cve-vul Update back_password_reset.md History

1 contributor

18 lines (14 sloc) | 865 Bytes

Background administrator password reset vulnerability

vuln in /include/web_check.php

```
}elseif ($Type=="findok"){ //  密码找回

    $umail=test_input(verify_str($_POST['Email']));
    $umm=test_input(verify_str($_POST['umima']));
    $urzm=test_input(verify_str($_POST['uyzm']));
    $fhurl=str_replace("SEMCMS_Remail.php","",$_POST['furl']);

    if(empty($umail) || empty($umm) || empty($urzm)){

        echo'<script language="javascript">alert("请输入密码与认证码！");history.go(-1);</script>';

    }else{                                                    只对邮箱和验证码做了判断

        $query=$db_conn->query("select * from sc_user where user_email='".$umail."' and user_rzm='".$urzm."'");

        if (mysqli_num_rows($query)>0){

        $db_conn->query("UPDATE  sc_user SET user_ps=md5($umm)  WHERE user_email='".$umail."' and user_rzm='$urzm'");

        echo'<script language="javascript">alert("操作成功返回登陆！");location.href="'.$fhurl.'";</script>';

        }else{

         echo'<script language="javascript">alert("邮箱或者验证码错误");location.href="'.$fhurl.'";</script>';
        )

    }
```

In line 54 of the file, three variables are Judge whether it is empty; test_input and verify_str are keywords to detect whether the string has SQL and XSS. Let's ignore it here.

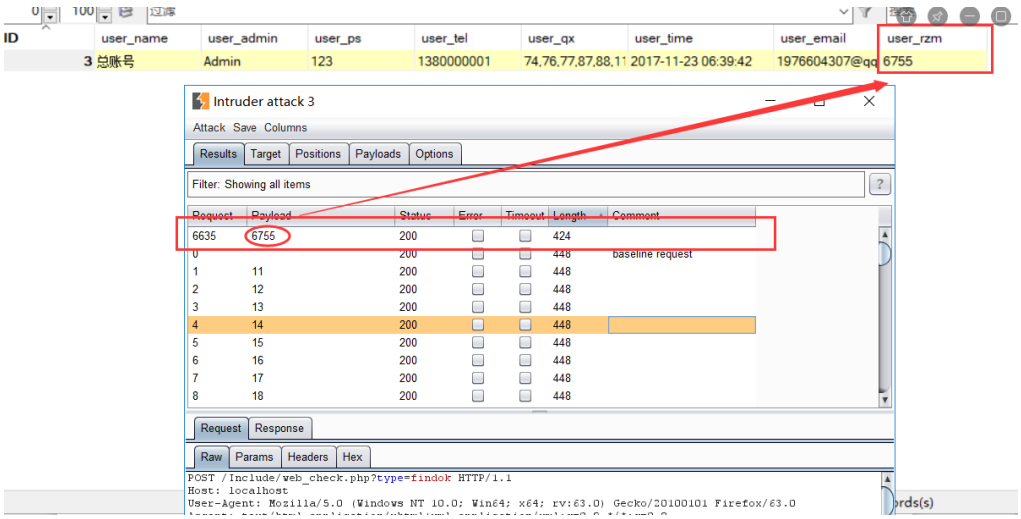
In line 60 of the file

```
$query=$db_conn->query("select * from sc_user where user_email='".$umail."' and user_rzm='".$urzm."'");
```

The validity of $umail and $urzm is verified by database queries.Moreover, $urzm is generated by the random number Rand (10,10000).

```
13    if ($postEmail!=""){ // 判断是否输入邮箱
14
15      $result=$db_conn->query("select * from sc_user where user_email='".$postEmail."'");
16      $row = mysqli_fetch_array($result,MYSQL_ASSOC);
17
18      if (mysqli_num_rows($result)>0){
19
20        $fsjs=rand(10,10000);  //邮件认证码
21        $fhurl=str_replace("SEMCMS_Remail.php","",$_POST['furl']);
22        $smtpusermail=$smtpemailto;
23        $smtptoemail=$postEmail;
24        $mailtitle="来自".$_SERVER['SERVER_NAME']."密码找回邮件！";
25        $mailcontent="网站管理员你好：<br>你的邮箱是：".$postEmail."<br> 点击<a href='".$fhurl."?umail=".$postEmail."&type=ok' target='_blank'>找回密码</a>
26                . " 或者复制以下链接到浏览器浏览 <br>"
27                . "".$fhurl."?umail=".$postEmail."&type=ok <br>认证码：".$fsjs."<br>请妥善保管！";
28
29      $db_conn->query("UPDATE sc_user SET user_rzm='$fsjs' WHERE user_email='".$postEmail."'");
30
31    // 邮件发送
32
33    echo  SendEmail($smtpserver,$smtpuser,$smtppass,$smtpusermail,$smtserverport,$smtptoemail,$mailtitle,$mailcontent);
34    echo'<script language="javascript">alert("已发送到你的'.$postEmail.'邮箱！");location.href="'.$fhurl.'";</script>';
35
36        }else{
37
38         echo'<script language="javascript">alert("此邮箱不存在！");history.go(-1);</script>';
39
40        }
41
42    }else{
43
44        echo'<script language="javascript">alert("请输入正确的邮箱！");history.go(-1);</script>';
45    }
```

And updated to the database in line 29



Finally, the verification code is obtained by direct blasting with burp tool