文件上传漏洞小总结

转载

dianmangji9200 于 2019-08-04 10:50:00 发布 106 收藏
文章标签： php javascript 前端 ViewUI
原文链接：http://www.cnblogs.com/Qi-Lin/p/11297452.html

欢迎查看upload-labs writeuphttps://www.cnblogs.com/Qi-Lin/p/11296761.html

前端绕过

绕过js,通过bp中的proxy中的option中的选项移除掉javascript脚本，或者通过直接在浏览器中删除掉js

绕过mime-type

mime是多用途互联网邮件扩展类型，用于设定某扩展名文件的打开方式，如.png在数据包的中的content-type为image/png，所以可以通过bp截断绕过

绕过黑名单

黑名单没有白名单安全，可能有遗漏

- php可以改为php3,php4,php5,phtml上传
- .htaccess绕过，.htaccess是apache服务器中的一个配置文件，可以实现301重定向，自定义404错误页面，改变文件扩展名，阻止或允许用户访问特定目录或文件等。可以将.htaccess的内容写入sethandler application/x-httpd-php，这可以设置当前目录所有文件都用php解析。不过对应http.conf中allowoverride 应设置为all
- 大小写绕过，只适用于windows，windows大小写不敏感
- 空格绕过，windows中文件扩展名后的空格会做空处理
- 点号绕过，windows下最后一个.会被自动剔除
- 特殊符号绕过，windows下，如果上传的文件名后缀为php::$DATA会在服务器生成后缀为Php的文件，内容和上传内容相同，并被解析
- 组合绕过，如1.php空格.
- 如果上传大小有限制可以先上传小文件，然后利用小文件上传大文件
- 如果代码是对黑名单进行空替换，可以利用双写绕过

绕过白名单

在系统对文件名读取时，如果遇到0x00会认为读取结束，如：1.php0x00.jpg在上传时认为是jpg,但在新建该文件文件时保存为1.php
但在php5.3之后的版本已经修复，并且受gpc,addslashes函数影响

get型截断

post截断

图片webshell

利用图片的webshell需要利用文件包含漏洞，这是因为在php中使用include,include_once,require,require_once函数包含的文件无论文件名称是什么都会被当做php代码执行

- 可以在代码中加入相关字符，如简单的为：

```
GIF98A
<?php
phpinfo()
?>
```

- 也可以利用隐写将木马追加到图片结束符后

利用竞争条件上传

- 文件上传后是先保存为一个临时文件，然后再重命名保存文件，如果网站允许上传任意文件，可能检查上传文件是否包含webshell，如果包含就删除，使用unlink删除文件。也可能发现不是指定类型，就使用unlink删除。所以，如果在删除之前访问上传的文件，就会执行文件中的代码
- 例如：在文件中写入如下代码，此文件在执行时，新建一个shell.php的文件包含木马

```
<?php
fputs(fopen('shell.php',w),'<?php @eval($_post["pass"]) ?>');
?>
```

- 在上传时不断发送http请求，请求该文件，可以利用一个python脚本如：

```
import requests
while true:
    requests.get("路径")
```

转载于:https://www.cnblogs.com/Qi-Lin/p/11297452.html