Alibaba Security Response Center | CAINIAO 菜鸟·安全响应中心

我是如何挖掘物流行业安全漏洞的

- Adam
- 菜鸟SRC2018年度英雄榜TOP1

我是如何一个月挖到年度第一的

除了**运气**，主要是**有计划**和**时间充足**。

比如：我十几天时间发现某重要src 50个bug，拿到2000分。这足以说明有计划比错误的努力重要。

01

首先分析全国物流状况，再决定入手方式

- 在这之前我去沿海玩了十几天，当时就想我要拿菜鸟SRC TOP 10，没想到一个月后就冲到TOP 1。
- 冲榜思路：开工之前我对全国物流快递业务进行了大量调研和分析。分析规则，算是apt的前身吧，为接下来搞事儿做了一些心理上的准备。
- 漏洞成分比例：常见的漏洞类型基本上占80%。但是现金比例可能只有40%。当然这个都是看伤害的，伤害和比分成比例的，逻辑错误引起批量订单和个人信息泄露占比较高，一个普通人低成本都可以完成的完整攻击链获得的伤害完全不是几个高危可以比较的，这样的漏洞通常价值500以上。
- 本人技术真的很普通，不善于后渗透，但是什么都懂一点点，可能是和性格有关，比较执着。

02

模拟黑客和架构设计师视觉

- 从开发设计的角度。因为认识很多开发人员，所以了解他们所想。
- 敢于怀疑一切漏洞的存在，然后再去验证它。实际上真的很多应验了。这里不深入说明，因为目前我还在挖蚂蚁金服的。核心意思是从设计之初到现在系统最后成型的过程漏洞。
- 最重要的就是社工搜集问题，但不是指真的社工骗人。也不能用漏洞去骗人，要以最普通的平民百姓的权限的角度去刺探业务，过程中就会获取可观的敏感信息。

03

冲榜成功的主要原因

1. 大量弱口令。现在很少了，但是应该还是有弱口令的。
2. 挖掘物流快递行业安全漏洞的白帽子可能不多。
3. 运气比较好，运气是我一直拥有的。
4. 挖掘思路不按常理出牌。侧向或者apt方式等。

备注：由此从测试结果看来，以后想拿高分的话，一部分侧重点是一个攻击链，或者情报、命令执行。如果你能证明一个低成本的攻击链，可能会给很高分

04

资产收集

- 资产收集主要是bing和百度的site和domain语法，当然次要还用了次要的sublist3r和layer。因为找到次要的域名也不值钱，我都是搞核心站点。
- 分析业务链，这个才是漏洞最多的问题。最少30%高危漏洞是从分析业务链上面得到的，根本都没开始挖洞。这个方式就看你们自己能想象到什么了。我比喻结果了，分析exe里面的http请求，apk等配置文件，甚至看新闻什么的。此处漏洞存在于想象力。
- 不建议社工，确实一个严重的sso系统漏洞是社工引起的，通过社工我得到了80个左右不同域名后台的权限。
- 分析js，构造js里面api的url。主要看两个js，appjs和核心逻辑的js。

05

弱口令方法

- 当时基本上每天都能弄到几个弱口令后台。因为太多系统搞不过来。每个系统随便搞几个就提交了。甚至一个系统打包一个然后提交了。或许我想法不太一样，大部分人把弱口令心思放密码上面，我心思完全在账号上。
- 可以爆破，分为：没验证码的情况。和验证码有效，但是通过拦截数据包的情况下爆破有效。
- 不可以爆破的，手动爆破，偶尔这样盯着干。这种情况也有几个案例，比如一个官网客服系统所有的密码都是111111，只要手工尝试成功账号就可以了。

06

可以爆破弱口令的手段

- 固定一个特定密码去爆破账号，比如123456。先爆破自己准备的500个top账号。再Fuzzer账号规则。结果大致有以下几种比如Adam+123类似的，比如Adamsto123456 。比如纯数字4-8位的账号，比如三段码，四段码就是地区形势的。
- Fuzz出来了账号规则在爆破密码。只准备了10几个以内的弱密码，为了提高效率是越少越好。然后账号可以每一个字符指定类容，让中的爆破尽量10000次以内。我都是控制5000次的。然后搞的站很多，所以收获量很乐观。
- 拦截爆破。当时很多系统都没验证码，或者说有验证码真实有效，但是burp拦截状态无效。

物流行业常见的弱口令

111111
123456
888888
666666
admin123
abc123
012345
a123456
a1234567
123456789
654321
111222
001122
admin@123
……

07

漏洞存在于坚持和运气

- 说这个的原因主要是想告诉大家不要轻易放弃。
- 有人认为漏洞参数可能有很多可以容易理解的逻辑，但是在我眼里只看结果。比如你xss域名A但是你却得到了域名B的后台登陆权限，B域名是我真的想搞的，A域名是我修改fuzz出来的，估计此生一例吧。
- 比如一个秘密账号都错误的情况，爆破1分钟后数据包展示的响应包每一个都是错误的没成功的，普通人可能就关闭浏览器或者不管了，但是你刷新一下网页，可能你就cookie有效了。
- 甚至多个src我都遇到了这个问题：动工dos，低速度打开web某个路径是绝对的403或者500。但是你以最快速的手动刷新页面3-5次，结果你会发现后台可以查询数据，而且是可以查询数据库交互那种。

08

我在物流快递行业的战绩

190个漏洞审核通过

序号	状态	漏洞编号	漏洞名称	类型	提交时间	安全币
1	已修复	CNSRC-180910-823	【双11众测】[redacted]	web安全漏洞	2018-09-10 10:14:22	280
2	已修复	CNSRC-180910-769	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:30:11	30
3	已驳回	CNSRC-180910-766	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:28:41	0
4	已驳回	CNSRC-180910-764	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:27:06	0
5	已修复	CNSRC-180910-761	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:23:25	116
6	已修复	CNSRC-180910-756	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:20:57	116
7	已修复	CNSRC-180910-752	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:17:56	120
8	已驳回	CNSRC-180910-746	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:15:01	0
9	已修复	CNSRC-180910-742	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:13:03	90
10	已修复	CNSRC-180910-736	【双11众测】[redacted]	web安全漏洞	2018-09-10 00:10:44	120

Demo1 物流A公司sso系统

为了尽快熟悉该公司业务，各种合法手段都尽量试一试。通过新闻消息信息收集到了一个物流的exe，其实是核心sso的网点客户端。但是网点应用程序名字和物流名字毫无关联。通过这个exe搞到多个高危漏洞。漏洞有：

1. 网点资料都集成到了exe里面，包括各种账号规则，甚至有相关系统的弱口令也直接写进去了。（当然肯定是通过这个弱口令进入了大量的相关域名后台）
2. api接口未授权查询。也就是说查询数据不需要会话认证。
3. 命令读取，可以读取服务器所有文件。
4. 逆向exe源码发现，程序都没做任何敏感信息加密的，没做各种防御xss或者防止注入的手段。想想这如果是被外国黑客搞到，后果估计是泄露数据直接是亿级别了。
5. 当然这个物流的好几个sso系统我是拿到了后台登陆权限的。

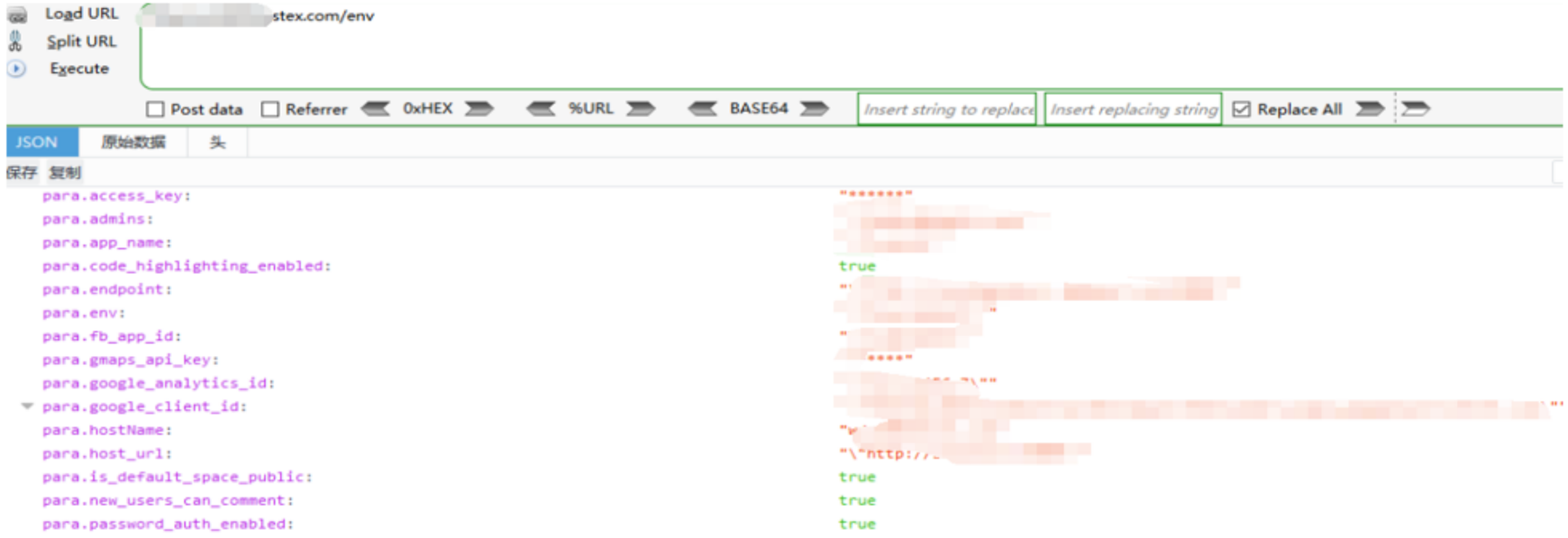
Demo2 物流B公司sso系统

多因子认证、密码账号+短信验证码，正面攻击无懈可击。

绝大多数人可能就放弃了，这个系统我也拿到了登录权限。

Demo3 物流C公司sso系统spring泄露

- autoconfig beans configprops dump env health info metrics mappings shutdown trace 等等路径导致信息泄露。
- Trace 泄露uri接口，导致url未授权可越权查询数据库



Demo4 物流公司sso系统sql注入

- 因为即使拿到了框架url可以未授权查询框架东西，可是有注入。

```
erience any problems during data retrieval
GET parameter 'type' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 243 HTTP(s) requests:
---
Parameter: type (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: page=1&limit=10&type=-6270' OR 1141=1141 AND 'Njde' LIKE 'Njde

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: page=1&limit=10&type=777' OR SLEEP(5) AND 'THnn' LIKE 'THnn

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: page=1&limit=10&type=777' UNION ALL SELECT 86,86,CONCAT(0x716a706a71,0x474c4d75634a53556c784f4a77697
4b42706785776650b0677a79727157 4f624d787a4c76,0x7171767171),86,86,86-- DnEN
---
[21:49:19] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[21:49:19] [INFO] the back-end DBMS is MySQL
web application technology:
back-end DBMS: MySQL
[21:49:19] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 103 times
```

```
[21:52:32] [INFO] fetching tables for database
[21:52:32] [INFO] used SQL query returns 11 entries
[21:52:32] [INFO] starting 2 threads
[21:52:32] [INFO] resumed: department
[21:52:32] [INFO] resumed: department_copy
[21:52:32] [INFO] resumed: ge_answer_banner
[21:52:32] [INFO] resumed: ge_answer_check
[21:52:32] [INFO] resumed: ge_answer_menu
[21:52:32] [INFO] resumed: ge_answer_modify
[21:52:32] [INFO] resumed: login_verify
[21:52:32] [INFO] resumed: news
[21:52:32] [INFO] resumed: para
[21:52:32] [INFO] resumed: para_scoold
[21:52:32] [INFO] resumed: user_file
Database:
+-------------------+---------+
| Table             | Entries |
+-------------------+---------+
| para_scoold       | 44403   |
| user_file         | 6197    |
| news              | 3935    |
| ge_answer_modify  | 835     |
| ge_answer_menu    | 818     |
```

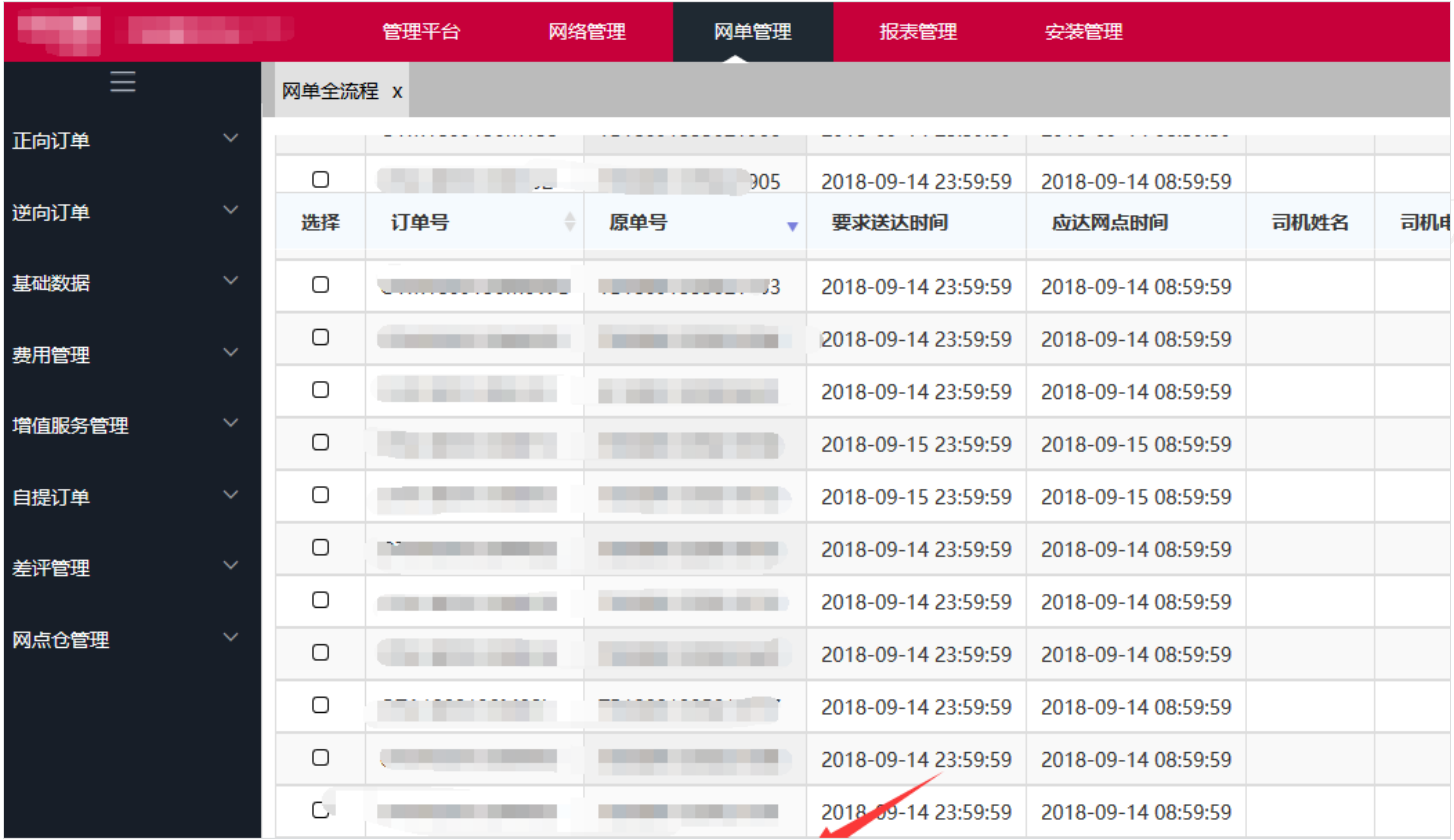
Demo4 双11活动某后台权限严重漏洞

- 给严重是因为进入了系统，海量个人未加密信息。唯一有点小失落的是这个系统无数越权，只给我认了一个，因为是同类型的。其实很满足了。
- 这个漏洞很有趣的原因是爆破无效，正面无懈可击，我就喜欢动歪脑筋。我尝试看看有没相关域名，或者旧系统，因为接触的系统多了就懂了一些套路吧。然后真让我发现了一个旧系统aaa.bb.com和aaax.bb.com相差一个字符。
- 但是aaa.bb.com也是无法正面的。但是好处是现在这个aaax.bb.com系统居然可以注册了!!!!!!!!!

Demo4 旁站&旧站XSS到后台登录

- 于是晚上2点多的我也突然来兴致盎然，x肯定要x了aaa1.bb.com十几个payload以后，第二天就收到了一大堆aaa.bb.com的后台。

- 结果是值得开心的。他们的居然是明文账号密码保存在cookies的结果不用说了。。
- 因为这只是普通后台，不需要短信验证，所以密码账号直接登录了



[redacted]

选择	订单号	原单号	要求送达时间	应达网点时间	司机姓名	司机
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-15 23:59:59	2018-09-15 08:59:59		
☐	[redacted]	[redacted]	2018-09-15 23:59:59	2018-09-15 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		
☐	[redacted]	[redacted]	2018-09-14 23:59:59	2018-09-14 08:59:59		

Alibaba Security Response Center | CAINIAO 菜鸟·安全响应中心

THANKS !

QQ : 1073450832