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:

```
<?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
<?php
 $pageSplit = explode("/",$page);
 if(isset($pageSplit[1]))
 $pageSplit[1] = (strtolower($pageSplit[1]) == 'list') ? $pageSplit[0].' List' :
 $pageSplit[1];
?>

<?php require_once('inc/topBarNav.php') ?>
 <!-- Content Wrapper. Contains page content -->
 <main id="main" class="main">
   <?php if(in_array($page, ['home'])): ?>
     <div class="col-12">
       <div id="site-header" style="--bg: url(<?= validate_image($_settings->info(
       'cover')) ?>)">
         <div class="header-content">
           <div class="siteTitle"><?= $_settings->info('name') ?></div>
           <hr class="border-light opacity-100 mx-auto" style=
           "width:100px;border-width:3px">
           <a href="<?= base_url.'?page=booking' ?>" class="btn btn-lg btn-primary
```

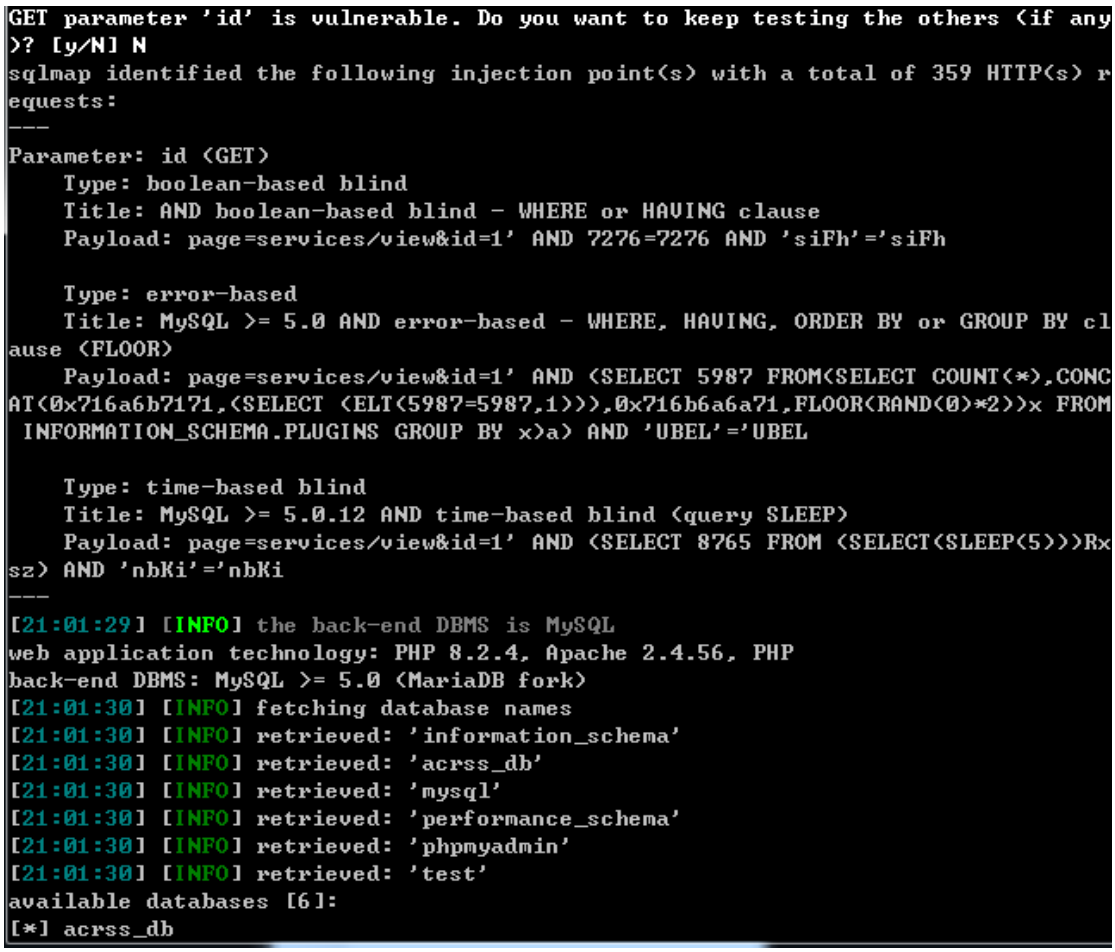
```
        <div id="msg-container">
        <?php if($_settings->chk_flashdata('success')): ?>
        <script>
          alert_toast("<?php echo $_settings->flashdata('success') ?>",'success')
        </script>
        <?php endif;?>
        </div>
        <?php
          if(!file_exists($page.".php") && !is_dir($page)){
              include '404.html';
          }else{
            if(is_dir($page))
              include $page.'/index.php';
            else
              include $page.'.php';

          }
        ?>
```

/services/view.php:

```
<?php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `service_list` where id = '{$_GET['id']}' and
    `status` = 1 ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
    }else{
        echo '<script>alert("service ID is not valid.");
        location.replace("./?page=services")</script>';
    }
}else{
    echo '<script>alert("service ID is Required.");
    location.replace("./?page=services")</script>';
}
?>
```

SQLMAP:



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