信息泄漏漏洞-用户信息

0x01 用户信息泄漏原理

拿评论区举例

评论区的一些个人信息一般都是加密的，如果网站加密方式是通过前端进行加密或打*号的方式的话，那么他在传输是就是等于明文传输了，那么我们就可以通过抓包查看返回包获取到他人泄漏的个人信息如: 用户的身份证,银行卡,电话号码,尽用户自己能看到的信息等等

0x02 漏洞点

1.各种评论区

如前端用户名或者手机号是 133******10 在流量交互是明文的并未加密，此时抓包查看 获取用户信息的接口进行分析观察是否存在泄漏用户个人信息。

2.各种播报栏目

如下图这种播报栏，也是一样 信息加密处理不当的话，我们是可以看见下面这些匿名用户都是谁，他的 uid 啊这些等等信息。这不又是个 100 或者 50 块钱了么，轻轻松松

项目战报

匿名用户在 某金融行业公益众测项目项目中 疯狂斩杀连续提交 4 个漏洞

2022-04-02 10:57:08

匿名用户在 某金融行业公益众测项目项目中 疯狂斩杀连续提交 2 个漏洞

2022-04-02 10:39:47

Hot_pot在 某互联网行业标准众测项目项目中 疯狂斩杀连续提交 2 个漏洞

2022-04-02 07:08:02

匿名用户在 某金融行业公益众测项目项目中 疯狂斩杀连续提交 3 个漏洞

2022-04-01 16:59:57

匿名用户在 某金融行业公益众测项目项目中 疯狂斩杀连续提交 2 个漏洞

2022-04-01 16:32:33

3.各种用户排行榜

比赛排行，积分排行，抽奖实时播报等等，都是需要获取用户信息

4.转账提现处

转账处比如 a 转 100 给 b，此时输入 b 的账户，点击程序会验证账户是否存在 -> 返回对应的用户信息 -> 转账成功

如果该站点对返回的用户信息未加密得当或者是返回了其他个人信息比如:返回了身份证，姓名，手机号等等

提现处可看银行卡，身份证这些信息是否加密脱单

5.客服服务处

发起客服聊天时如果信息加密处理不当或者返回了不该返回的用户信息时是可以在返回包中看见客服的工号，姓名等信息

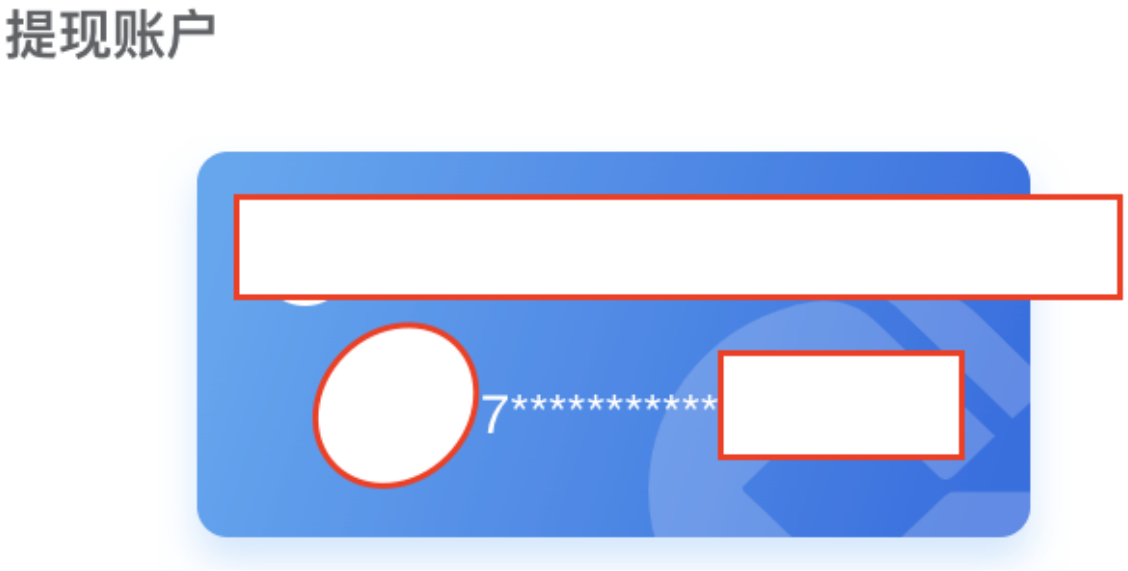
6.各第三方平台

Github，一些员工如果安全意识不足 上传仓库中包含了自己个人公司邮箱和密码，源代码数据库密码，等等泄漏

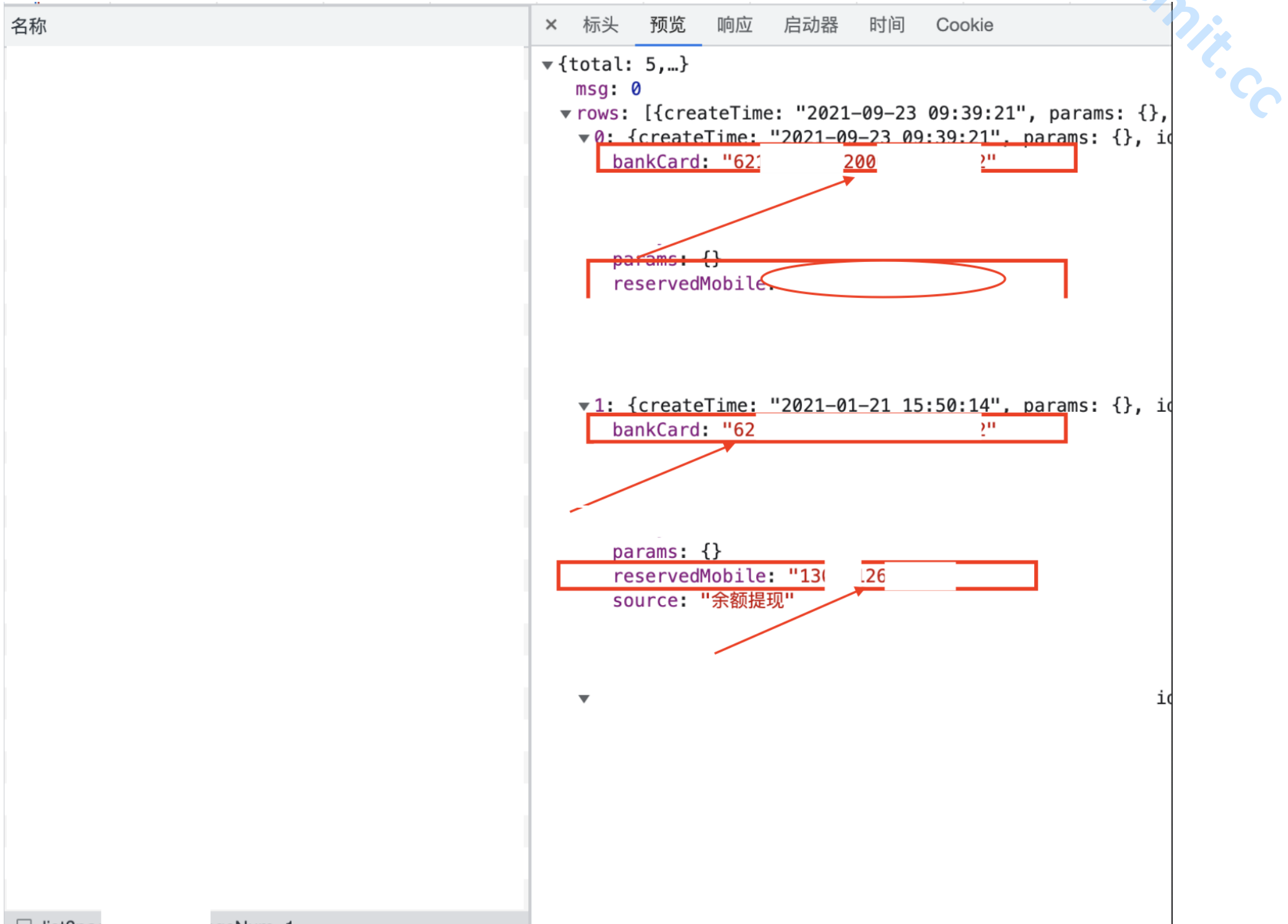
0x03 一个简单的案例

用户信息泄漏具体要根据不同厂家而定,就比如 a 厂家可能收前端的自己身份证，银行卡泄漏，这种一般都是低危 或者 运气好可以评中

该案例是到自己的个人信息处在前端看银行卡号是被打了*号的



但是抓包可以看并没有加密*号,完完全全都是明文


名称
标头
预览
响应
启动器
时间
Cookie
{total: 5,…}
msg: 0
rows: [{createTime: "2021-09-23 09:39:21", params: {},
0: {createTime: "2021-09-23 09:39:21", params: {}, ic
bankCard: "621 200 2"
params: {}
reservedMobile:
1: {createTime: "2021-01-21 15:50:14", params: {}, ic
bankCard: "62 2"
params: {}
reservedMobile: "130 126
source: "余额提现"