ctf php文件上传图片格式,CTF-WEB：文件上传

转载

燕仰 于 2021-04-12 14:54:32 发布
文章标签： ctf php文件上传图片格式

文件上传

一句话木马

利用文件上传漏洞往目标网站中上传一句话木马，然后就可以在本地获取和控制整个网站目录。利用一句话木马进行入侵时需要满足木马上传成功未被查杀，知道木马的路径在哪并保证上传的木马能正常运行。一个简单的 PHP 一句话木马如下：

@ 表示后面即使执行错误也不报错，eval()函数表示括号内的语句字符串什么的全都当做代码执行，$_POST['flag']表示从页面中获得 flag 这个参数值。

上传过滤

为了使得网页不容易被攻击，网页经常需要通过一些手段来过滤不希望接收的文件。首先是 multipart/form-data 过滤，该过滤需要在表单中进行文件上传时，就需要使用该格式，意思是他通过表单会对文件格式再进行一次判断，并会在后端进行判断。这种过滤只支持小写字符，因此绕过方法为将抓到的包中的 Content-Type 字段中的 “multipart/form-data” 中随便一个字母改为大写。

第二是文件类型过滤，为了不让用户随便传些文件，只是要让用户上传图片时，就可以限制只能上传图片。还有一种是文件后缀名过滤，例如后缀名是 “.php” 的文件都拦截不能上传，如果是在解题的情况下可以尝试用 PHP 其他后缀进行上传例如：php2, php3, php4, php5，phps, pht, phtm, phtml。

webshell

当网页已经上传过一句话木马时，说明可以利用该木马连接到网页上，例如下面这个网页。

“web” 的含义是显然需要服务器开放 web 服务，“shell” 的含义是取得对服务器某种程度上操作权限。webshell 常常被称为入侵者通过网站端口对网站服务器的某种程度上操作的权限，可以使用蚁剑或者菜刀等工具进行提权。以蚁剑为例，打开蚁剑后右键选择添加数据。

然后填入需要提权的网页 url，以及一句话木马的连接密码。

添加之后可以右键进行一系列操作，例如可以查看网页的文件，选择文件管理。

之后就可以查看并操作网页的文件了，例如这个网页的 html 目录下就有 flag。

例题：求 getshell

打开网页，这个明显是文件上传漏洞，题目要求传入一个图片，不能是 php。

这是后缀名黑名单检测，注意到使用了 multipart/form-data，所以通过对请求头中的 Content-Type 进行大小写绕过，将 multipart/form-data 随便一个字母改成大写。然后这个网页只能上传文件，因此把 Content-Type 字段的值改为 “image/jpeg”。最后还有个文件扩展名过滤，测试后发现 “.php5” 后缀没有被过滤。综上所述文件上传的包修改如下，上传获得 flag。

例题：upload1

打开网页，看到一个文件上传的按钮，考虑上传一句话木马之后用蚁剑连接。

首先先看一下源码，源码会对传入的文件的类型进行过滤，也就是说如果传的不是图片，上传按钮会被禁用并弹窗报错。

```
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(/^.+\./,''); //删除文件的名称
if(['jpg','png'].contains(ext)) //检查后缀是否为 jpg 或 png
{
submit.disabled = false;
}
else
{
submit.disabled = true;
alert('请选择一张图片文件上传!');
}
}
```

由此可见过滤是在前端，我们只需要绕过前端的过滤就照样能提交一句话木马。先将一句话木马的后缀名改为 jpg，然后上传到网页。接着按上传按钮，然后用 Burp 抓包，修改文件名的后缀为 “.php”。

上传成功后会返回一个文件名，直接访问是没有用的，使用蚁剑进行连接。

连接之后在 html 目录下有个 flag.php，打开就能看到 flag 了。