

智能时代风险的安全治理思路探讨

--摸清家底实践

• 权小文@WebRAY



1

背景介绍

“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。”

- 习近平在网信工作座谈会上的讲话。（2016年4月19日）

背景介绍 | 从校园网看安全现状

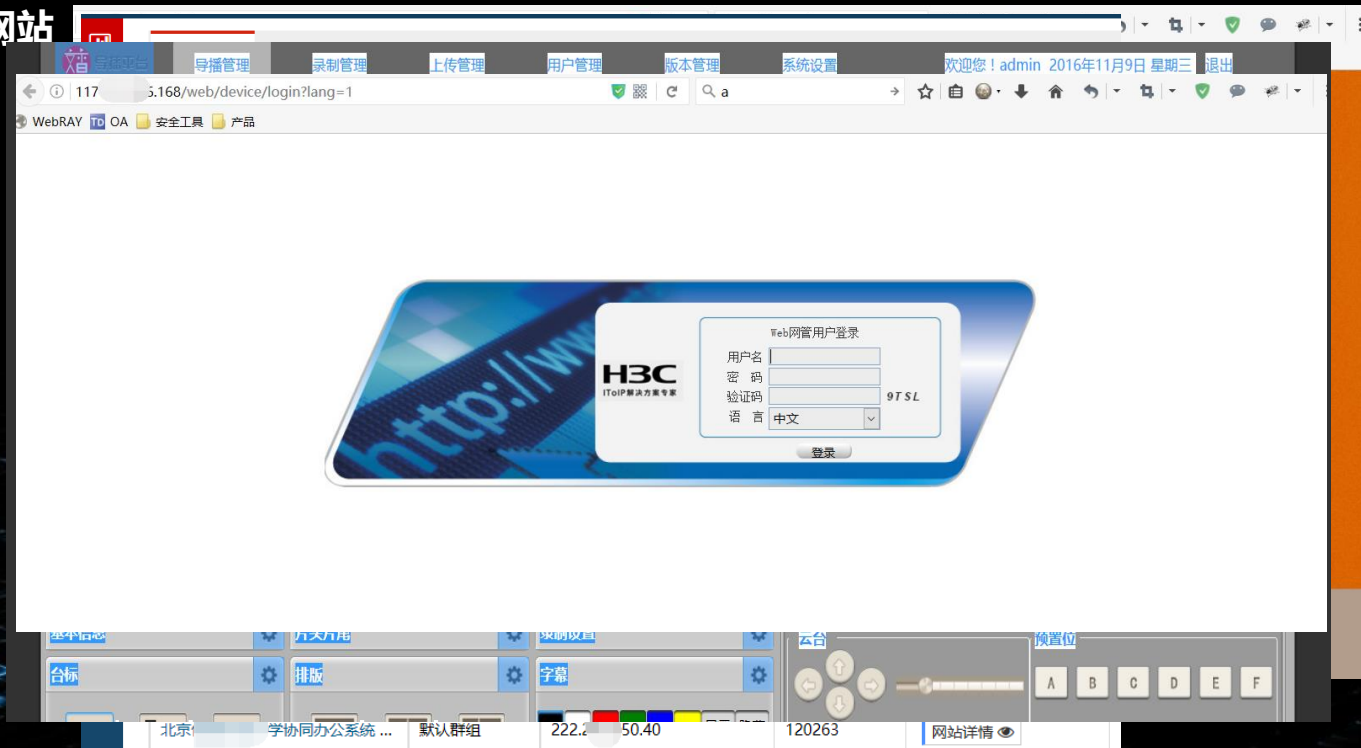
1、利用学校资源搭建商业网站

2、废弃网站未能及时退运

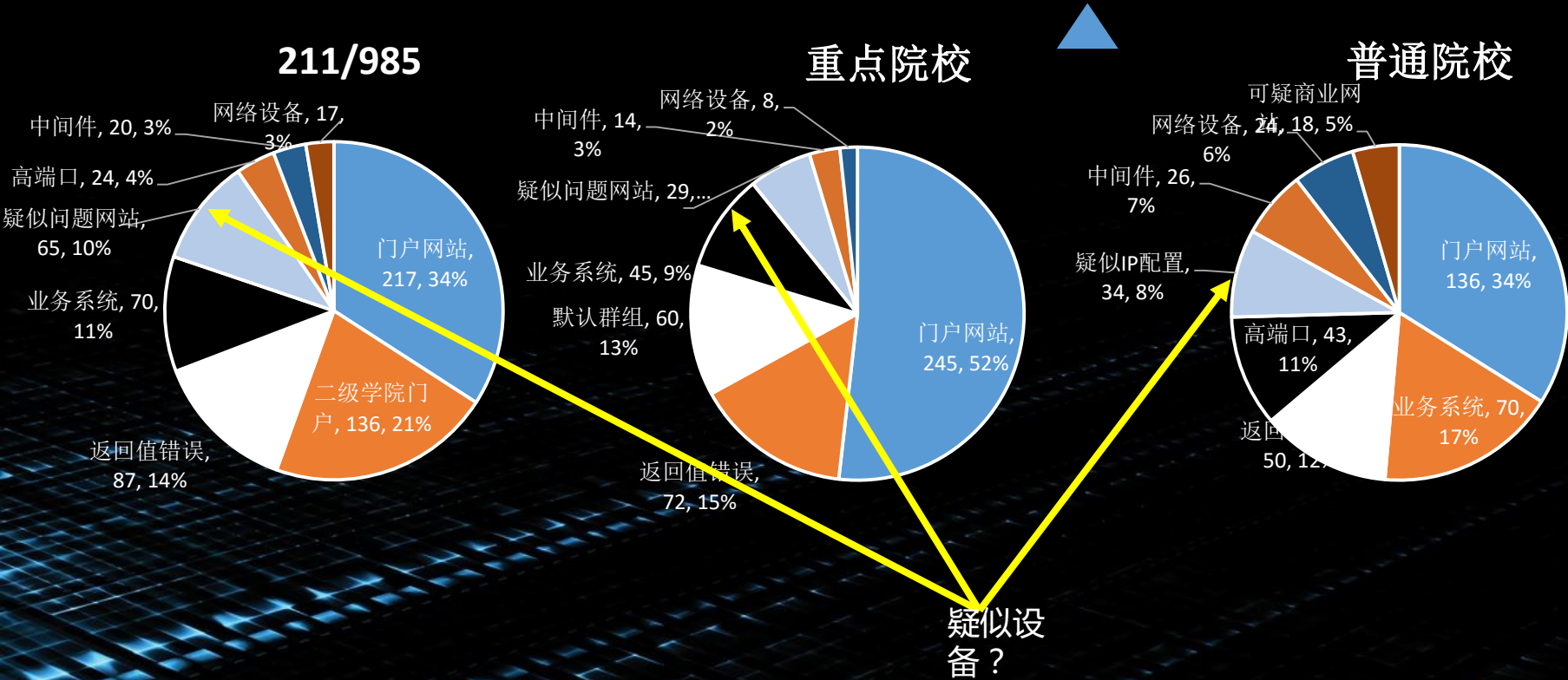
3、未知站点访问量异常

4、视频监控配置公网IP，
且存在弱口令

5、打印机、网络设备配置公网IP，
且存在弱口令



背景介绍 | 教育行业Web应用分布情况



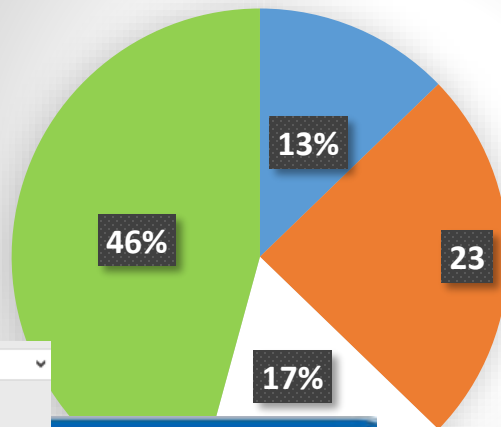
背景介绍 | 智能设备普查

门禁专家

登录名: abc

DCN

智能设备



- 摄像头
- 打印机
- 门禁系统
- 其他设备

HD HIKVISION

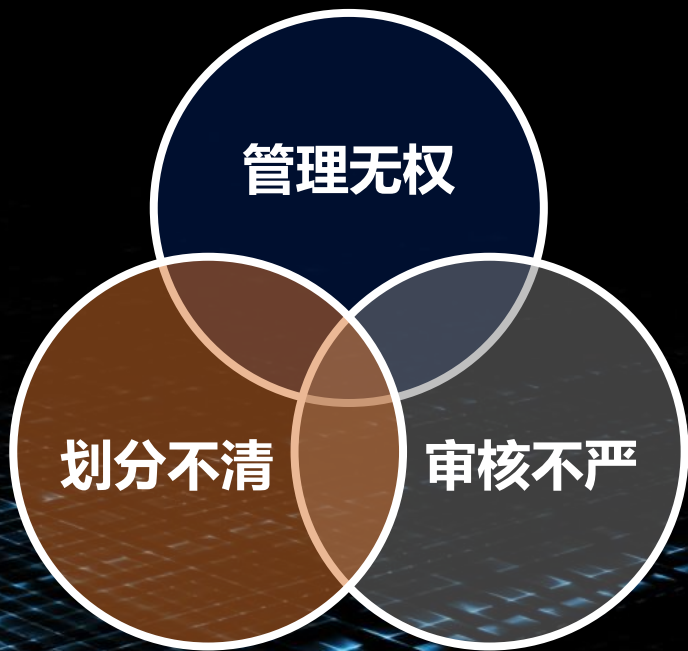
用户名
密 码

中文

YVS5

背景介绍 | 结论1：有人建，没人管。有人用，没人防

- 数量多，使用权、管理权分散
- 系统私搭乱建现象严重，常规手段无法监测网站数量
- 责、权、利不好界定，“网络中心”“信息中心”成为业务部门替罪羊
- 专业人员配置不足
- 退运的系统，无人监督管理，成为孤岛



背景介绍 | 结论2：智能设备大多弱口令或者无口令

门禁专家

门禁专家

登录名: abc

首页 加卡 用户 记录 配置 退出

密 码:

搜索 最前页 上一页 下一页 最后页 刷新最新记录 第 1 页 / 共 49 页 2017-07-26 18:58:23

记录序号	卡号	姓名	状态	时间
972	1928468970		远程开门[#1号门]	2017-07-26 18:58:22
971	1928468970		远程开门[#1号门]	2017-07-26 18:58:20
970	100001		允许 进门[#1号门]	2017-07-21 12:51:29



2

实践方案

“摸家底”系统

网络空间威胁
发现系统

第一阶段

网络空间资产发现

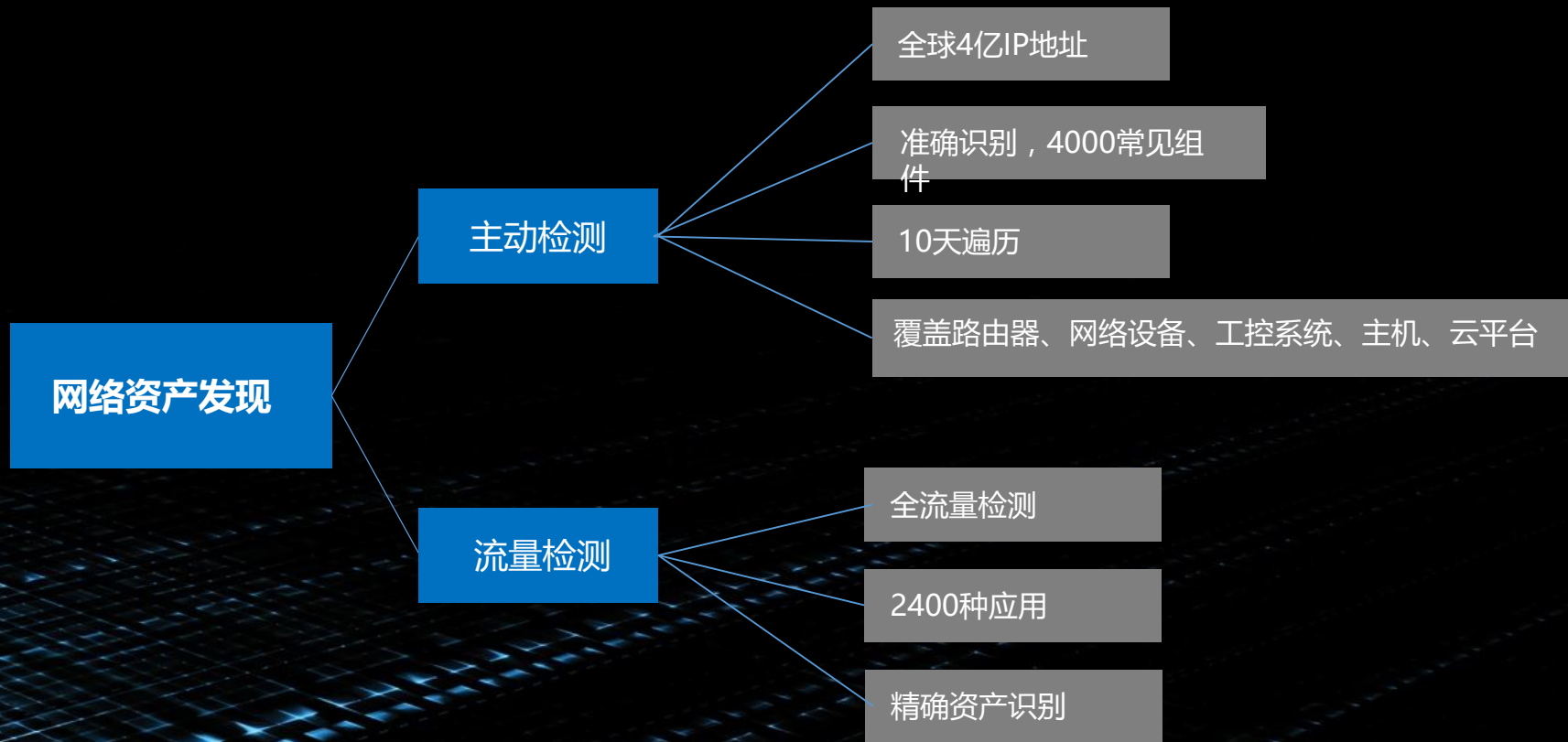
第二阶段

网络空间漏洞检测

第三阶段

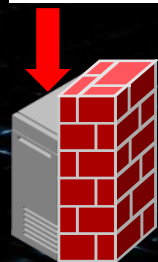
安全事件通报/处置

阶段1：网络空间资产发现



阶段1：网络空间资产发现

名称	数量
路由器	37+
打印机	10+
各种应用程序	3900+
工控设备	360+
操作系统	20+
网络安全设备	45+

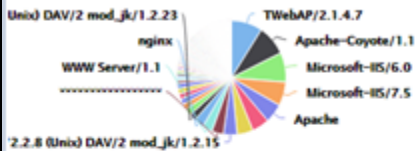


镜像流量：

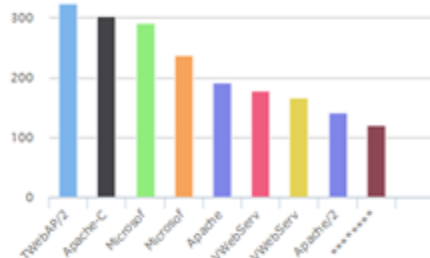
- 1) 资产识别 (**DPI+AI**) ;
- 2) 对流量进行**webshell**被动学习 ;

阶段1：网络空间资产发现

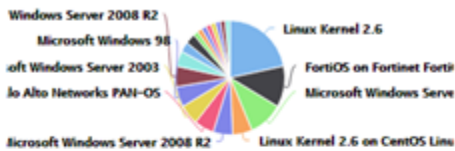
中间件分布



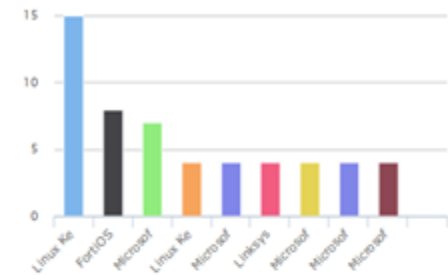
中间件Top10



操作系统分布

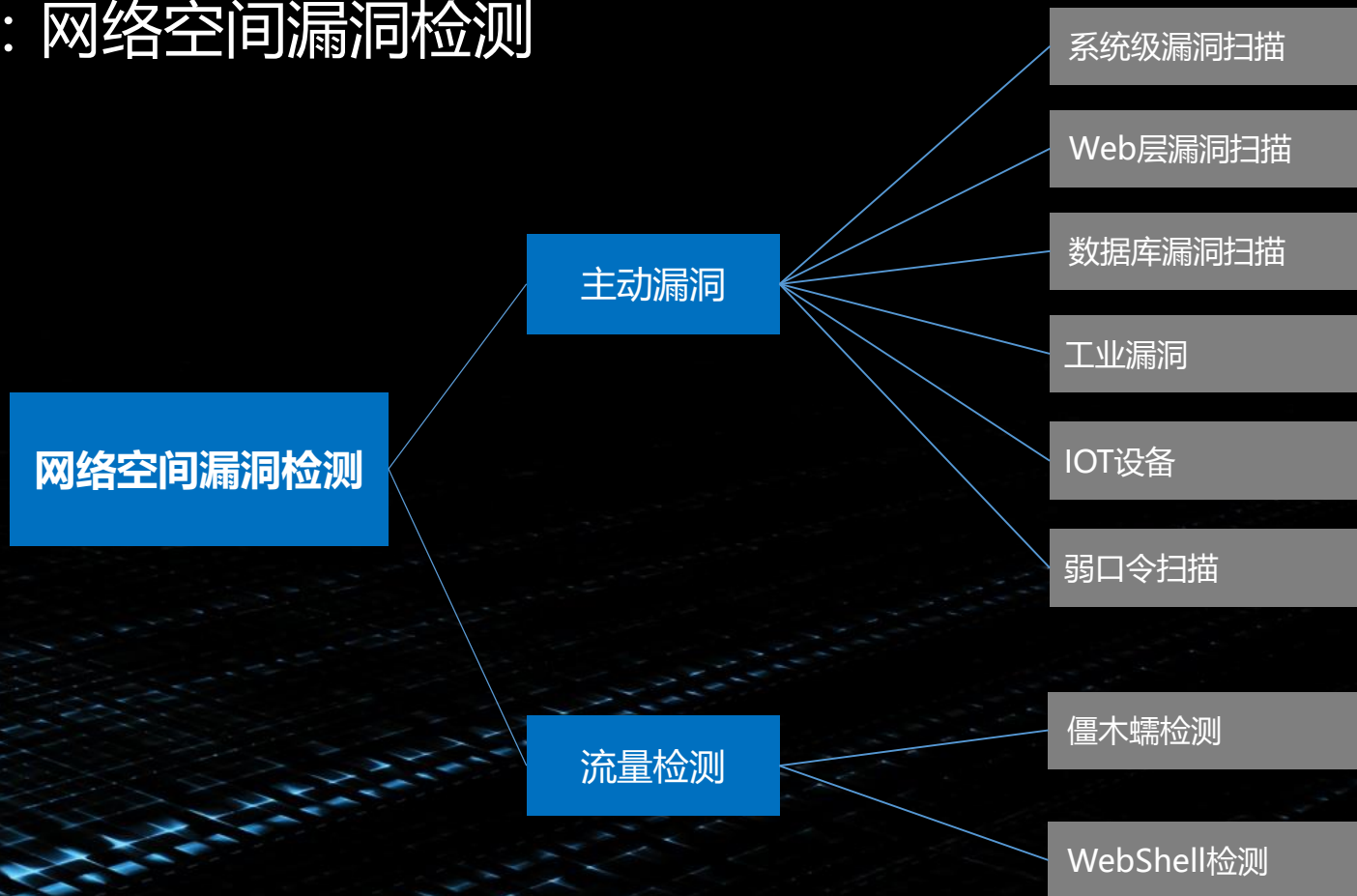


操作系统Top10



网站名称	URL	IP	中间件	操作系统	语言	编码	物理地址
2f .96.216.58	http://202.196.216.58	6.58	ZK Web Server	--	--	gb2312	
“两学一做” 计划	http://shen .xu.xcu.edu.cn	91.19	YlinkWAF	--	--	UTF-8	
经贸管理学院	http://msc .qda.edu.cn	32.3	YlinkWAF	--	--	utf-8	
图书馆	http://rbk.xc .du.cn	91.19	YlinkWAF	--	--	UTF-8	
经济学院	http://se .lu.cn	91.19	YlinkWAF	--	--	utf-8	
tu .xcu.edu.cn:8000	http://enst .xcu.edu.cn:8000	1.55	YlinkWAF	--	--	gb2312	
“两学一做” 学习教育网	http://lyz .edu.cn	91.19	YlinkWAF	--	--	UTF-8	
16 91.57	http:// .191.57	91.57	YlinkWAF	--	ThinkPHP	utf-8	
	http://rensi .edu.cn	91.19	YlinkWAF	--	--	UTF-8	
研究所	http://weijin .du.cn	91.19	YlinkWAF	--	--	UTF-8	
经贸管理信息系统	http://gra .du.cn	61.43	YlinkWAF	--	ASP.NET	gb2312	

阶段2：网络空间漏洞检测



阶段2：网络空间漏洞检测

名称	数量
Web漏洞	900+
系统漏洞	70000+
数据库漏洞	2900+
工控漏洞	460+
敏感词库	20000+
暗链词库	300+
后台词典库/webshell	4000+ (部分来自守望者实验室)
弱密码库	80万条

类别名称	
✓已启用	A1 注入[244]
✓已启用	A2 失效的身份认证和会话管理[4]
✓已启用	A3 跨站脚本 (XSS) [46]
✓已启用	A4 不安全的直接对象引用[59]
✓已启用	A5 安全配置错误[30]
✓已启用	A6 敏感信息泄漏[18]
✓已启用	A7 功能级访问控制缺失[4]
✓已启用	A8 跨站请求伪造 (CSRF) [2]
✓已启用	A9 使用含有已知漏洞的组件[11]
✓已启用	A10 未验证的重定向和转发[3]

风险级别	
类别名称	
✓已启用	数据库安全[2923]
总计1条记录	

风险级别	
类别名称	
✓已启用	Linux安全[39036]
✓已启用	SMTP安全[135]
✓已启用	网络设备安全[1151]
✓已启用	Windows安全[4452]
✓已启用	数据库安全[2923]
✓已启用	合规性检测[45]
✓已启用	P2P安全[76]
✓已启用	虚拟机安全[110]
✓已启用	DNS安全[133]
✓已启用	SNMP安全[33]
✓已启用	Unix安全[21047]
✓已启用	Web安全[4990]
✓已启用	默认账号[104]
✓已启用	RPC安全[36]
✓已启用	移动设备[51]
✓已启用	远程溢出[277]
✓已启用	后门检测[104]
✓已启用	安全设备[193]
✓已启用	FTP安全[246]

阶段2：网络空间漏洞检测

高风险
高风险
高风险
高风险
高风险
高风险
高风险
高风险
高风险
中风险
中风险
中风险
中风险

OpenSSH sshd
CVE-2015-5600

CNCVE
CNCVE-2015-560

风险级别
严重

影响网站详情

网站名称

公共基础教研部

河南医学高等专科学校

河南财政金融学院

科研处

cloud.ananas.zut

EIC创新中心

新乡医学院三全学院

河南省免疫规划信息

1.网站概述

1.1网站基本信息

网站名称

URL

IP

域名

中间件

操作系统

语言

编码

MAC地址

物理地址

所属用户

所属群组

备案状态

1.2检测基本信息

网站漏洞评分

漏洞总计

漏洞分布

3.1 漏洞详情

漏洞名称	所属分类	所属类型	出现次数
Apache 2.2.x < 2.2.25多个漏洞	Web安全	系统漏洞	1

3.1 漏洞详情

漏洞名称	所属分类	所属类型	出现次数
Cookie未配置HttpOnly标志	A2 失效的身份认证和会话管理	WEB漏洞	1

详细描述 HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。

解决方案 为SetCookie配置HttpOnly属性

URL	http://fzxx.henu.edu.cn/home/search/information/p/8.html
问题参数	
测试用例	GET /home/search/information/p/8.html HTTP/1.1 Accept: */* Referer: http://fzxx.henu.edu.cn/Home/Search/information/sub/ Host: fzxx.henu.edu.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: CWA_Uid999=37988939301977981152;CWA_lasttime999=1500290001976;CWA_repeat999=15;CWA_rti999=0;PHPSESSID=kd5f5lsp06im6ij53ddhmfc077
备注信息	Cookie中没有包含httponly属性：iischool_crypt=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=fzxx.henu.edu.cn
漏洞验证	浏览器验证
操作	误报删除

Apache 2.2.x < 2.2.25多个漏洞	Web安全	系统漏洞	1
Apache 2.2.x < 2.2.24多个XSS漏洞	Web安全	系统漏洞	1
Apache 2.2.x < 2.2.23多个漏洞	Web安全	系统漏洞	1
Apache 2.2.x < 2.2.22多个漏洞	Web安全	系统漏洞	1
Apache HTTP Server mod_proxy_ajp拒绝服务漏洞	Web安全	系统漏洞	1

阶段2：网络空间漏洞检测

	Web资产名称
[-]	1207
时间	
2017-07-14 16:28:32	
2017-07-14 16:28:17	
2017-07-14 16:28:17	
2017-07-14 16:21:02	
2017-07-14 16:21:02	

WebShell详情	
请求链接	http://192.168.8.60:8080/jsp/leo.jsp
服务端口	8080
请求方式	GET
协议	HTTP/1.1
请求头	Accept : /*/* Accept-Encoding : gzip,deflate Connection : Keep-Alive Cookie : JSESSIONID=FEB34FE542C55F71C502590B59210AD2 Host : 192.168.8.60:8080 Referer : http://192.168.8.60:8080/jsp/leo.jsp User-Agent : Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0
请求数据	
响应头	Content-Type : text/html;charset=gb2312 Date : Fri, 14 Jul 2017 08:18:13 GMT Server : Apache-Coyote/1.1 Transfer-Encoding : chunked
返回状态	返回值200 疑似后门

[İA %p Ü Aİ](#)
[CMD AÜ Aİ](#)
[İµ J³ Eö ĐÖ](#)
[¶ Öü](#)
[Silic Group](#)

μ±Ç°ÄÛÄ±£° E:\apache-tomcat-7.0.78-windows-x64\apache-tomcat-7.0.78\webapps\sp\

CPV⁺AE+ : C\ D\ E\

[下载原始文件](#)

验证①

除血

删除

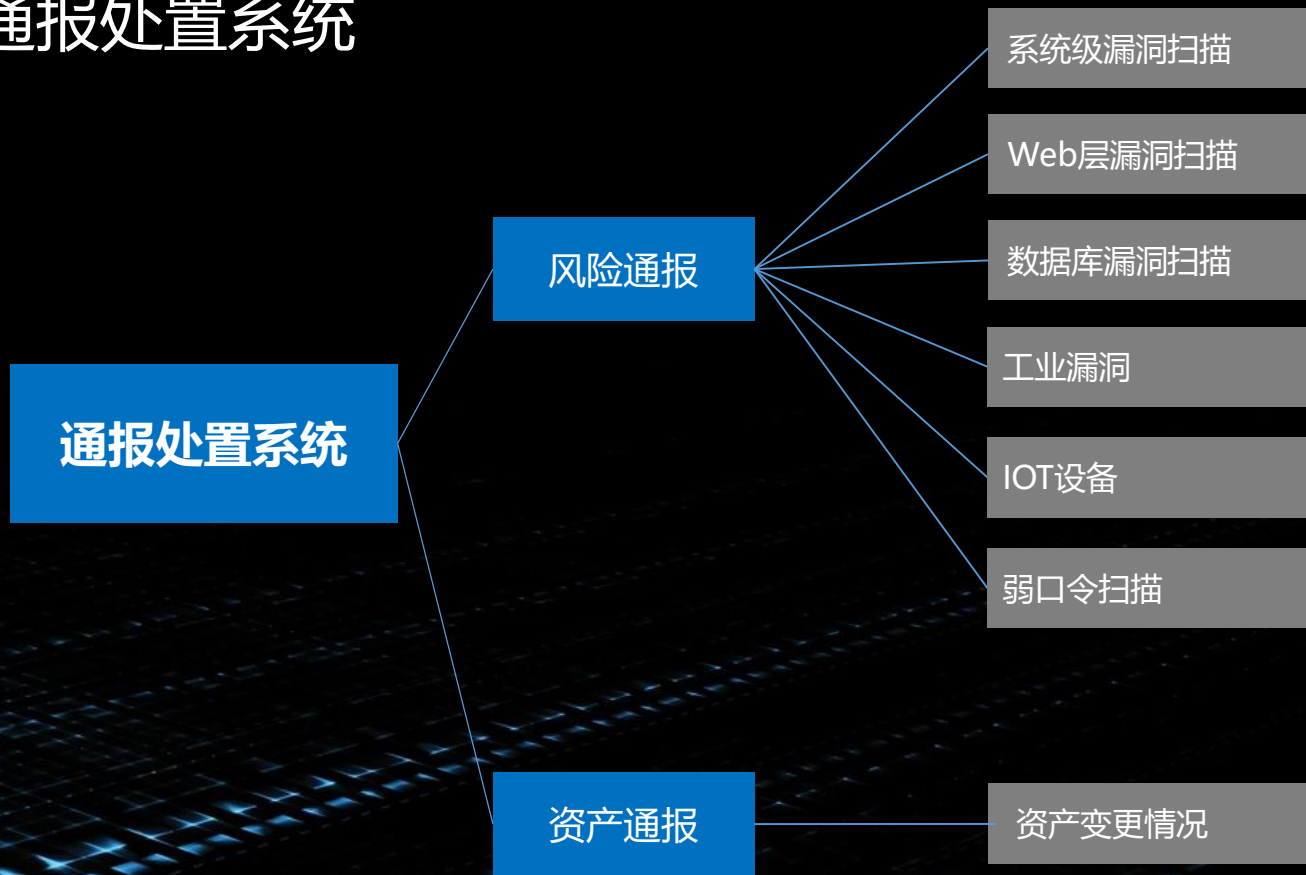
删除

删除

删除

删除

阶段3：通报处置系统



阶段3：风险资产事件通报处理

test002, 欢迎您!

修改密码

退出

网站管理

自动通报

手动通报

流程状态

通报管理

通报配置

通报统计

手工录入

批量导入

模板文件:

浏览...

导入

支持Excel文件导入, 点击[下载样例模板](#), 了解格式约定。

单位名称

模糊查询

单位地址区县:

行业类别:

开始查询

序号	单位名称	网站名称	行业类别	单位地址	网站域名 (选择接口提供数据)	IP地址	区县	行政区划代码	创建日期
1	品药品监督管理局分局	品药品监督管理局分局	公安		http://www.gov.cn				2017-04-09 14:41:49
2	区环境保护局	区环境保护局	公安		http://www.gov.cn			330402	2017-04-09 14:41:31
3	区公共资源交易中心	区公共资源交易中心	公安		http://www.x.com		区	330402	2017-04-09 14:41:13
4	区城乡建设委员会	区城乡建设委员会	公安		http://www.gov.cn			330402	2017-04-09 14:40:59
5	区人民代表大会常务委员会	区人民代表大会常务委员会	公安		http://www.gov.cn		区	330402	2017-04-09 14:40:00
6	区商务局	区商务局	公安		http://www.sp.gov.cn		区	330402	2017-04-09 14:39:39
7	区交通委员会	区交通委员会	公安		http://www.com		区	330402	2017-04-09 14:39:15
8	区就业服务管理局2	区就业服务管理局2	公安		http://www.sp.r.cn		区	330402	2017-04-09 14:36:38
9	区就业服务管理局1	区就业服务管理局1	公安		http://www.com		区	330402	2017-04-09 14:36:16
10	区经济和信息化委员会	区经济和信息化委员会	公安		http://www.w.com		区	330402	2017-04-09 14:35:48

阶段3：风险资产事件通报处理



test002, 欢迎您!

 修改密码 退出

网站管理

自动通报

手动通报

流程状态

通报管理

通报配置

通报统计



总计通报任务：7个

已完成任务数：4个

未上报任务数：1个

执行中任务数：2个



网页篡改

任务3



通报单位数量

■ 数量：2323

通报类型

■ 系统数量：12321

通报任务编号

■ 任务编号：00916732

通报发布时间

■ 20150112:12:30

通报事件等级

■ 三级

处置周期

- 20150112:12:30-



网页挂马

通报任务信息



网站变更

任务4



网站运行

通报任务信息



阶段3：风险资产事件通报处理



test002, 欢迎您!  修改密码  退出 

网站管理

自动通报

手动通报

流程状态

通报管理

通报配置

通报统计

总计通报任务：6个

已完成任务数：1个

未上报任务数：0个

执行中任务数：2个

未接收任务数：3个

未复核任务数：0个

 单位通报

111

123

WEB安全漏洞

网站篡改

 事件通报

网站篡改

通报单位数量

■ 数量：

通报类型

■ 类型：

通报任务编号

■ 任务编号：

通报发布时间

■ 时间：

通报事件等级

■ 等级：

处置周期

■ 周期：天

创建通报任务

进入通报管理

欢迎指正，谢谢



权小文@WebRAY

北京 昌平

