第七期

业务安全实战攻防

平安SRC线上沙龙系列主题活动

- 时间：2024.11.22 14:00~17:00

主办方 平安安全应急响应中心 PINGAN Security Response Center

合作伙伴 补天 漏洞响应平台 | 百度安全应急响应中心 Baidu Security Response Center | 度小满安全应急响应中心 Du Xiaoman Security Response Center | 无糖信息 | DAY 1 | TIMELINESEC | 北山学院 | 长亭科技

业务深耕下的逻辑漏洞攻防实战

Longwaer

Day1安全团队

演讲嘉宾简介：

ID：Longwaer

Day1安全团队核心成员

国内安全行业资深从业人员

补天漏洞响应平台特邀白帽讲师

国内多家SRC-TOP级白帽

目录

PART ONE

简单粗暴的信息收集

简单粗暴的信息收集

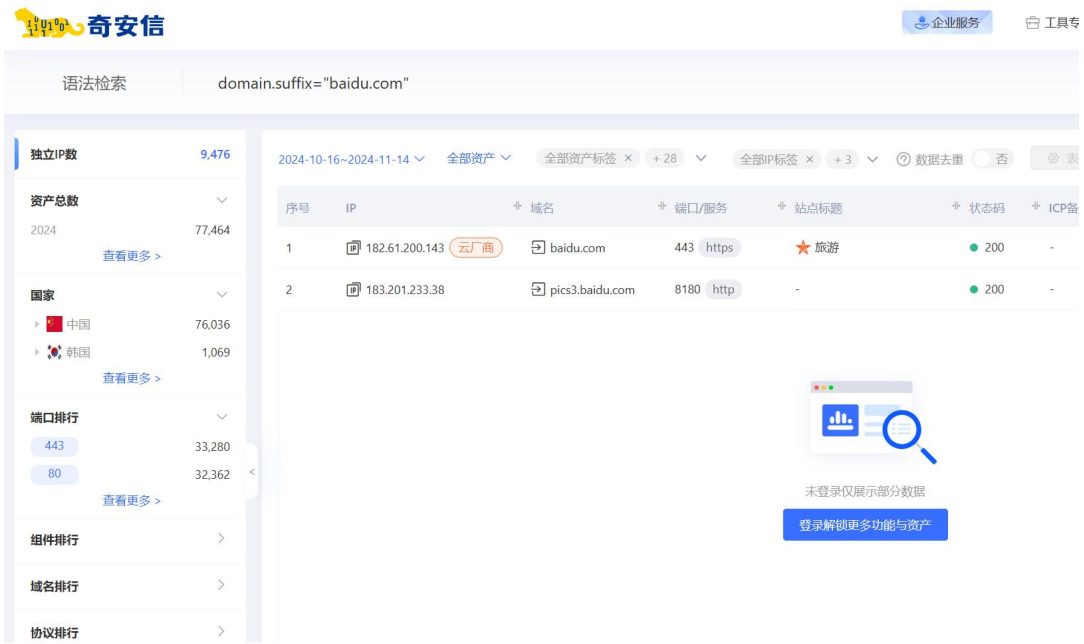
PINGANSECURITYRESPONSECENTER

ARL : 灯塔

简单粗暴的信息收集

PINGANSECURITYRESPONSECENTER

Fofa:https://fofa.info/



Hunter:https://hunter.qianxin.com/

简单粗暴的信息收集

PINGANSECURITYRESPONSECENTER

公告、一些往期的众测

还有就问问朋友都挖哪些?

朋友：这个站 你要能挖出洞来。

算你厉害！！！！

01 活动详情

活动时间：2024年11月12日至12月2日24点

活动范围：产险互联网资产，包括但不限于：

好车主、好生活、企业宝、创保网、保险商城、产险官网等，以及相关App、网站和小程序。（以及其他可确认为产险资产，要能证明危害）

*业务情报和隐私合规问题不在本次活动收集范围内

漏洞奖励：

有效中危及以上漏洞1.5倍奖励

漏洞等级	奖励/元
严重	12000
高危	5000
中危	1500
低危	100

大众认知中的逻辑漏洞

大众认知中的逻辑漏洞

PINGANSECURITYRESPONSECENTER

改个id？ 修改个返回包？

遍历下隐藏参数？

请求	payload	状态码	错误	超时	长度	注释
12	11	200			429	
10	9	200			430	
11	10	200			430	
56	55	200			430	
0		200			431	
9	8	200			431	
13	12	200			431	
14	13	200			431	
1	0	200			445	
16	15	200			448	
29	28	200			448	
38	37	200			448	
59	58	200			448	

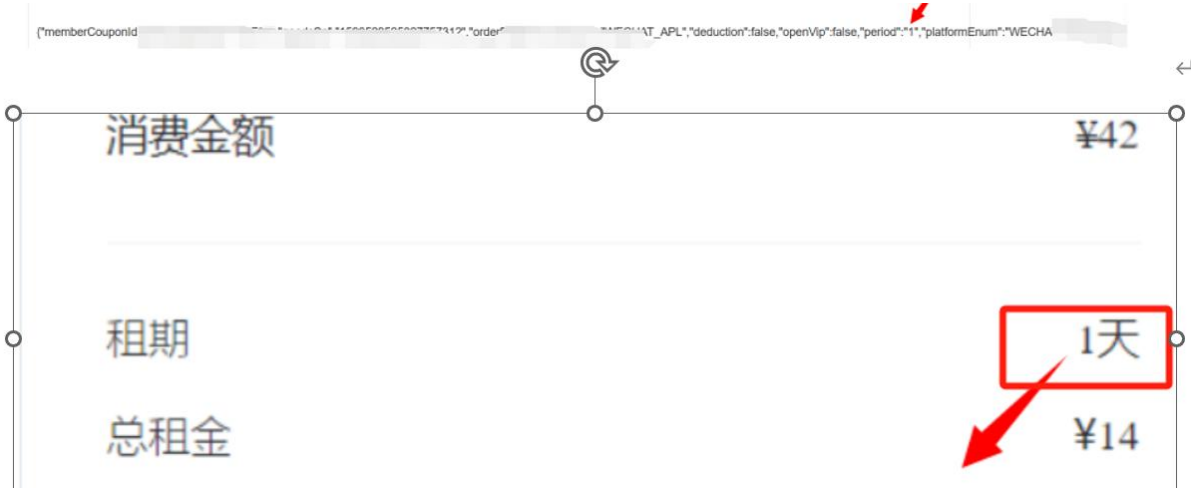
大众认知中的逻辑漏洞

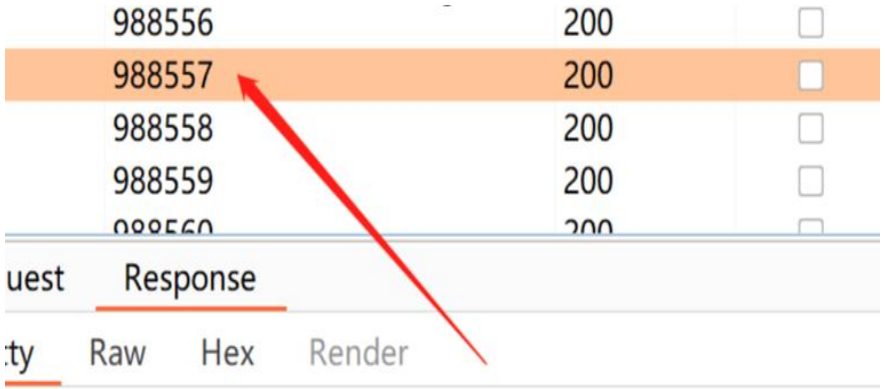
PINGANSECURITYRESPONSECENTER

支付修改个天数？并发点个赞？

六位数的验证码爆破？

等等……





大众认知中的逻辑漏洞

PINGANSECURITYRESPONSECENTER

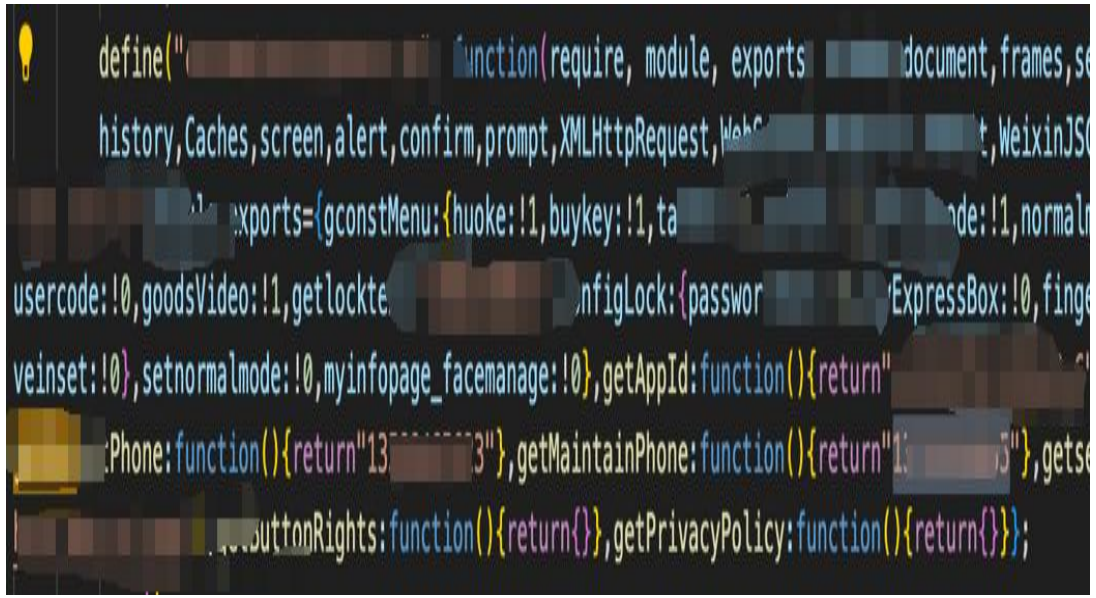
如果你只会这些，那你知道的还是太少了！

有想法的逻辑漏洞

PINGANSECURITYRESPONSECENTER

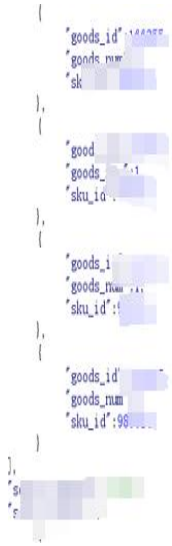
其实…它还有这些..这些...这些

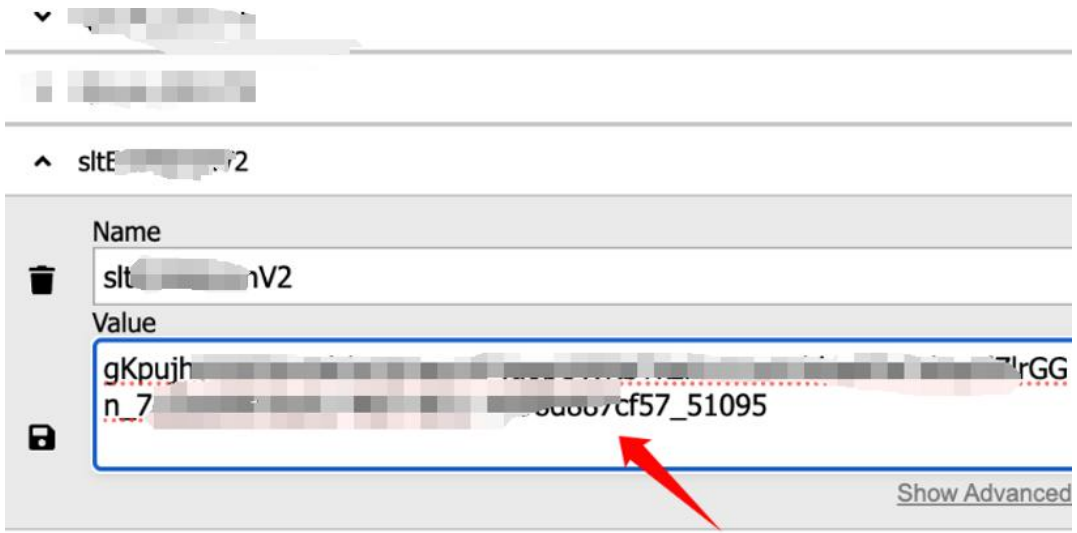

```
},
e.pr                    ubmitOrder = function (t) {
  return this.http.post('/' + e.SERVICE_NAME + '/directCustomer/submitOrder', t).then((function (e) {
    return e.data
  }))
},
e.SERVICE_NAME = 'api/                    redeem',
e
```



有想法的逻辑漏洞

PINGANSECURITYRESPONSECENTER





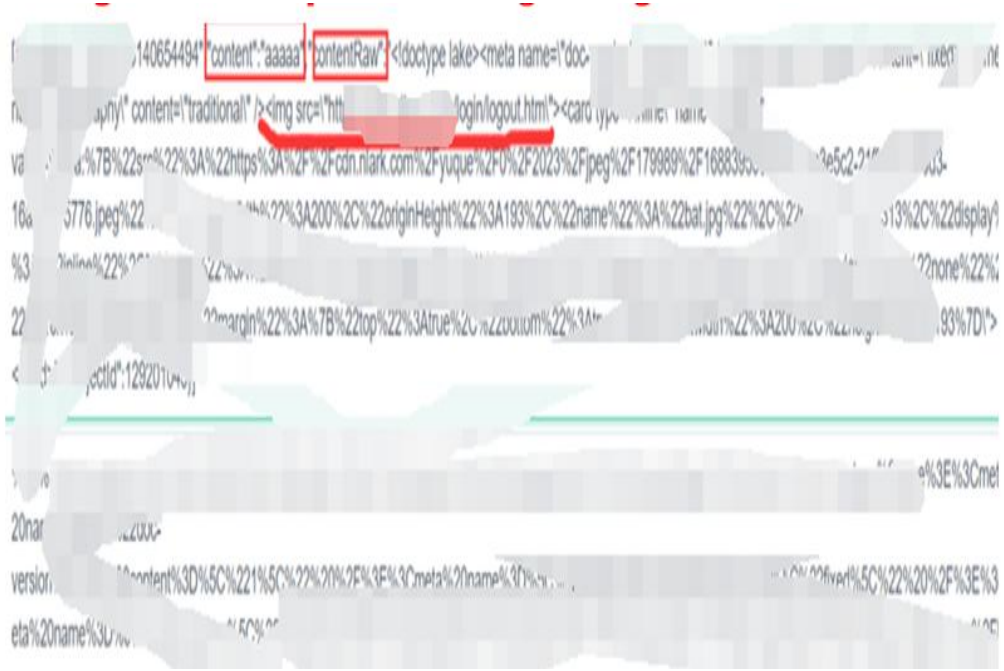
PART THREE

逻辑漏洞经典组合场景

案例一

PINGANSECURITYRESPONSECENTER

参数可控，导致网站瘫痪

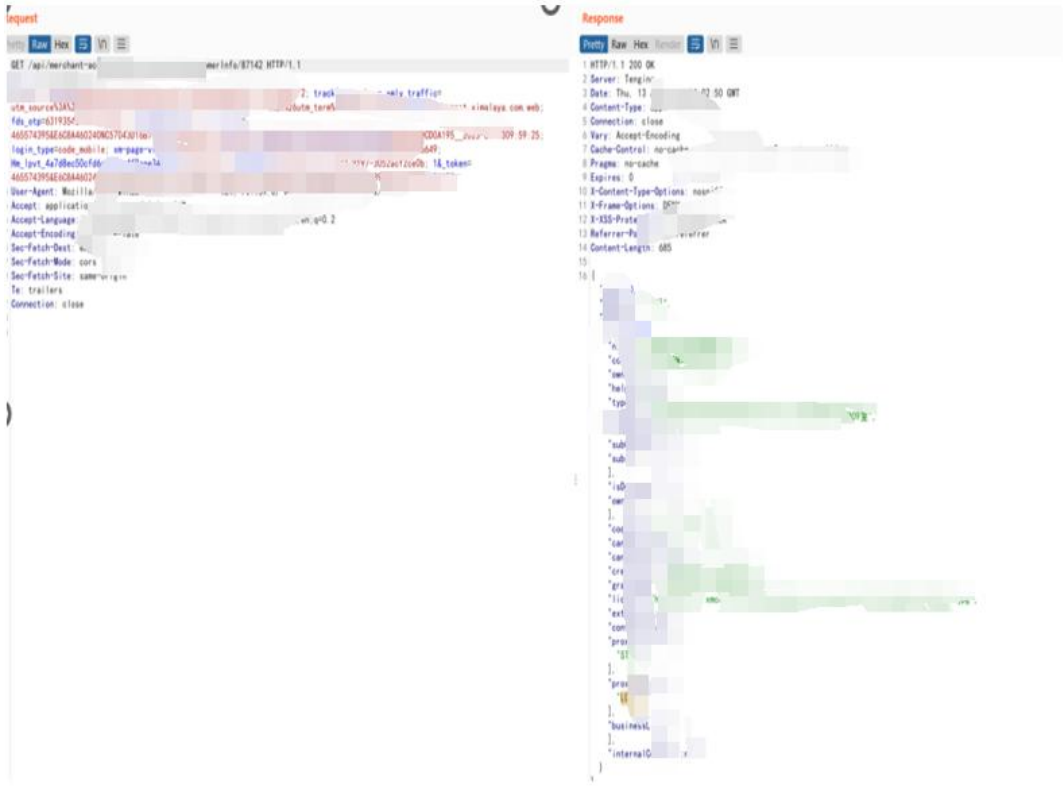


案例二

PINGANSECURITYRESPONSECENTER

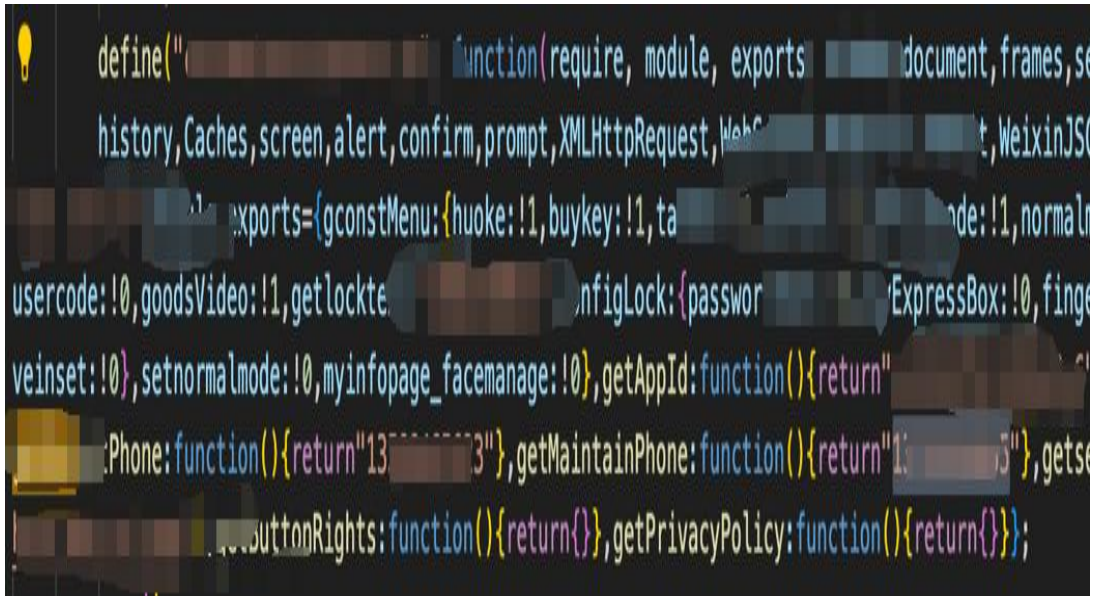
接口拼接，导致全站信息泄露

```
},
e.pr                                    ubmitOrder = function (t) {
  return this.http.post('/' + e.SERVICE_NAME + '/directCustomer/submitOrder', t).then((function (e) {
    return e.data
  }))
},
e.SERVICE_NAME = 'api/                              edeem',
e
```



案例三

PINGANSECURITYRESPONSECENTER



反编译，导致账号接管

案例四

PINGANSECURITYRESPONSECENTER

新人价，无限购买


```
{
    "goods_id":
    "goods_num
    "sk
},
{
    "good
    "goods_
    "sku_id
},
{
    "goods_i
    "goods_num
    "sku_id":
},
{
    "goods_id"
    "goods_num
    "sku_id":98
}
],
```

```
"is_border":0,
"is_all_self":1,
"order_list":[
    {
        "order_id":74315
        "order_id_str":
    },
    {
        "order_id":74315
        "order_id_str":
    },
    {
        "order_id":7431
        "order_id_str":
    },
    {
        "order_id":74
        "order_id_str":
    },
    {
        "order_id":7431548
        "order_id_str":
    }
],
```

案例五

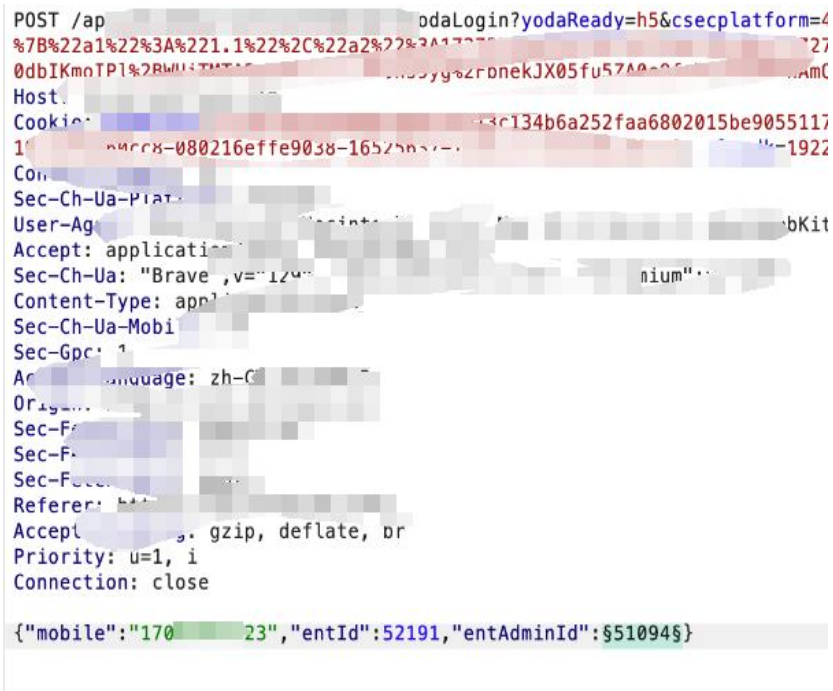
PINGANSECURITYRESPONSECENTER

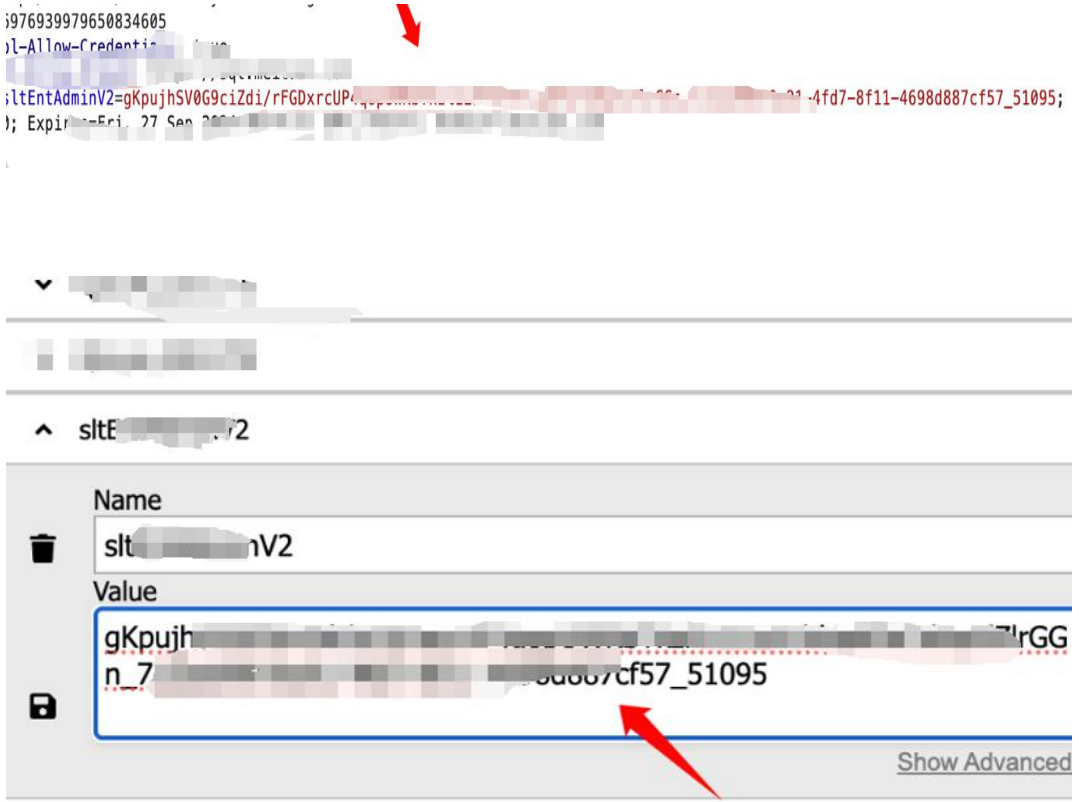
登陆口JS审计　　账号接管　　信息泄露

案例六

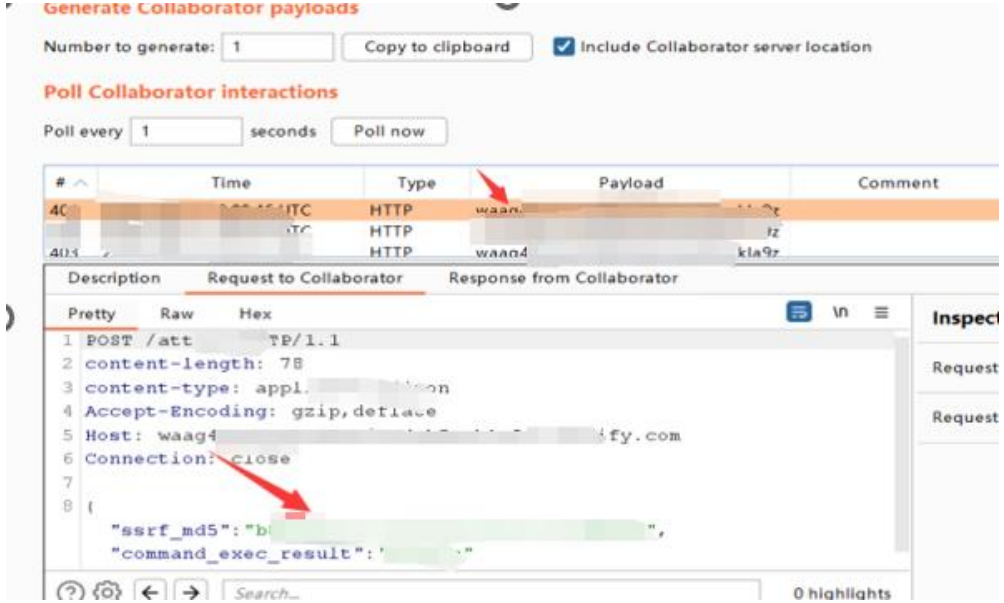
PINGANSECURITYRESPONSECENTER

组合拳泄露，导致账号接管





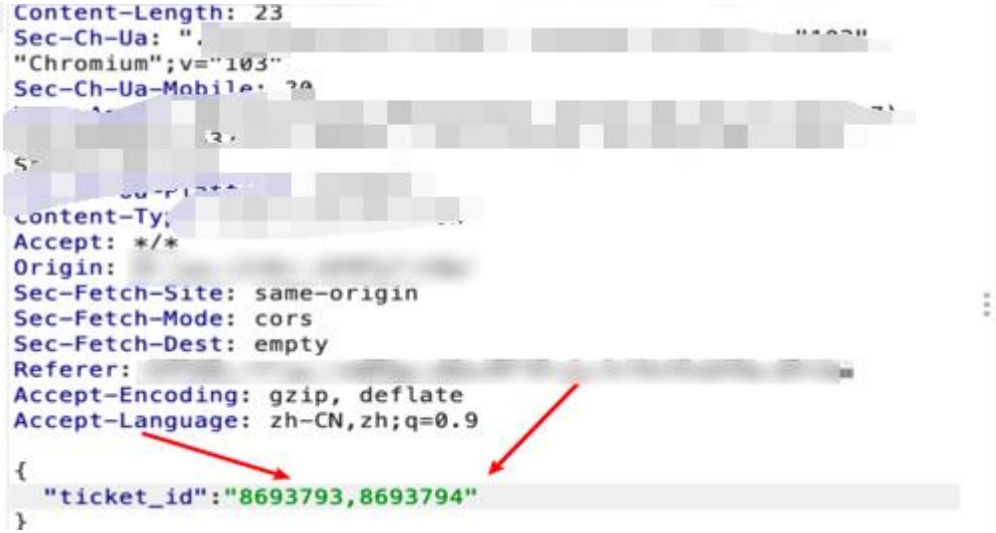
另类的SSRF，不要局限于某一功能点



PART ONE

实战场景中的一些tips分享

相当于更换了他的查询方式



逗号可以，分号也可以

感谢平安SRC应急响应中心 PINGANSECURITYRESPONSECENTER

祝愿平安SRC线上沙龙越办越好！！！

最后，祝所有的师傅日日出洞，洞洞严重

THANKS