

[CTF刷题篇]攻防世界Web进阶之upload1 Writeup

原创

[\[已注销\]](#) 于 2020-04-22 21:13:46 发布 561 收藏 1

分类专栏: [# 攻防世界 每日CTF](#) 文章标签: [php](#) [安全](#) [信息安全](#) [javascript](#) [安全漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43668710/article/details/105692512

版权



攻防世界 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



每日CTF

4 篇文章 0 订阅

订阅专栏

前言

这是一道文件上传题,常见的考点有:

1. 客户端过滤绕过 // 禁用JS
2. 文件扩展名绕过
3. 黑名单绕过
4. 白名单绕过
5. 内容类型绕过
6. 内容长度绕过

分析

回到这道题,一般先查看源码:

The screenshot shows a browser window with the address bar displaying "Not secure | 159.138.137.79:53699". The browser's developer tools are open, showing the "Elements" tab. A JavaScript code snippet is visible in the console, which is a modification to the Array.prototype.contains method. The code is as follows:

```
<script type="text/javascript">

Array.prototype.contains = function (obj) {
    var i = this.length;
    while (i--) {
        if (this[i] === obj) {
            return true;
        }
    }
    return false;
}
```

```

}

function check(){
upfile = document.getElementById("upfile");
submit = document.getElementById("submit");
name = upfile.value;
ext = name.replace(/^.+\./, '');

if(['jpg','png'].contains(ext)){
    submit.disabled = false;
}else{
    submit.disabled = true;

    alert('请选择一张图片文件上传!');
}
}
}

```

https://blog.csdn.net/qq_43668710

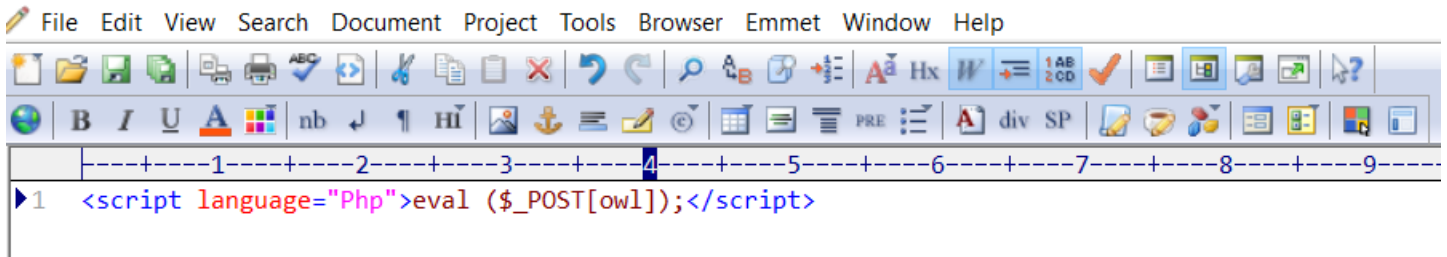
发现是在客户端验证,所以直接禁用JavaScript:



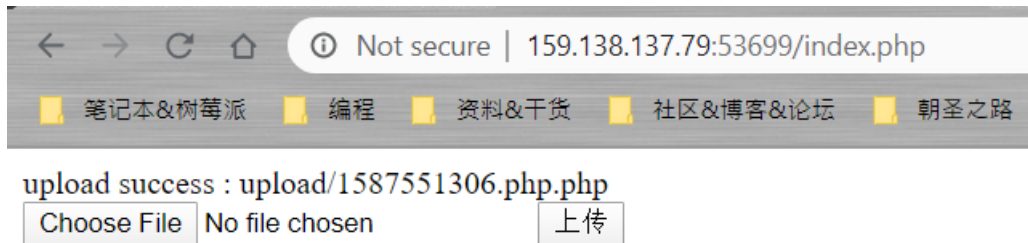
https://blog.csdn.net/qq_43668710

现在就是常规操作了,传webshell上蚁剑。

先整个webshell:

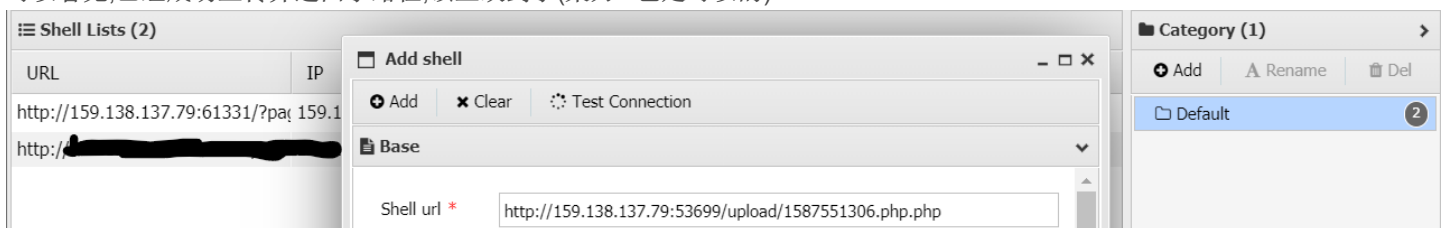


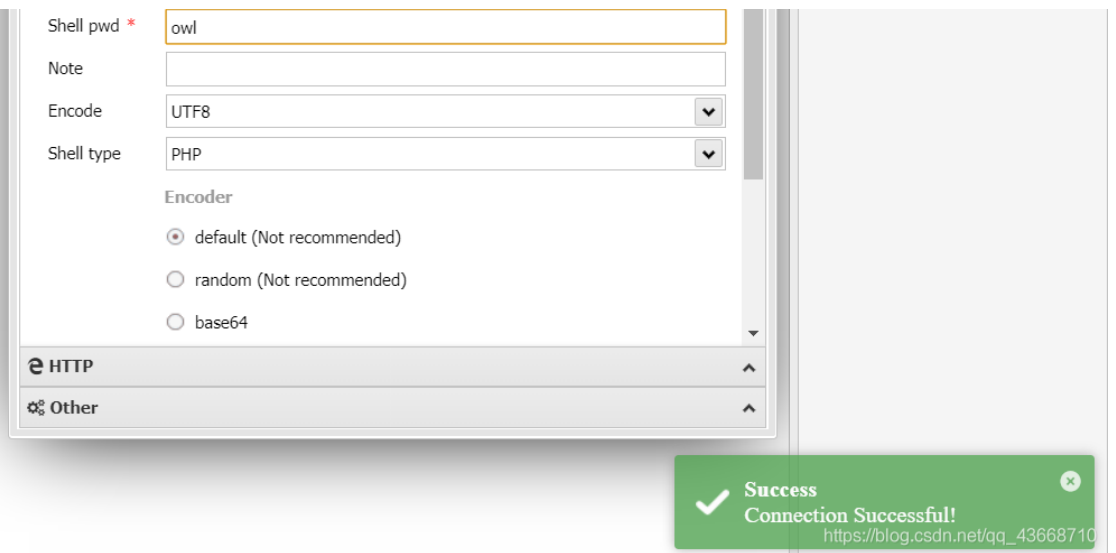
上传成功:



https://blog.csdn.net/qq_43668710

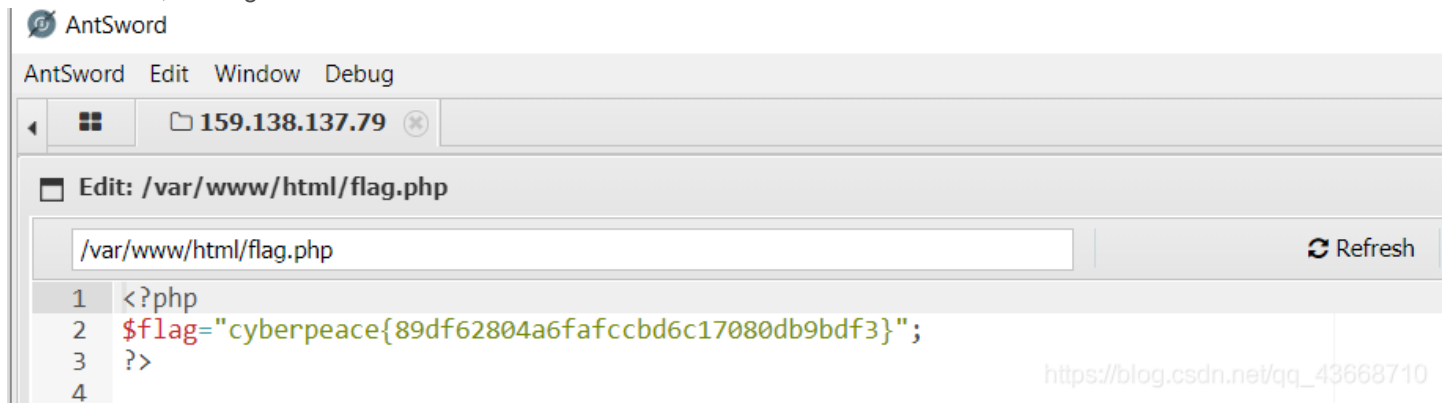
可以看见,已经成功上传并返回了路径,该上蚁剑了(菜刀也是可以的):





连接成功。

然后遍历目录,找到flag即可:



成功拿到flag!

结语

刷题的体验还是很不错的!

比起刚开始接触ctf时的那股不知所措的劲儿,现在遇上一些不是特难的题,终于有了自己的解题思路,而不是只能看别人的writeup!