唯品会 vip.com

唯品会安全应急响应中心
VIP Security Response Center

2016唯品会互联网电商安全峰会

电商安全的闭环

电商安全体系建设的血与泪

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

轻松玩转“互联网+”漏洞

四叶草安全
CloverSec Labs

Rabit2013

About Me

[Rabit2013@CloverSec]:~# whoami
ID： Rabit2013，Real name： 朱利军
[Rabit2013@CloverSec]:~# groupinfo
Job : CSO & CloverSec Labs & Sec Lover
[Rabit2013@CloverSec]:~# cat Rabit2013_Info.txt

- 西电研究生毕业（信息对抗、网络安全专业）
- 历届XDCTF组织与参与者
- 多届SSCTF网络攻防比赛组织与出题
- 某国企行业网络渗透评估
- 嵌入式漏洞挖掘挑战赛5个高危漏洞
- 通用Web应用系统漏洞挖掘若干
- 某国企单位安全培训
- ……

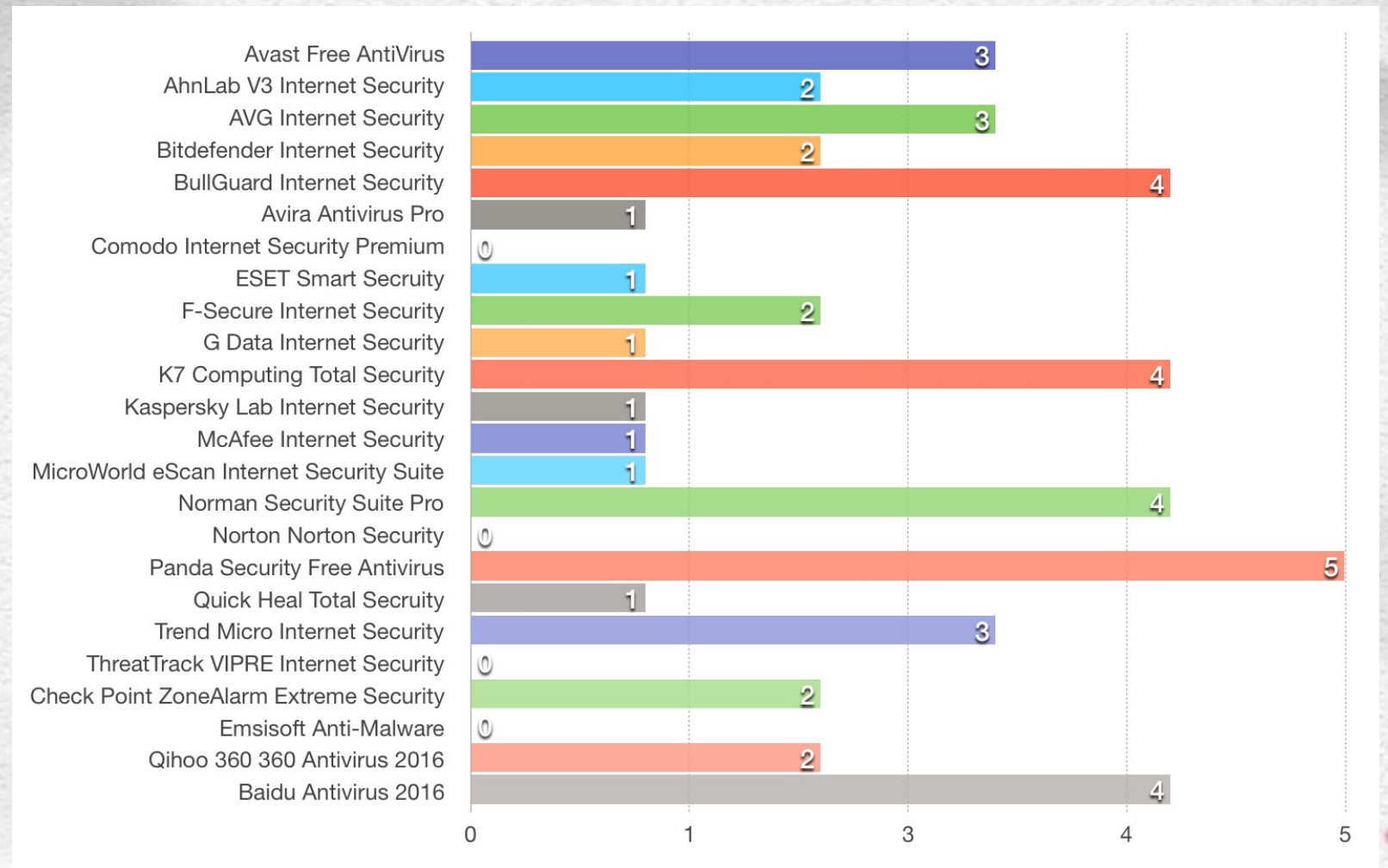
About Labs


四叶草安全实验室
二进制漏洞挖掘
Java&Flash
安全防御软件
主流浏览器
其他
操作系统
Web漏洞研究
主流Web应用
主流Web框架
主流中间件
其他
移动终端漏洞研究
Andriod&iOS及其他APP
移动智能设备
IOT/工控安全研究
其他
智慧城市
车联网
物联网

About Labs

- 发现多个Microsoft Windows内核提权漏洞（**CVE-2016-0095**）
- 发现多个Adobe Flash Player任意代码执行漏洞（**CVE-2015-7633，CVE-2015-8418，CVE-2016-1012，CVE-2016-4121**）
- 发现多个Oracle Java任意代码执行漏洞（**CVE-2016-3422，CVE-2016-3443**）
- 发现全球25款杀毒软件47个本地提权漏洞
- 发现多个360安全卫士内核提权漏洞（**QTA-2016-028**）
- 发现多个百度杀毒内核提权漏洞
- 率先发现苹果AirPlay协议认证漏洞
- 参加互联网嵌入式漏洞挖掘比赛，对某知名厂商提供的设备进行漏洞挖掘，提交了5个高危漏洞
- 为TSRC、AFSRC提交漏洞若干

About Labs


Avast Free AntiVirus 3
AhnLab V3 Internet Security 2
AVG Internet Security 3
Bitdefender Internet Security 2
BullGuard Internet Security 4
Avira Antivirus Pro 1
Comodo Internet Security Premium 0
ESET Smart Secruity 1
F-Secure Internet Security 2
G Data Internet Security 1
K7 Computing Total Security 4
Kaspersky Lab Internet Security 1
McAfee Internet Security 1
MicroWorld eScan Internet Security Suite 1
Norman Security Suite Pro 4
Norton Norton Security 0
Panda Security Free Antivirus 5
Quick Heal Total Secruity 1
Trend Micro Internet Security 3
ThreatTrack VIPRE Internet Security 0
Check Point ZoneAlarm Extreme Security 2
Emsisoft Anti-Malware 0
Qihoo 360 360 Antivirus 2016 2
Baidu Antivirus 2016 4
0
1
3
4
5

目录

- 何为“互联网+”？
- 存在哪些安全风险？
- 如何玩转“互联网+”的漏洞？
- 如何“玩”得更高大上？

CloverSec Labs

唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

CloverSec Labs

互联网+

无线路由	防御软件	工业系统	
摄像头	联网汽车	智能家居	
云办公	云WAF	智能手表	.....
运维系统	智能网关	监控系统	
Web应用	各类CMS	各类OA	

一切可以联网的系统

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

CloverSec Labs

漏洞

传统漏洞

新型漏洞

CloverSec Labs

传统漏洞

CloverSec Labs

新型漏洞

CloverSec Labs

归根结底

- 系统本身
  - 系统输入
  - 系统逻辑
- 数据传输
  - 安全传输
  - 协议安全

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

CloverSec Labs

怎么Start

白盒审计

黑盒测试

灰盒审计

CloverSec Labs

代码检查法、静态结构分析法、静态质量度量法、逻辑覆盖法、基本路径测试法、域测试、符号测试、路径覆盖、程序变异和动态调试法。

初次见面 → 深入分析 → 漏洞利用

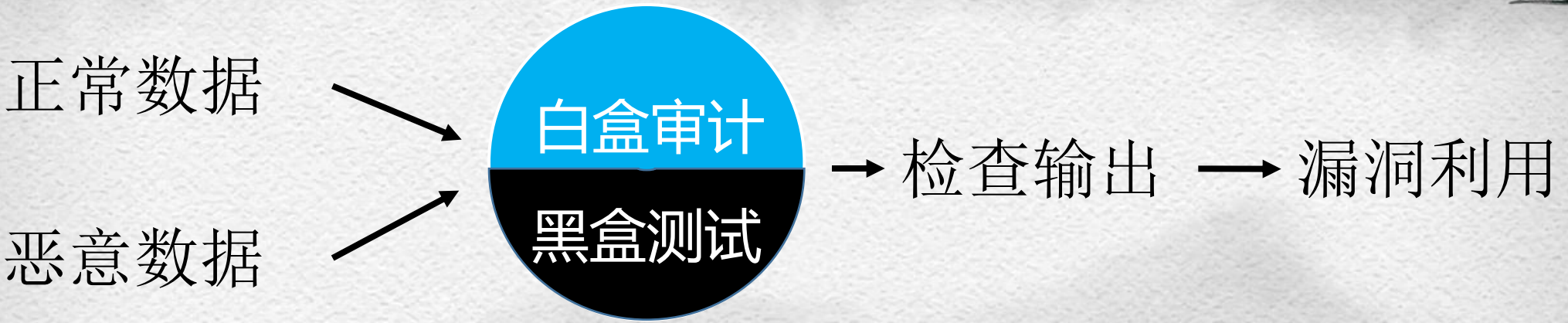
白盒审计

CloverSec Labs

黑盒测试中Fuzz测试，也叫做“模糊测试”，是一种挖掘软件安全漏洞、检测软件健壮性的黑盒测试，它通过向软件输入非法的字段，观测被测试软件是否异常而实现。

黑盒测试

CloverSec Labs



如何开始玩？

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

CloverSec Labs

“玩”什么？

唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

CloverSec Labs

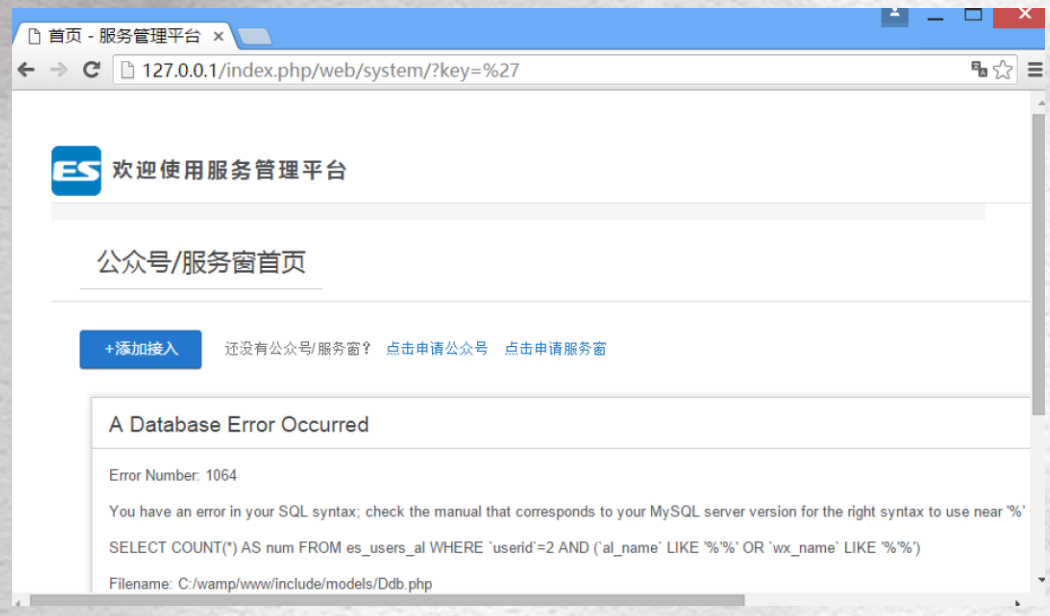
案例

安全防御设备

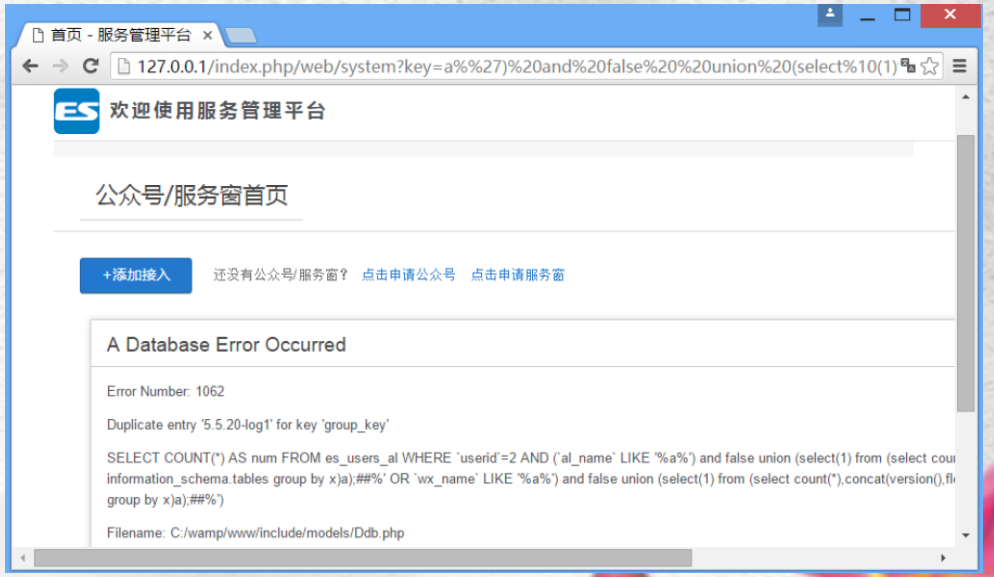
Web系统 | 路由器 | 智能设备

工控设备 | 网络摄像头 | 监控设备

Web应用漏洞挖掘

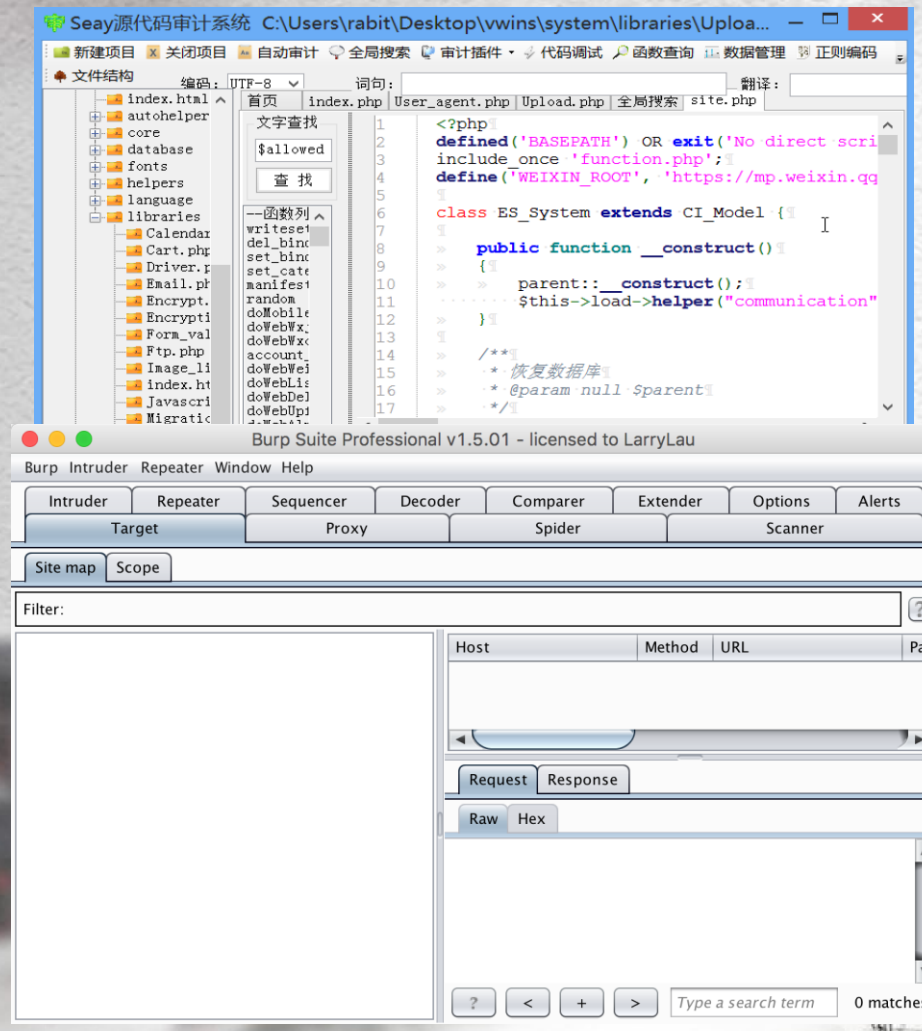


- 网站业务
- 前台后台
- 初次检查各类输入点



- 初次漏洞探测
- 异常监测
- 定位漏洞
- 构造Payload

Web应用漏洞挖掘



- 系统业务熟悉
- 根据业务熟悉代码框架
- 漏洞定位与测试

```
$tname = value($parent, 2, false, 'images');    //类型: images/vi
$fname = value($parent, 3);                     //文件命名
$allowed = value($_GET, 'allowed');             //格式限制
$size = intval(value($_GET, 'size'));           //大小限制KB
$userid = intval(value($_GET, 'userid'));       //用户ID
if (empty($userid)) $userid = $user['userid'];
$arr = array();
$tname = in_array($tname, array('images','audio','voices','video
$arr['upload_path'] = FCPATH."uploadfiles/users/".$userid."/".$t
if ($tname == 'audio' || $tname == 'voices') {
    $arr['allowed_types'] = 'mp3|wma|wav|amr';
}elseif ($tname == 'videos'){
    $arr['allowed_types'] = 'rm|rmvb|wmv|avi|mpg|mpeg|mp4';
}else{
    $arr['allowed_types'] = 'gif|jpg|jpeg|png';
}
if ($allowed && $allowed != "undefined") {
    $arr['allowed_types'] = $allowed;
}
$arr['file_name'] = ($fname)?$fname:SYS_TIME.rand(10,99);
if ($size > 0) {
    $arr['max_size'] = $size;
}
```

Web应用漏洞挖掘

- 业务逻辑熟悉
- 黑盒测试
- 检测测试异常
- 定位漏洞

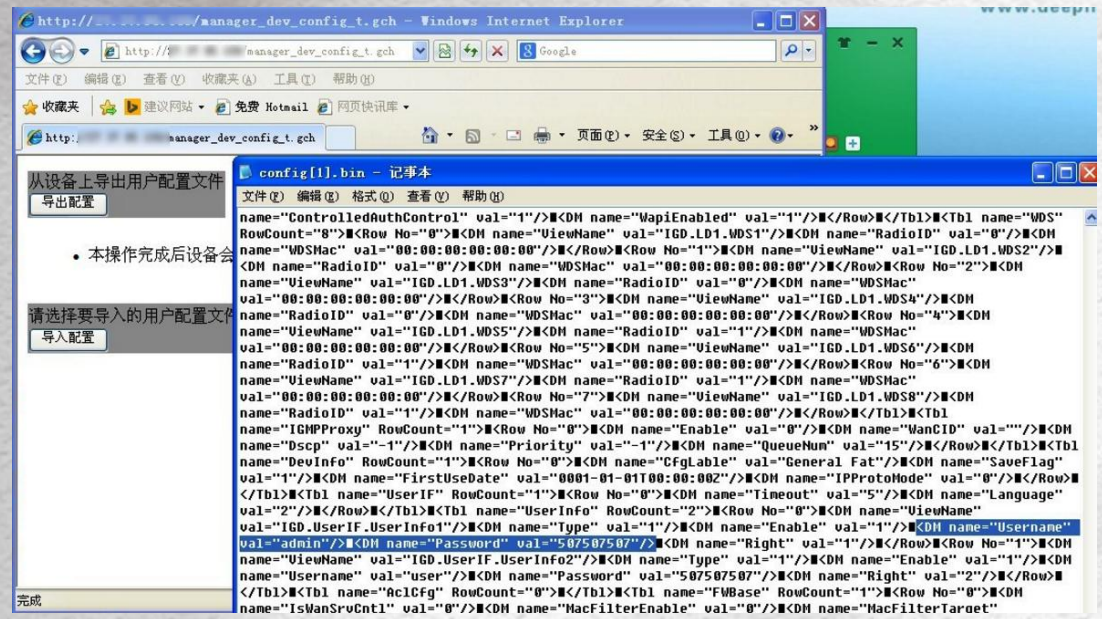
涉及13家厂商中17个设备

天玥网络安全审计系统
Netoray NSG 上网行为管理系统
Netoray SMB 企业易网通
Netoray NSG 上网行为管理系统
Netoray TOG 莱克斯带宽管理系统 V5.0
网神信息技术（北京）股份有限公司
poweraegis 5500 上网行为管理系统
InforCube NSG 上讯上网行为管理系统
神州数码上网行为管理系统
VOLANS SR上网行为审计网关
瑞星上网行为管理系统
网御上网行为管理系统 Leadsec ACM
网睿兴安日志系统
艺创专业上网行为管理设备 e-strong ibm

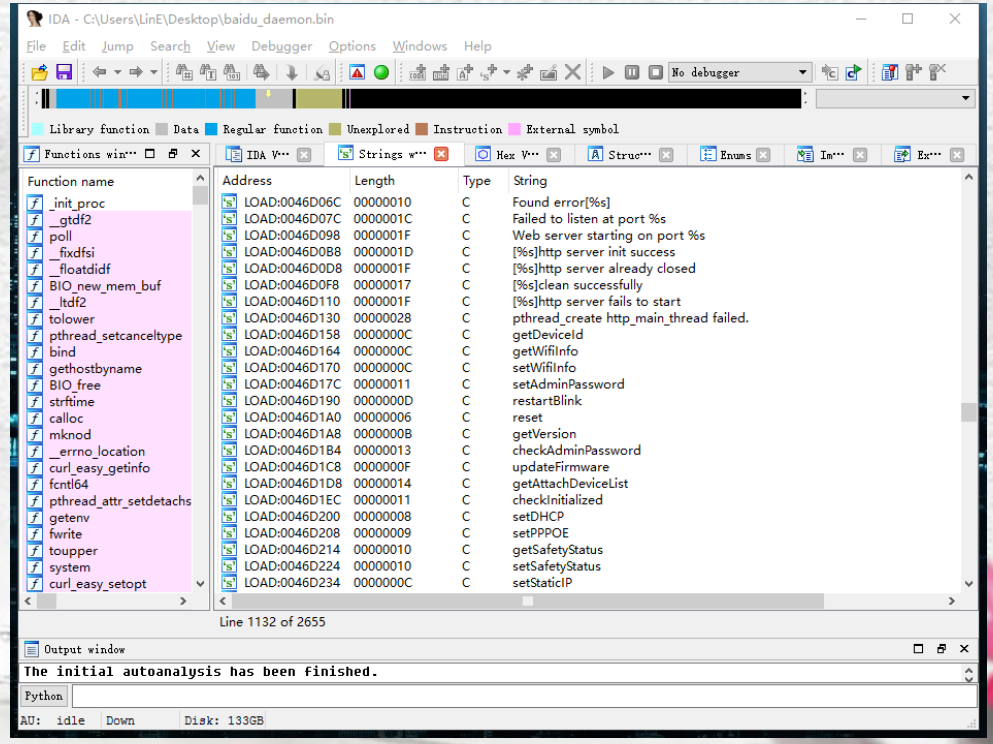
```
payload = "recovery_passwd.cgi?act=2&username=111%27%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(5)))HcCu)%20AND%20%27zMcG%27=%27zMcG&usermail=1111@qq.com&ajax_rnd=716299799539486470000&user_name=undefined&session_id=undefined&lang=undefined"
```

唯品会安全应急响应中心
VIP Security Response Center

路由器漏洞挖掘



- 路由器业务了解
- 相关开放信息收集
- 检查开放接口

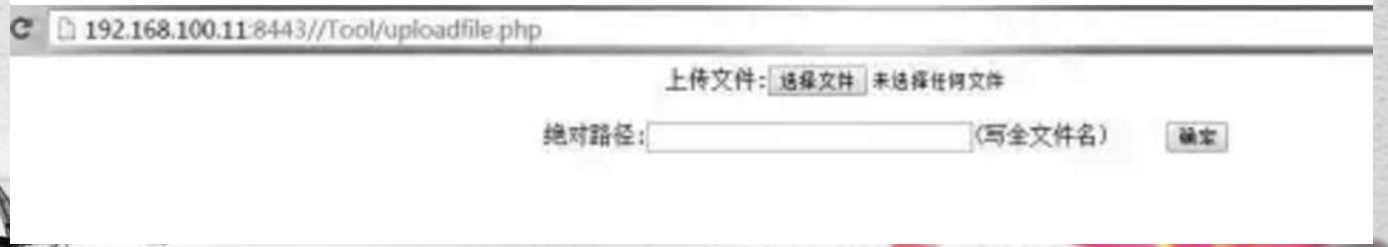


- 拆硬件
- 固件Dump分析
- 定位各类业务逻辑
- 分析利用漏洞

路由器漏洞挖掘

- 业务功能了解
- 功能逻辑的了解
- 黑盒漏洞测试
- 相关弱点利用

任意文件上传的位置/Tool/uploadfile.php,



智能联网设备漏洞挖掘

- 业务功能了解
- 网络通信数据跟踪
- 云端认证漏洞挖掘
- 相关弱点利用

- 固件Dump
- 固件逆向分析
- 定位漏洞
- 构造Payload

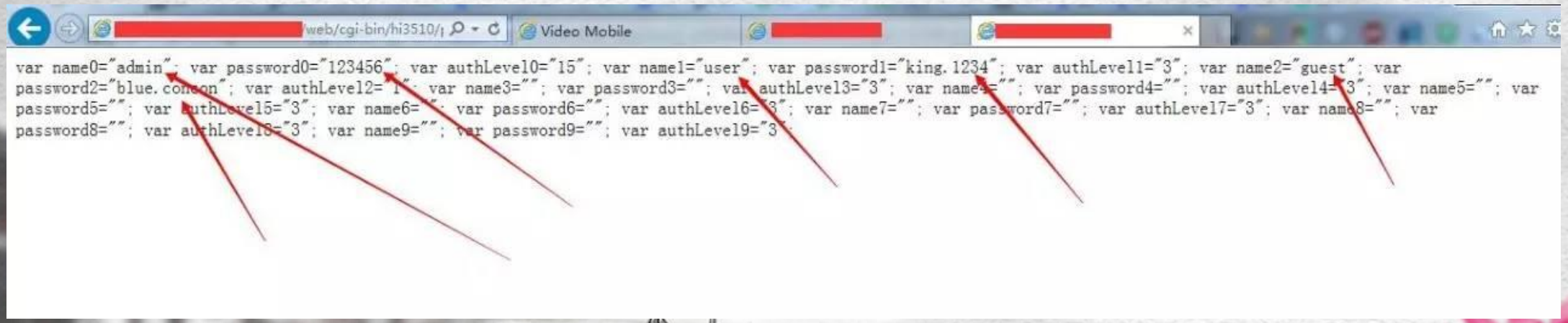
```
Environment size: 665/65532 bytes
ar7240> md 80060000 64
80060000: 8e030000 24422000 54e20007 8e020000    ....$B .T.......
80060010: 02002821 0c017a68 02203021 54400014    ..(!..zh. 0!T@..
80060020: 00001021 8e020000 3c068000 3c03802b    ...!....<...<..+
80060030: 7e244b00 00461021 8c65dfa0 00042080    ~$K..F.!.e.... .
80060040: 00021302 26430040 00021140 ae630000    ....&C.@...@.c..
80060050: 00a21021 00451027 00021143 00021300    ...!.E.'...C....
80060060: 00461021 0801801c 00441021 00001021    .F.!.....D.!...!
80060070: 8fbf0024 8fb30020 8fb2001c 8fb10018    ...$... ........
80060080: 8fb00014 03e00008 27bd0028 23bdffd0    ........ ...(#...
80060090: afb30028 00e09821 afb10020 00c08821    ...(...!... ...!
800600a0: afb0001c 00a08021 afbf002c afb20024    ........!...,...$
800600b0: 8cc20010 8c920000 30420001 1440003b    ........0B...@.;
800600c0: 2404ffea 3c02802a 244307e0 90620039    $...<..*$C...b.9
800600d0: 30420004 14400005 00000000 9062002d    0B...@.......b.-
800600e0: 30420008 14400004 27a60010 0c003be4    0B...@.. ....;.
800600f0: 02202021 27a60010 02002821 0c017ff1    .  !'.....(!....
80060100: 02402021 0404fff4 10400028 00408021    .@ !.....@.(.@.!
80060110: 88420000 2403ffbf 00411024 14400023    .B..$....A.$.@.#
80060120: 2404fff0 8e220000 30428000 10000002    $....".. 0B......
80060130: 02201821 8e23000c 24620004 c0430000    . .!.#..$b...C..
80060140: 24630001 e0430000 10600213 00000000    $c...C...`......
80060150: 8e420048 02202021 24420001 0c019765    .B.H.  !$B.....e
80060160: ae420048 3c02802b 8c42dfa0 02220023    .B.H<..+.B..."."#
80060170: 00021143 00021300 00531025 30430040    ...C.....S.%0C.@
80060180: 10600009 aa020000 3a040004 2406ffbf    .`......:...$...
ar7240>
```

工控设备漏洞挖掘

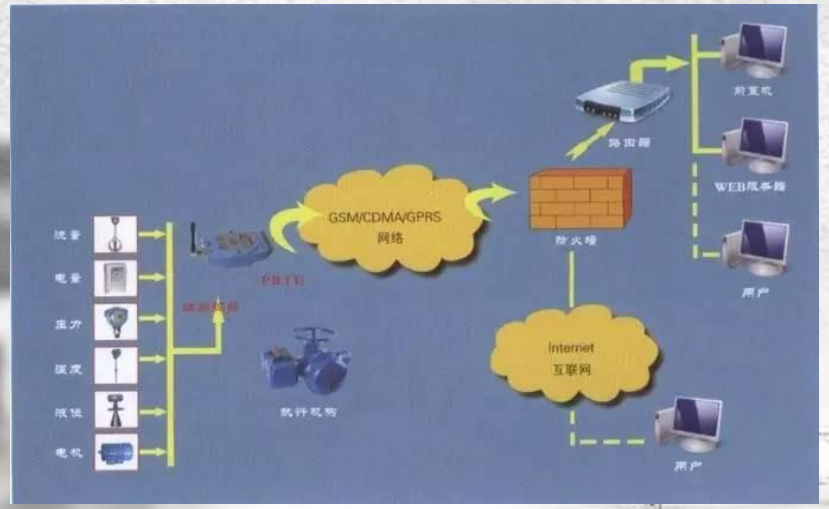
- 业务了解
- 漏洞定位

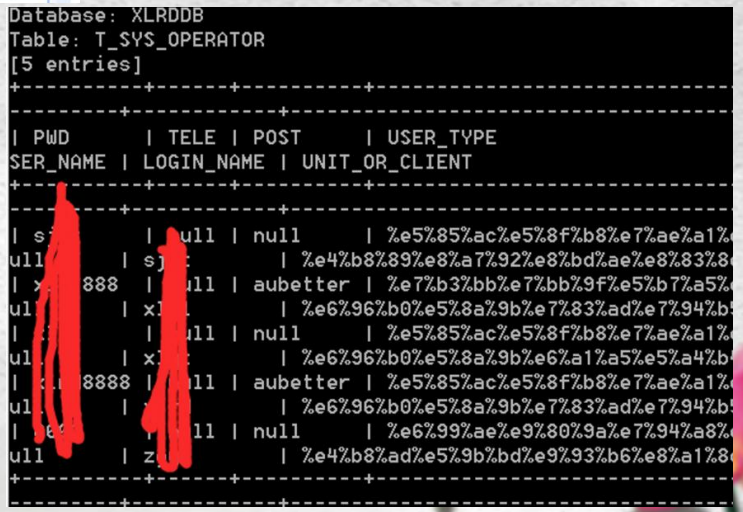
网络摄像漏洞挖掘

- 业务功能了解
- 敏感信息泄露定位
- 相关弱点利用



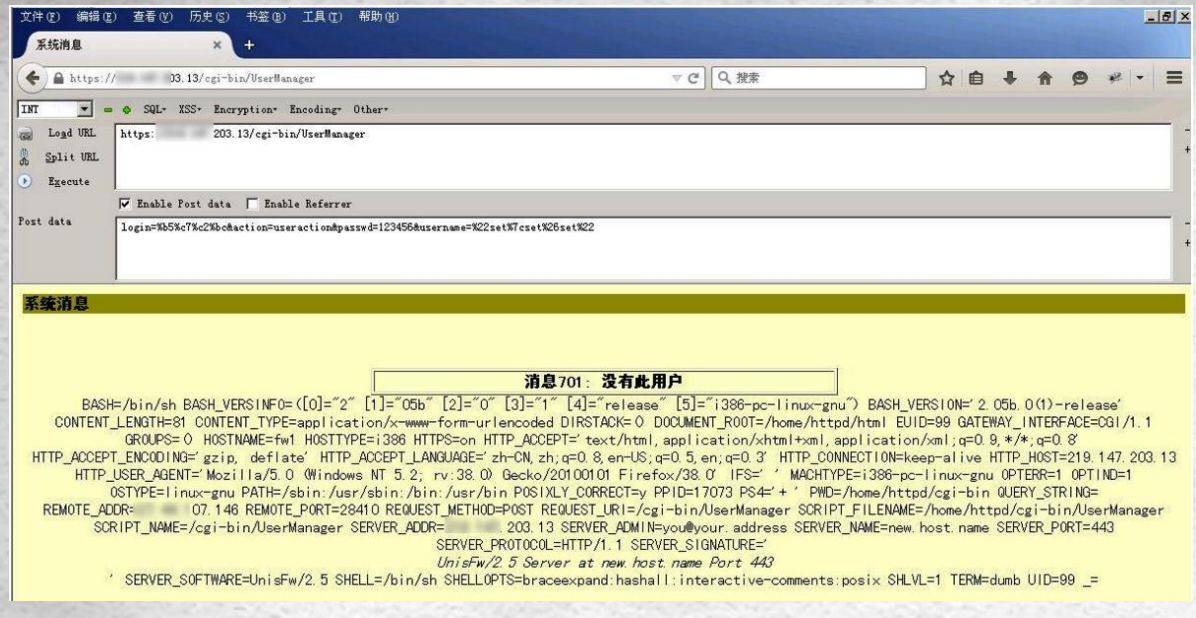
监控设备漏洞挖掘



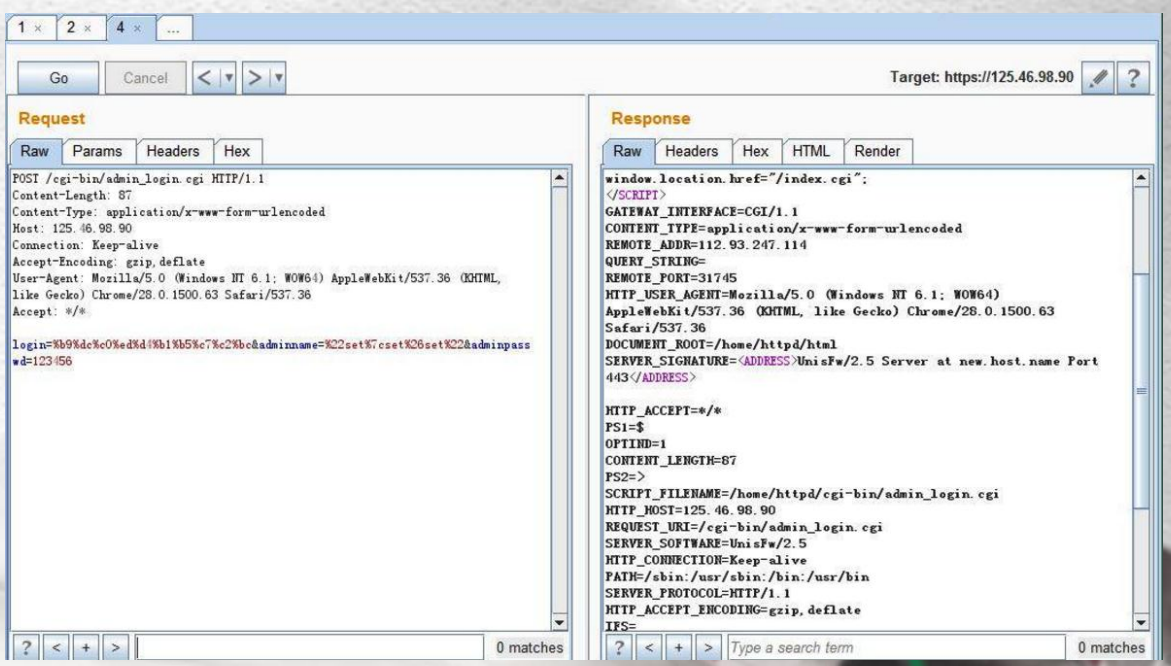


- 业务功能了解
- 熟悉输入输出数据
- 黑盒漏洞测试
- 相关弱点利用

安全防御设备漏洞挖掘



- 业务功能了解
- 业务功能路由定位
- 相关漏洞测试
- 相关弱点利用



说一千道一万：

- 传统漏洞
- 新型漏洞
- 系统漏洞测试
- 通信漏洞测试
- 系统业务漏洞
- 固件逆向分析

通信数据
通信协议

- 白盒审计
- 黑盒测试
- 灰盒测试

+ 思路

继续“玩”

接近目标区域

前往

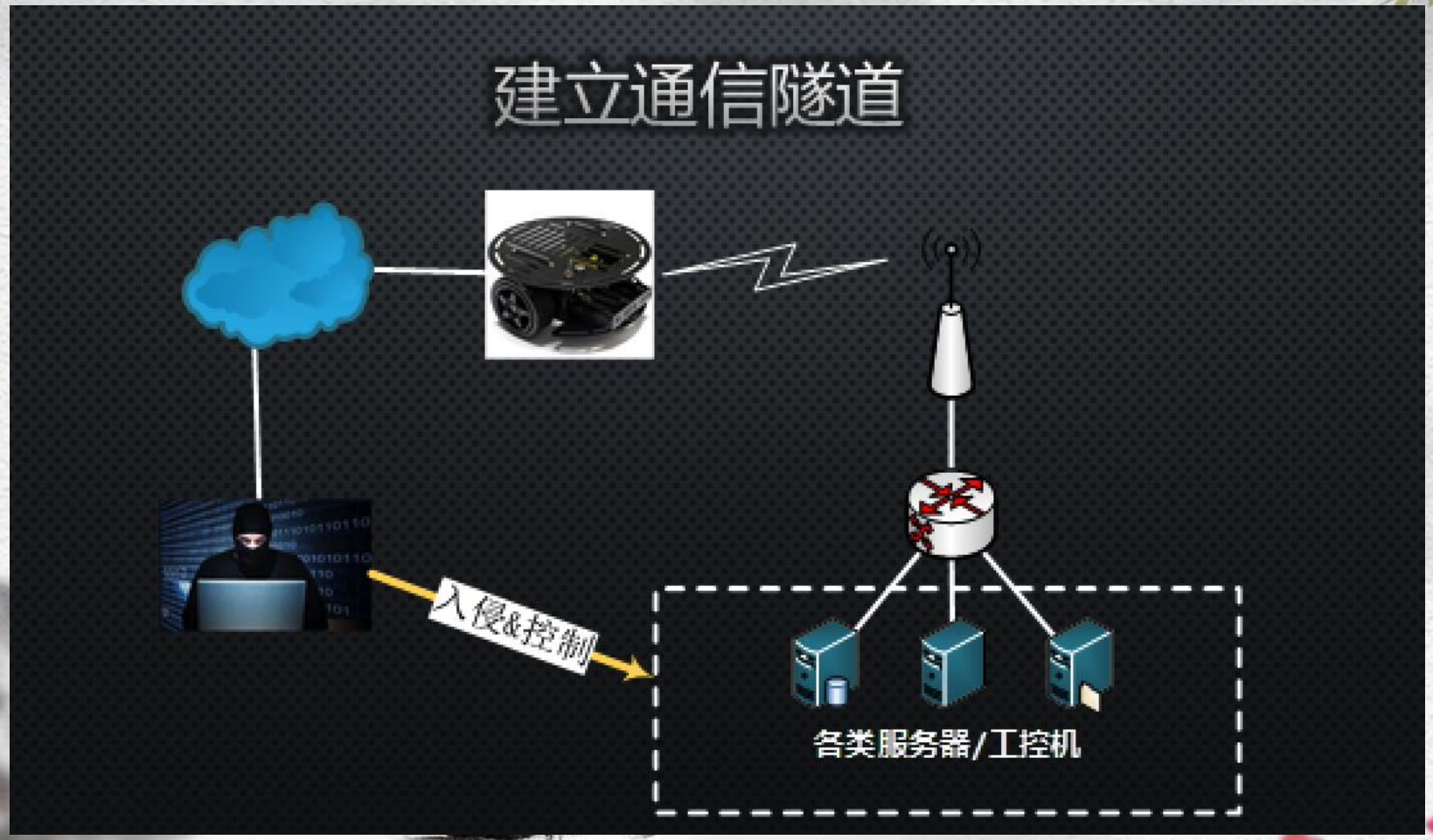
目标区域

投放AGENT设备

投放

扫描&连入网络

建立通信隧道



唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

继续“玩”.....

Give It To You

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center