主要是前两天，上海交大有个 0ctf 的比赛 自己做了一下 有一些收获 涨姿势了 就写一些关于 web 方向的 writeup
比赛不给组队是个比较蛋疼的事情 逆向 溢出无力啊 要加油学习 还有很多有趣的东西要研究
0ops 组织的 0ctf 的比赛链接：http://ctf.0ops.net 平台在比赛结束之后还有开放 好评 大家还可以上去练习
0×01 web1 Spy
web1 的题目

给出了一个 ip
http://202.120.7.5/
要比较数的大小

第一关 尝试输入过后 发现只能 3 位数 而对方的数字 都是 4 位数 比他的小
第一关比较简单 查看一下源码 发现是 maxlength 限制了长度 用火狐 自带的调试器 或者是用 firebug 修改一下长度就可以突破

当然了 使用抓包改包 把发送的数据修改也是同样可以的
第二关
http://202.120.7.5/XvPzL13tt2yaG6Vv123Kkk.php
看起来差不多 只是使用的相同的方法 会说你故伎重演 要换种思路才行
多次尝试输入之后发现 他是有一定几率返回 3 位数的 所以只要我们输入 999 遇到 3 位数时就可以赢了
可以采用爆破的方法 burp 设置一下爆破 一直发同一个 999 的请求 就有机会过关

第三关
http://202.120.7.5/ZK8F2HFAYfashfu2b1JFIO3.php
要比较谁输入的倒数比较小 小的获胜
尝试最大的 99999 发现赢不了
容易发现他的是正的数 尝试一下负数 -1 就过关了

第四关
http://202.120.7.5/F9823HABVofu829jfiRF9F.php
这次要比 ascii 码的乘积的大小
怒查 ascii 表 fuzz 尝试一些 .发现可以小数点 换个思路 也是有别的进制的表示方法 比如 16 进制 0xaaaa 就可以了

0ops{Zu1L1h4iD35hUxu3J1aj14oC0s1neUF0}

Ox02 web2 System

http://202.120.7.107:888/
登陆的话 容易想到的是 万能密码登陆
admin' or '1'='1
发现报错了
那么我们测试用注释 admin' or '1'='1'–
发现也报错了
换个姿势 admin' or '1'='1'#
原来这里是过滤了– 这次比赛好像比较喜欢过滤– 用#代替了就可以了后面还会有 然后发现就可以了
Welcome! 0ops{He1loEv3ry0neM1a4444444444o}

Ox03 web3 Signal

http://202.120.7.106/
发现又是一个登陆 都是发现是个 ip 作为自己的 id 还要密码的登陆
这题有点蛋疼 研究了很久 也没搞出来
砸 exp 看到/cgi-bin/ 以为会有远程命令执行 测过发现也不行
然后思路就断了
中间也试过组字典去爆破 无果
到后来做出来的人太少 主办方给出了提示

之前在极客大挑战 ecshop 的一个漏洞 有看过一个数组绕过的类型检测的技巧
这次可以用 ps[]=数组绕过了检查

死猫牛题目一上来就给秒杀了 吓尿全场 后来他说用 defcon 2013 web500 的猥琐技巧可以绕过 就是这个 ps[]=
直接去找 writeup 来看看
http://www.blue-lotus.net/def-con-ctf-qualifier-2013-3dub-5-writeup/
0ops{H3110K17tY_1S_0u3_BeSt_FFfFfr1en:D}

0×04 web4 OnlyAdmin

http://ctf.0ops.net/attachment/download/onlyadmin.zip
http://202.120.7.107/login.php

看起来是个源码审计的东西
那就下下来看看呗
在 core.php 第 4 行开始的 CreateUserTable()看到

```
01 function CreateUserTable()
02 {
03         # Create user table
04         $query =
05                 "CREATE TABLE IF NOT EXISTS `only_admin_know_flag` ".
06                 "(".
07                 "`username` VARCHAR(24) NOT NULL, ".
08                 "`password` VARCHAR(32) NOT NULL, ".
09                 "`access_level` INT(10) UNSIGNED NOT NULL DEFAULT 0".
10                 ")";
11         mysql_query($query);
12
13         # Create super user
14         $password = strtoupper('e1bf0a56169f9d224c30bf6c8f06238b');
15         $query =
16                 "INSERT INTO `only_admin_know_flag` ".
17                 "VALUES ( ".
18                 "'Admin', '$password', 1337".
19                 ") ";
20         mysql_query($query);
21 }
22 .....
```

这里是关键的函数 这里给了一些数据库的操作 发现给了个 Admin 的用户 估计就是想办法去登陆这个用户
这里给出的 md5 解不开 也不会那么简单 让你去跑 md5

```
1 "`username` VARCHAR(24) NOT NULL, ".
```

这句是关键 注册的 username 是 24 位的 这里可以使用 mysql 的截断
使用一个 Admin 开头的 追加超过 20 位空格 最后还需要加上个空格防止 这一串空格被过滤
在 core.php 80 行

```
1 function Register()
2 {
3         $uname = trim($_POST['username']); # trim usernames
4 ......
```

这里用了 trim 对开头以及结尾的空格进行了过滤

使用 Admin a 注册就可以被截断变成了 Admin 在用 Admin 和你自己的密码登陆就可以了
Hello Admin. You would be logged in with an access_level of 1337.
FLAG: 0ops{4811b89431816721abfdbf43012286f5}
Your account has been deleted

Ox05 web05 Deadline

http://202.120.7.105:888
查看一下源代码 发现了注释

```
1 <!-- P2dldGRlYWRsaW5lb2Y9 -->
```

解一下 base64
?getdeadlineof=
是个参数 带进去看看
http://202.120.7.105:888/index.php?getdeadlineof=1
都给了参数了 尝试一下注入呗
发现有过滤 sqlmap 也跑不动
这题一直没人做出来 除了一大早可以用 sqlmap 跑后来就不行了
然后主办方就给出来提示

fuzz 测试测试 发现了一个有趣的东西 换行符 %0A
会去测试这个也是因为之前的一个韩国 codegate 题目的练习
http://appleu0.sinaapp.com/?p=136
加上了%0A 之后发现就可以各种注入了
可以使用 union 联合查询 order by 不出来 那么手工加一下 union select 到 4 就出错了
那么可以确定 字段是 3
http://202.120.7.105:888/index.php?getdeadlineof=3%0Aand%201=2%20union%20select%201,2,3
一开始眼拙还以为没有输出 后来才看到输出是在 2 这个位置 转换成了日期 时间了
使用

http://202.120.7.105:888/index.php?getdeadlineof=3%0Aand%201=2%20union%20select%201,hex%28loaD_file%280x2F6574632F706173737764%29%29,3

发现报错了 估计是太大 有个想法手工一位位去 做出来比赛都结束了
直接上 sqlmap

```
sqlmap -u "http://202.120.7.105:888/index.php?getdeadlineof=1%0A"
--file-read /etc/passwd
```

这样子就能读取到文件了 在文件的最后一行会有 key
0ops{AbCdEfG123zzy7896321KKkk-==||><}
比赛之后 主办方发了一部分源码出来

```
01 if ( ! empty($_GET['getdeadlineof'])) {
02                 $fflag = true;
03                 $a = $_GET['getdeadlineof'];
04
05                 if (!preg_match( '/^[0-9]+-?[0-9]*$/m' , $a)) {
06                 //if
(preg_match( '/(select|union|\\|\/|\' |\s)+/s' , $a)) {
07                                 die("又在瞎搞! 注意点儿! ");
08                 }
09
10                 mysql_select_db(' 0ctf' , $my);
11                 if ($result = mysql_query("select * from web400 where
id=" .$a." order by id", $my)) {
12
13                 } else {
14                                 die("出错了! 瞎搞什么! ");
15                 }
16                 mysql_close($my);
17 } else {
18                 $fflag = false;
19 }
```

在这里 %0A 是绕过了 preg_match('/^[0-9]+-?[0-9]*$/m', $a) 这里 m 参数
只检测^ $之间的 即换行之后就不进行正则匹配 就绕过了

最后的结果是第 10 名