ctf题目php文件上传如何绕过_php文件上传漏洞-客户端JavaScript检测绕过-[ACTF2020 新生赛]Upload复现...

原创

weixin_39632524 于 2021-01-14 15:56:28 发布 114 收藏
文章标签： ctf题目php文件上传如何绕过

本文链接：https://blog.csdn.net/weixin_39632524/article/details/112950656

文件上传漏洞

文件上传漏洞是指由于程序员在对用户文件上传部分的控制不足或者处理缺陷，而导致的用户可以越过其本身权限向服务器上上传可执行的动态脚本文件。这里上传的文件可以是木马，病毒，恶意脚本或者WebShell等。“文件上传”本身没有问题，有问题的是文件上传后，服务器怎么处理、解释文件。如果服务器的处理逻辑做的不够安全，则会导致严重的后果。

webshell

WebShell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称之为一种网页后门。攻击者在入侵了一个网站后，通常会将这些asp或php后门文件与网站服务器web目录下正常的网页文件混在一起，然后使用浏览器来访问这些后门，得到一个命令执行环境，以达到控制网站服务器的目的(可以上传下载或者修改文件，操作数据库，执行任意命令等)。 WebShell后门隐蔽较性高，可以轻松穿越防火墙，访问WebShell时不会留下系统日志，只会在网站的web日志中留下一些数据提交记录。

web C/S模式文件上传流程

客户端JavaScript检测(通常检测文件扩展名)

服务器端MIME类型检测(Content-Type内容检测)

服务器端目录路径检测(检测跟path参数相关的内容)

服务器端文件扩展名检测(检测跟文件extension相关的内容)

服务器端文件内容检测(恶意代码检测)

文件上传检测

客户端JavaScript检测

在文件上传第一步，客户端会对准备上传的文件进行检测，一般会对文件的类型进行限制，比如只允许上传jpg、png、gif等文件，防止攻击者直接上传恶意代码文件。

绕过方法：这个绕过其实比较简单，我们只需要更改木马问价的文件后缀为允许的文件类型，然后burp抓包，在报文中更改上传的文件名后缀为php等可以解析的文件类型就可以。下面这个就是一个例子：

文件上传类型检测

MIME类型检测

服务器端会对客户端上传的文件的Content-Type字段的值进行检测，如果其类型为白名单允许的，那么能够上传，否则失败。比如网站有MIME类型检测的话，直接上传php木马文件必然失败，只能上传白名单中的文件类型。

绕过方法：burp截取上传文件的数据包，更改Content-Type字段的值即可。

目录路径检测

目录路径检测，一般就检测路径是否合法，但稍微特殊一点的都没有防御。

绕过：

1.%00、0x00截断绕过

/fckeditor264/filemanager/connectors/php/connector.php?
Command=FileUpload&Type=Image&CurrentFolder=fuck.php%00file.jpg HTTP/1.0

s1awwhy.php.jpg 改为 s1awwhy.php0x00jpg，当文件系统读取到0x00或者%00时，会认为文件已经结束

文件扩展名检测

服务器端可能会根据自己设定的黑白名单对客户端提交的文件扩展名进行判断，如果上传的文件扩展名是黑名单里面所限制的，则不允许提交，否则正常上传。

例如，.php被禁用，那么就可以在php后面加上一个任意文件名后缀。s1awwhy.php------>s1awwhy.php.abc

文件内容检测

服务器端可能会对文件头部进行检测，可以通过在一句话木马前面加上文件头部，从而实现绕过。

htaccess攻击

方法 1 ：

.htaccess文件调用php的解析器其解析另一个文件名包含“s1awwhy”的文件，从而实现木马文件的解析。
.htaccess文件内容如下：

SetHandler application/x-httpd-php

攻击方法：上传.htaccess文件，然后上传文件名包含hack的木马文件。

方法 2 ：将.jpg文件当做.php文件来解析

.htaccess文件内容如下：

AddType application/x-httpd-php .jpg

攻击方法和方法1一样。

[ACTF2020 新生赛]Upload

首先进入题目可以看到可以上传文件，基本可以猜出是文件上传。

试了一下，有文件名扩展过滤，只能上传图片，jpg、gif、png

看一下源码，发现有客户端JavaScript检测。

绕过这个客户端检测有两种方法。

方法 1 ：火狐浏览器直接删除客户端检测代码，然后上传webshell文件

方法 2 ：burp抓包更改文件扩展名

先构造一个恶意文件，先用phtml文件试一下。

方法 1 ：

删除浏览器客户端检测代码，直接上传phtml文件

发现直接能够上传成功，并且有文件路径。能够访问，上传成功。

可以用菜刀进行连接，也可以传参得到flag。

方法 2 ：

更改文件名后缀绕过客户端检测，然后抓包更改文件名，上传phtml文件。

上传成功。之后的步骤和方法 1 一样了，用菜刀连接或者传参拿flag。