

文件上传

简介:

文件上传一般是指，网站中如果存在web文件上传漏洞，那么那么恶意用户就可以利用文件上传漏洞将可执行脚本程序上传到服务器中，获得网站的权限用户可以通过上传恶意脚本，从而控制整个网站。这个而已脚本被称为webshell。也就是网页后门。也就是文件上传攻击指的是，通过上传漏洞将webshell上传到服务器，从而开启一个网站后门。

JS 检测绕过攻击

即绕过前台的js检测文件后缀名:

使用浏览器的插件，删除检测文件后缀的JS代码，然后上传文件即可绕过。即通过前台浏览器控制台删除触发检查的函数。

先将文件改成允许上传的后缀名，其次发送完上传的报文后，抓包修改文件名。


```
POST /upload/upload2.php HTTP/1.1
Host: www.ccctf.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----18441182091610745159615033231
Content-Length: 352
Referer: http://www.ccctf.cn/upload/js.html
Cookie: id=1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----18441182091610745159615033231
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg

<?php
phpinfo();
?>

-----18441182091610745159615033231
Content-Disposition: form-data; name="submit"

submit
-----18441182091610745159615033231--
```



文件后缀绕过攻击

即将文件后缀设置成1.php.xxxx。在Apache的解析顺序中，是从右到左开始解析文件后缀的，如果最右侧的扩展名不可识别，就继续往左判断。

文件类型绕过攻击

如果服务器是通过content-type来对文件进行判定的，那么我们就可以通过抓包修改content-type从而实现越过服务器过滤。

文件截断绕过攻击

截断类型:PHP%00截断 截断原理：由于00代表结束符，所以会把00后面的所有字符删除。截断条件：PHP版本小于5.3.4，PHP的magic_quotes_gpc为OFF状态。如：如果需要上传jieduan.php那么我们只要上传jieduan.php%00.jpg,那么后台php运行的时候就会自动截断%00后面的字符串。就只剩下jieduan.php。成功上传。

竞争条件攻击

一些网站上传文件的逻辑是先允许上传任意文件，然后检查上传的文件是否包含WebShell脚本，如果包含则删除该文件。这里存在的问题是文件上传成功后和删除文件之间存在一个短的时间差（因为要执行检查文件和删除文件的操作），攻击者就可以利用这个时间差完成竞争条件的上传漏洞攻击