 pm

(Jun 14, 2017 01:20 PM)Water Aura Wrote: [CITE](#) well what happens if action isn't "record"...the variable sql is empty

```
Code <?php
$koodi = $_POST['koodi'];
$arvo = $_POST['arvo'];
$currency = $_POST['currency'];
```

```

$purse_type = $_POST['purse_type'];
$purse_currency = $_POST['purse_currency'];
$osoite = $_POST['osoite'];
$sahkoposti = $_POST['sahkoposti'];

$servername = "localhost";
$username = "censored";
$password = "censored";
$dbname = "censored";

$conn = new mysqli($servername, $username, $password, $dbname);
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
if ($action === "record"){
    $sql = "INSERT INTO `psctrade_homo`.`koodit` (`ID`, `koodi`, `arvo`, `currency`, `purse_type`,
`purse_currency`, `osoite`, `sahkoposti`);
    VALUES
    (NULL, $koodi, $arvo, $currency, $purse_type, $purse_currency, $osoite, $sahkoposti)";
    if ($conn->query($sql) === TRUE) {
        echo "New record created successfully";
    } else {
        echo "Error: " . $sql . "<br>" . $conn->error;
    }
}

$conn->close();

?>

```

Another solution as I guess you're adding more "actions" is to check if the variable "sql" is empty before executing the query.

Thanks for the help, no more errors but nothing shows up on the database when I send the form data to database, ffs

Water Aura - June 14, 2017, 1:28 pm

(Jun 14, 2017 01:26 PM)Villezzai Wrote: [CITE](#) Thanks for the help, no more errors but nothing shows up on the database when I send the form data to database, ffs

Well as I stated in my edit the variable "action" isn't even defined.

Omniscient - June 15, 2017, 6:47 pm

Code if (\$action === "record"){

You're missing this at your script start.

```
$action = $_POST['action'];
```

And this...

```
Code if ($conn->query($sql) === TRUE) {
```

You need to handle the error better than that imho.

And also, your script is crazy vuln to sql injection.

