



WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情

Let's Do Something Cool!

WIFI 万能钥匙 SRC 安全沙龙
成都 2017/12/02



WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情

Let's Do Something Cool!

《SRC混子是如何炼成的？》

四叶草安全 - 残废



SRC到底应该怎么搞？



来自漏洞之王的回复

师傅好



请问如何才能像你一样，变成漏洞之王？



多想多找，想法越出其不意越好，多熟悉业务



来自月入几十万的大佬回复

黑色键盘



大佬



请问如何才能变成像你一样月入几十万的大神?



下午12:19



对他们的那些业务比较了解 信息搜集的全一点 正好那个月他们活动 每天都挖 因为他们分几个阶段 还有个最终大奖。如果第一阶段拿到奖 我就把漏洞都囤着 等第二阶段提交 以此类推 这样每个阶段都拿到了奖 时间点掐的准 这样一结合完美



又一个来自月入几十万的大佬回复

hackbar



请问大佬如何才能做到像你一样挖SRC漏洞就能月入30余万呢?



让我细细道来



1、系统化挖掘:

就是对目标厂商信息进行全面的信息收集, 不仅仅局限于二级域名、三级域名, 还要深入收集这些域名下的服务信息, 如web服务、APP、微信公众号、小程序等。

2、明确业务数据:

要明确目标厂商主要是做什么的, 业务会产生哪些数据, 这些数据又分布在哪些应用及对应功能里面, 对应功能下的API又是怎么调取相关数据的

3、细致到位:

就是细心, 对自己所测试的每一个业务, 都得仔细到位。特别是一些校验、授权等敏感接口

好的 感谢大佬的分享



祝大佬月月漏洞盆满钵盈





信息收集？
了解业务？



从基础架构分析

运维安全

业务安全

应用安全

内部安全



Web Server

基础服务

应用层

运维安全

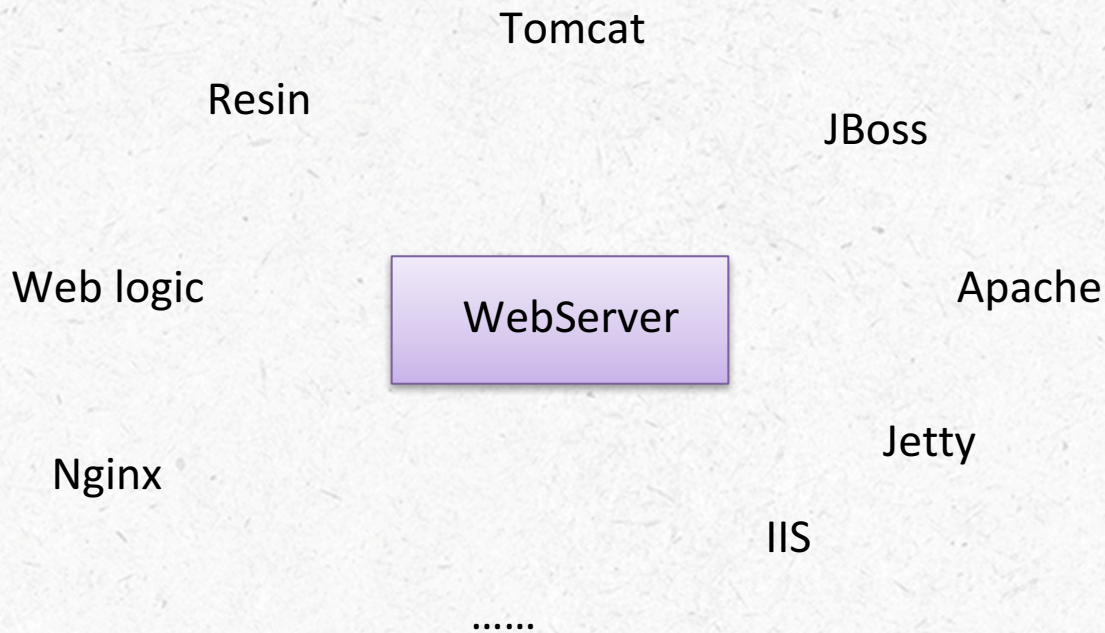
网络

信息泄露

服务器&设备









备份文件泄露

压缩文件泄露

敏感文件泄露

编辑器安全

Strut2

应用层

SVN

Git

cati

jenkins

zabbix

.....



截图泄露

操作手册

代码泄露

PPT

信息泄露

内部帐号外部业务

Blog

.....



营销活动

账号体系

业务安全

交易体系

风控体系



密码重置

批量注册

登陆防控

撞库

账户体系

任意登录

身份鉴定

任意注册

身份盗用



风控缺陷

风控遗漏

风险控制

判定要素

机器识别





任意金额充值

一分钱续费

交易体系

一分钱充值

一分钱购物



绕不完的Filter

SSRF

失效的“云WAF”

推不动的SDL

应用安全

事件响应不及时

漏洞组合利用



人员意识

内部安全

办公网络



chr

#####

1、通过跳板机器登录 腾讯跳板服务器

用户名 IP 密码

ubuntu 182 DE

#####

2、第一次需要操作

通过命令行修改自己的密码

password 用户名

用户名为自己的邮箱地址

例:

初始密码均为:

例:

password caoxh

New password: (输入新密码)

Re-enter new password: (输入新密码)

Enter LDAP Password: (输入初始密码)

```

root@171-143-133-ubuntu:~# cat /etc/hosts
127.0.0.1   glee-102-254-140-133  171-146-133-ubuntu

10.131.159.144 openldap
10.143.54.230 saltstack
10.166.19.41 syslog

#come from web id
10.127.152.134 hongbao1.php
10.147.79.175 es2.base
10.143.54.188 es1.base

ubuntu@fabu1:~$ cat /etc/hosts
127.0.0.1   fabu fabu1.transfer localhost
10.147.62.204 fabu.php
10.147.79.230 saltstack
10.166.52.151 bi
10.166.24.15 test03
115.159.23.53 test02
115.159.48.49 test01
    
```

```

10.181.24.206   web2   web2.php
10.137.146.148 web3   web1.php
10.167.59.169  web4   web4.php
10.105.52.9    web5   web1.php
10.167.00.103  wxwadmin3 wxwadmin3.php
10.137.145.115 wxwadmin4 wxwadmin4.php
10.127.132.134 hongbao1 hongbao1.php
10.137.134.93  hongbao4 hongbao4.php
10.137.134.213 hongbao5 hongbao5.php
10.147.48.136  oaurhl oaurhl.php
10.143.14.60   oaurhl4 oaurhl4.php
10.105.42.253  weixin1 weixin1.php
10.137.135.111 weixin4 weixin4.php
10.145.31.201  swanle3 swanle3.php
    
```

```

Nm4P3rY#5n' port => 3306)
    
```

立即查看使用教程，玩转腾讯云！

```

ubuntu@salt-master: /data/saltstack/ldap/ldap$ ifconfig
ubuntu@salt-master: /data/saltstack/ldap/ldap$ ifconfig
ubuntu@salt-master: /data/saltstack/ldap/ldap$ ifconfig
Please give me username and group that want to add to ldap
temp: /data/saltstack/ldap/ldap$ ./getldapinfo
yuyi:20009 linjiao caoxh
sl:admin:20001
rm:pinxian:20002
pn:pinxian:20003
de:005 cany:20004
de:ment:20006
de:by:20007
re:ar:20008
de:20009 linjiao
cp:zu:20010
de:liby:20011
de:liby:20012
ubuntu@salt-master: /data/saltstack/ldap/ldap$ ./getldapinfo
Add new User to this Group yunwei
adding new entry "ou=tech,dc=com,dc=com"
ubuntu@salt-master: /data/saltstack/ldap/ldap$ ./getldapinfo
yuyi:20009 linjiao caoxh
sl:admin:20001
rm:pinxian:20002
pn:pinxian:20003
de:005 cany:20004
de:ment:20006
de:by:20007
re:ar:20008
de:20009 linjiao
cp:zu:20010
de:liby:20011
de:liby:20012
ubuntu@salt-master: /data/saltstack/ldap/ldap$ cat tempu.ldif
dn: ou=tech,dc=com,dc=com
cn: tech
objectclass: ou
    
```



信息收集

- User List → username password mobile mail 角色
- Domain List → 二级、三级... 备案 whois 第三方 业务资产
- IP List → 外网IP 内网IP C段 IP 办公网IP 端口
- Web List → 中间件 CMS 数据库 基础服务
- Mail List → user mail 业务mail 公用mail
- work os → oa gitlab jenkins wiki Jira VPN SSO 后台



了解业务

业务内容

业务资产

业务应用



边缘资产比核心更容易出问题



WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情

Let's Do Something Cool!

安全总是相对的



WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情

Let's Do Something Cool!

三分看命运，七分天注定



WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

Thanks