攻防世界 web高手进阶区 8分题 blgdel

原创

思源湖的鱼 于 2020-09-13 16:19:08 发布 147 收藏 1

分类专栏： ctf 文章标签： 攻防世界 网络安全 ctf .htaccess

本文链接：https://blog.csdn.net/weixin_44604541/article/details/108562364

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

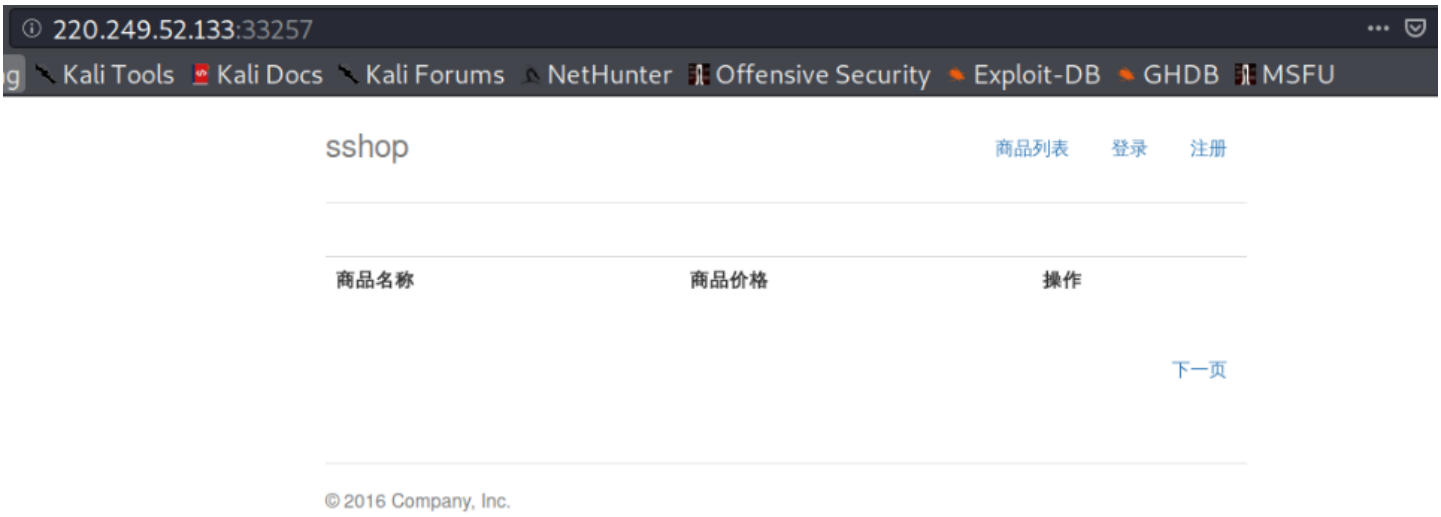
继续ctf的旅程

开始攻防世界web高手进阶区的8分题

本文是blgdel的writeup

解题过程

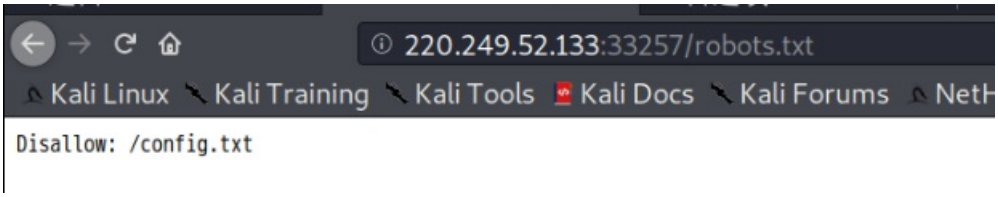
进来界面（后来发现这个界面是环境崩了）

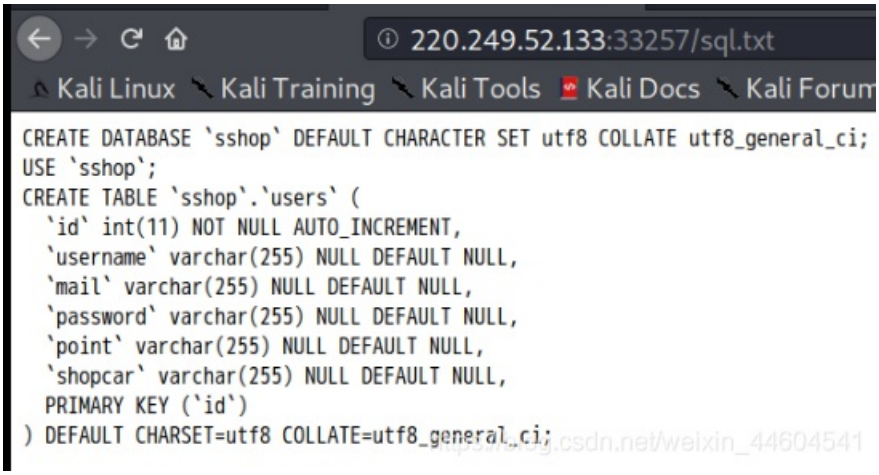


惯例看源码+御剑扫描

发现robots.txt和sql.txt

查看





进入config.txt查看

```
<?php

class master
{
 private $path;
 private $name;

 function __construct()
 {

 }

 function stream_open($path)
 {
  if(!preg_match('/(.*)\/(.*)$/s',$path,$array,0,9))
```

```
 return 1;
$a=$array[1];
parse_str($array[2],$array);

if(isset($array['path']))
{
 $this->path=$array['path'];
}
else
 return 1;
if(isset($array['name']))
{
 $this->name=$array['name'];
}
else
 return 1;

if($a==='upload')
{
 return $this->upload($this->path,$this->name);
}
elseif($a==='search')
{
 return $this->search($this->path,$this->name);
}
else
 return 1;
}
function upload($path,$name)
{
if(!preg_match('/^uploads\/[a-z]{10}\/$/is',$path)||empty($_FILES[$name]['tmp_name']))
 return 1;

$filename=$_FILES[$name]['name'];
echo $filename;

$file=file_get_contents($_FILES[$name]['tmp_name']);

$file=str_replace('<','!',$file);
$file=str_replace(urldecode('%03'),'!',$file);
$file=str_replace('"','!',$file);
$file=str_replace("'","!',$file);
$file=str_replace('.','!',$file);
if(preg_match('/file:|http|pre|etc/is',$file))
{
 echo 'illegalbbbbbb!';
 return 1;
}

file_put_contents($path.$filename,$file);
file_put_contents($path.'user.jpg',$file);


echo 'upload success!';
return 1;
}
function search($path,$name)
{
if(!is_dir($path))
```

```
 {
  echo 'illegal!';
  return 1;
 }
 $files=scandir($path);
 echo '</br>';
 foreach($files as $k=>$v)
 {
  if(str_ireplace($name,'',$v)!==$v)
  {
   echo $v.'</br>';
  }
 }

 return 1;
}

function stream_eof()
{
 return true;
}
function stream_read()
{
 return '';
}
function stream_stat()
{
 return '';
}

}

stream_wrapper_unregister('php');
stream_wrapper_unregister('phar');
stream_wrapper_unregister('zip');
stream_wrapper_register('master','master');

?>
```

代码审计

- 常规的伪协议php,zip,phar都被注销掉了
- 新注册了一个master协议

master协议的几个功能

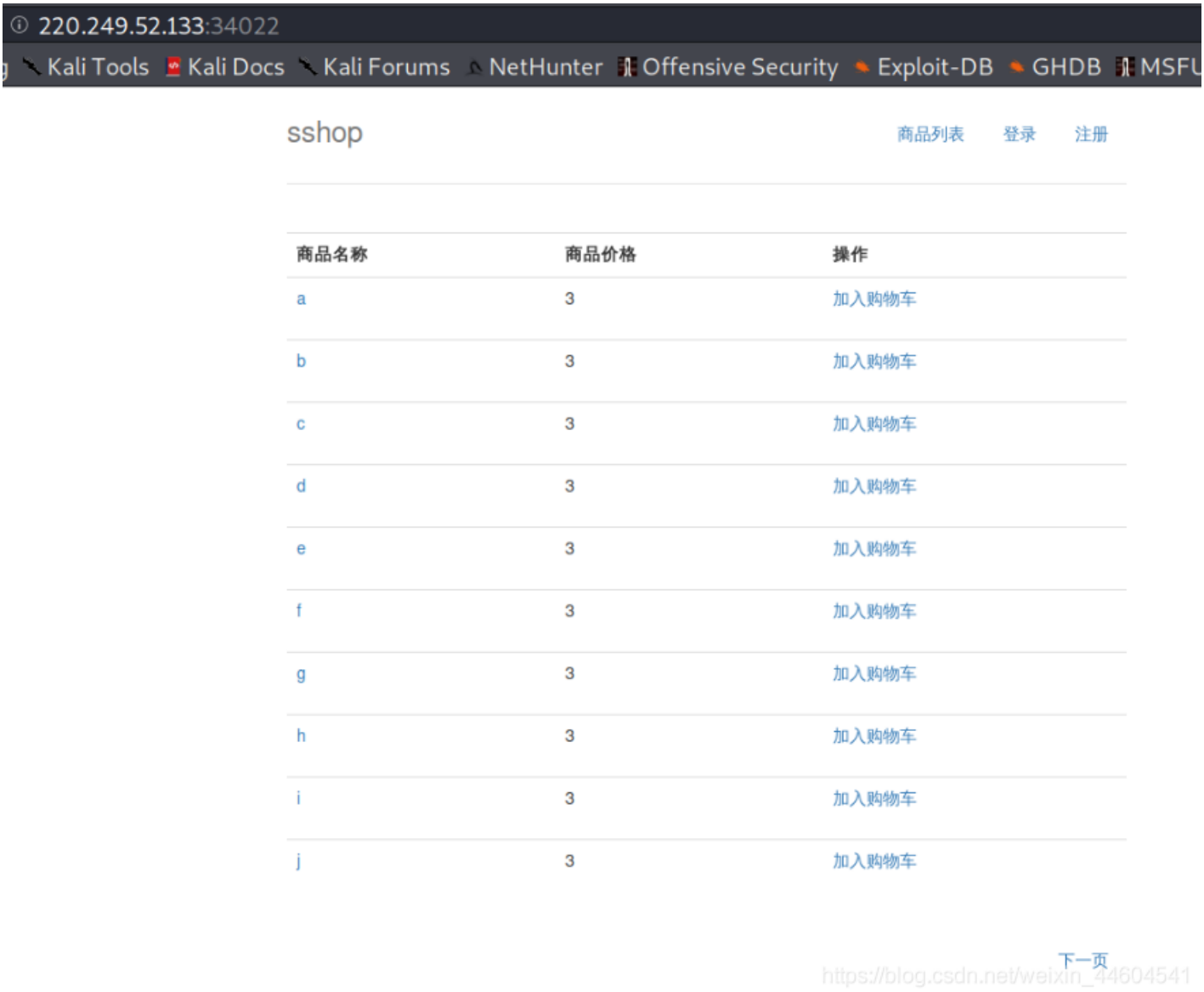
stream_open()
对path的传参和name的传参从字符串到变量，做了一个方法对应

upload()
对上传的文件内容中存在 `< " ’` . 全部替换为 `!`，然后如果匹配到 `/file: http pre etc/is` 就会报错，最后输出文件内容和文件路径

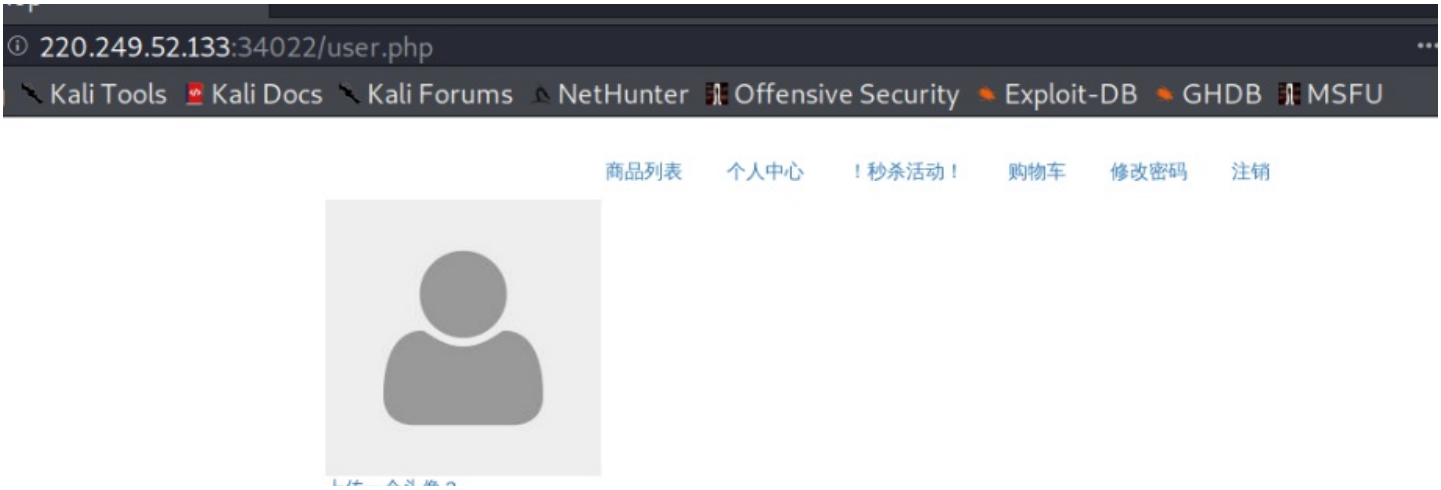
search()
判断了是否存在path路径，对当前目录进行遍历，存在和path路径，对当前目录进行遍历，存在和path路径，对当前目录进行遍历，存在和name相同的文件或者目录替换为空并列出当前目录

估摸着是用master协议进行文件上传了
回到原界面做些尝试
尝试注册登录好几次
没成功。。。哽住
怕不是环境崩了。。。

删除容器重新打开*n
终于正常了。。。
攻防世界的环境真的该整整，一直出问题

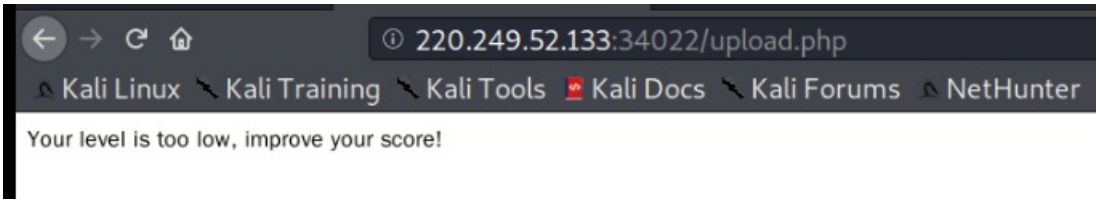


成功注册登录



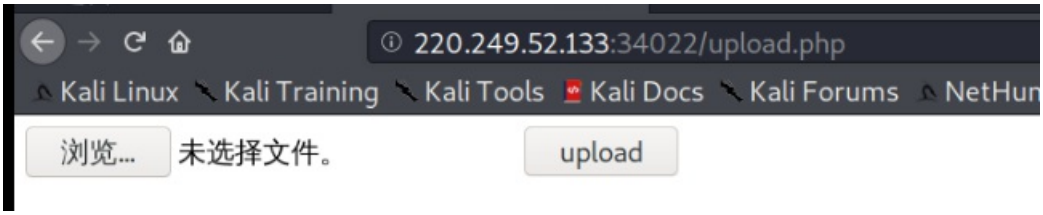
尝试点击各个按钮和在登录注册找密码界面sql注入
都无果

看到上传头像
猜测题意就是从这里着手了
结果返回

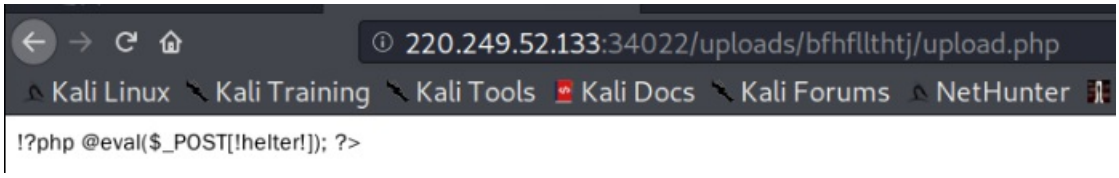


emmm
得想办法提升score
想到注册时的推荐人
尝试后发现推荐一个score+10
到100分后可以上传头像

剩余积分：120.0



根据前面的config
上传普通的一句话木马估摸着是行不通的
做个尝试



发现确实被改掉了
尝试上传jpg抓包修改后缀
失败
。。。。
看来是得按之前的想法
从master协议着手
去查了查
有这么个东西
.htaccess

可以写`php_value auto_prepend_file 1`这种语句

- 相当于文件包含，并在页面加载后自动运行
- 又因为本题文件上传后一个用户一个文件夹，所以.htaccess作用域只在用户文件夹下
- 再上传一个任意.php文件，然后通过访问加载php页面可以触发.htaccess的指令
- php_value

说白了就是通过上传漏洞，上传一个包含点上去
将上传漏洞变为上传+包含漏洞

根据config
可以构造

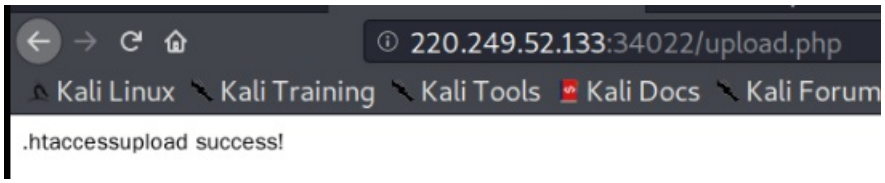
```
php_value auto_append_file master://search/path={}&name={}
```

这样的语句进行搜索
又`\`被正则了
要进行编码为`%2f`

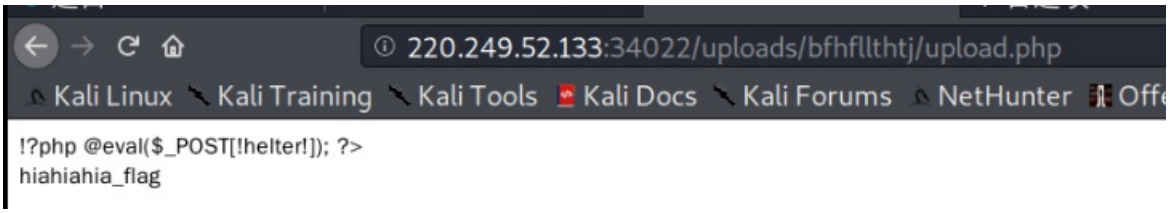
做了一些尝试后
构造payload

```
php_value auto_append_file master://search/path=%2fhome%2f&name=flag
```

保存为`.htaccess`文件
上传

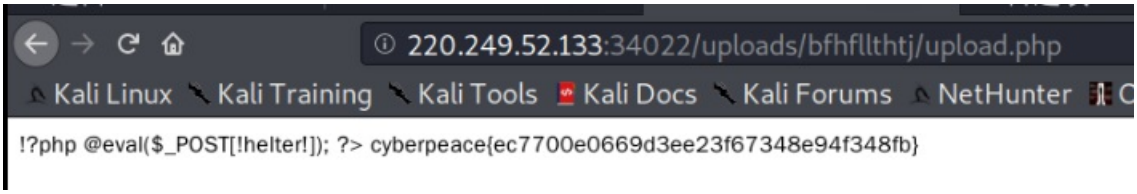


在之前上传的php文件里
返回了flag所在



修改payload

```
php_value auto_append_file /home/hiahiahia_flag
```



得到flag

结语

攻防世界的环境啊
被坑了不知道多少次了
泪流满面
。。。。。。
本题主要卡在.htaccess上
前面就是错路走的有点多

知识点

- robots.txt
- php代码审计
- 正则匹配
- 文件上传漏洞
- .htaccess
- php_value

又学到了新知识