金融Web应用系统漏洞分析方法

安赛- 林榆坚

OWASP 中国

The Open Web Application Security Project

关于我-安赛科技

OWASP 中国
The Open Web Application Security Project

- 姓名 : 林榆坚-linx
- 北京安赛创想科技有限公司CTO
- 知名漏洞扫描器AIScanner创始人
- 前百度网络安全工程师
- linx@aisec.cn

AISEC 安赛
Artificial Intelligence Security
让网络安全变得更轻松、更智能

目录

OWASP 中国
The Open Web Application Security Project

- 1. 金融行业安全现状
- 2. 问题根源
- **3. 现有解决方案面临的难题**
- 4. 三位一体的漏洞分析方法
- 4.1 主动式（全自动）Web2.0漏洞扫描
- 4.2 半自动式漏洞分析：业务重放+高覆盖度
- 4.3 被动式漏洞分析：应对0Day和安全死角

金融行业安全现状(1)网站

OWASP 中国
The Open Web Application Security Project

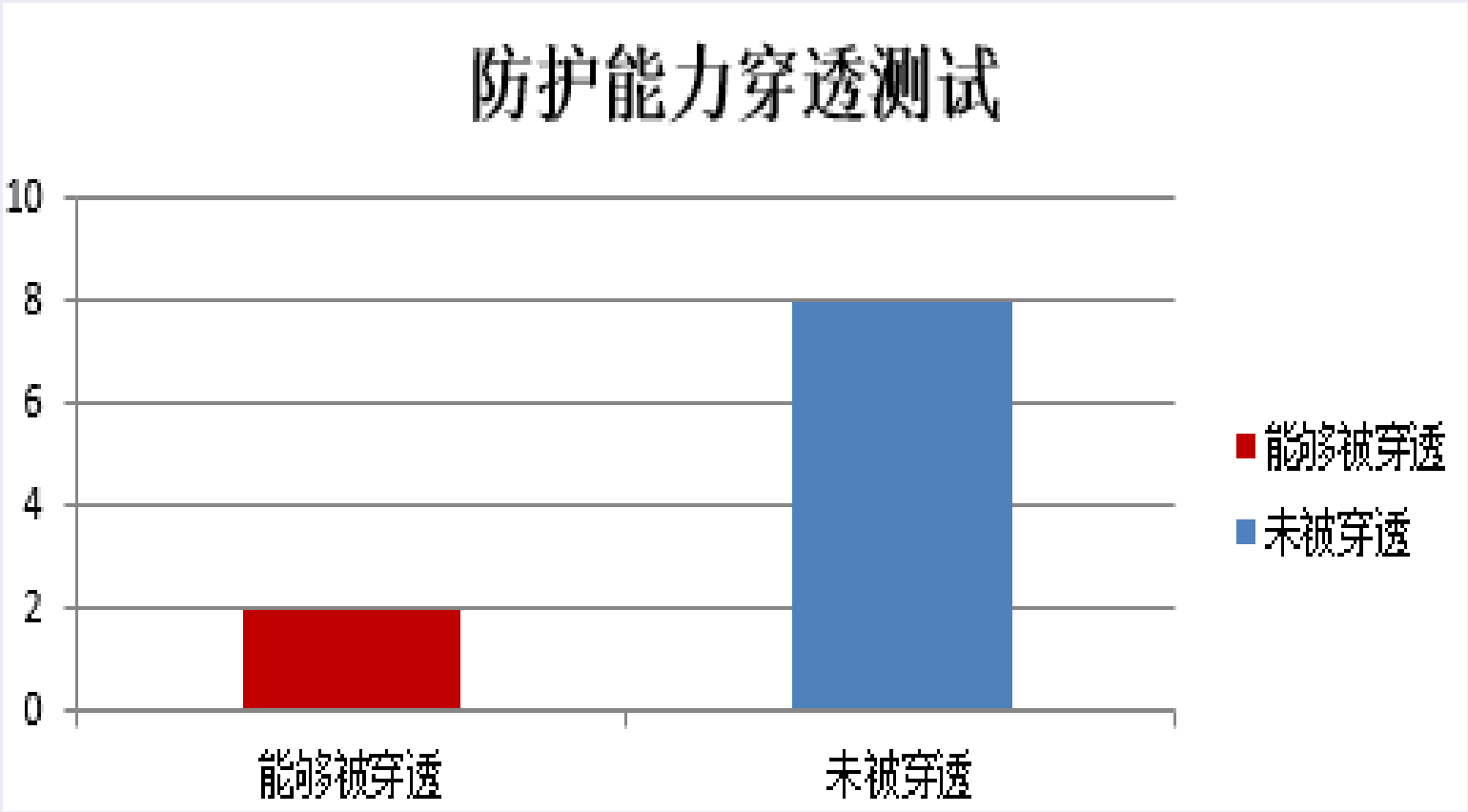
2013年，经国内安全监管机构研究发现：

- 154家银行的官方网站，35家存在高危漏洞，占总数的23%；26家存在中危漏洞，占比17%。
- 存在中危及高危漏洞的银行数量占检测总数45%，安全状况呈恶性发展趋势。
- 发现高中危漏洞数超过100个

金融行业安全现状(2)防护能力

OWASP 中国
The Open Web Application Security Project

- 20%的防护设备可被穿透-现有的攻击手段



- **斯洛登带给了我们什么？**

金融行业安全现状

OWASP 中国
The Open Web Application Security Project

- 基础网络设施漏洞情况，15%存在漏洞

设备现状

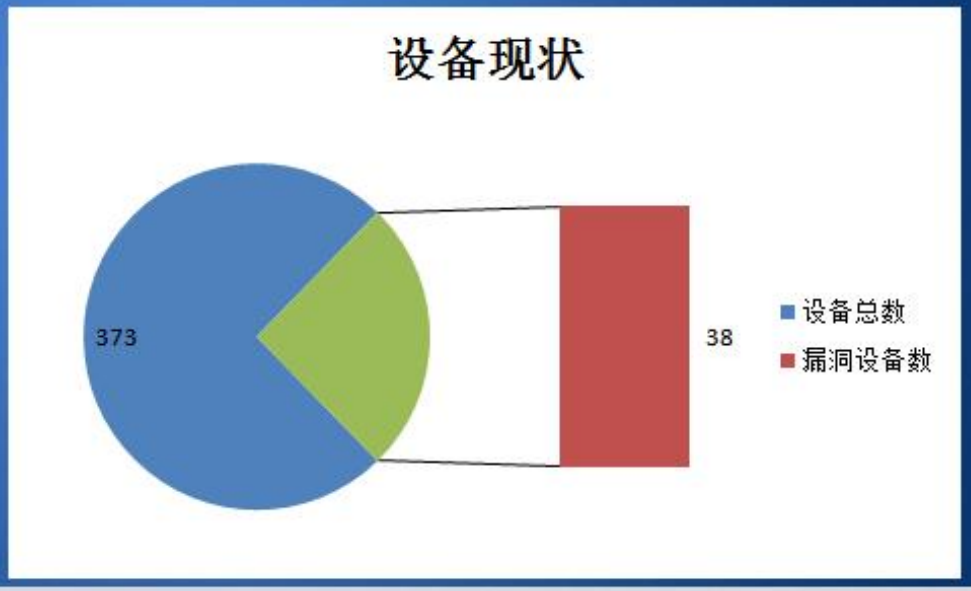
厂商分布

漏洞分布

漏洞危害

1 370多台路由器/交换机

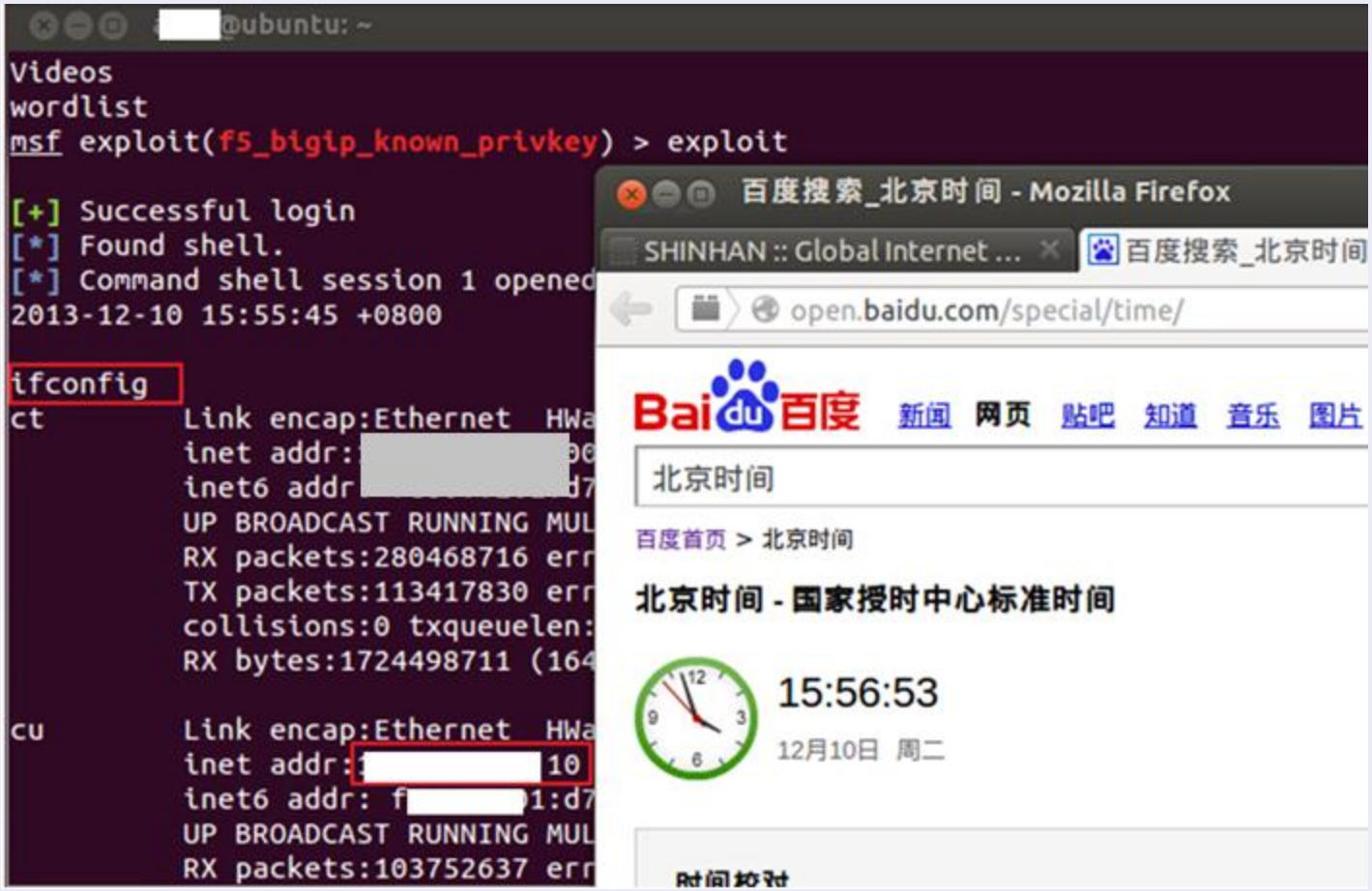
2 其中15%的设备存在漏洞



控制网络设备

OWASP 中国
The Open Web Application Security Project

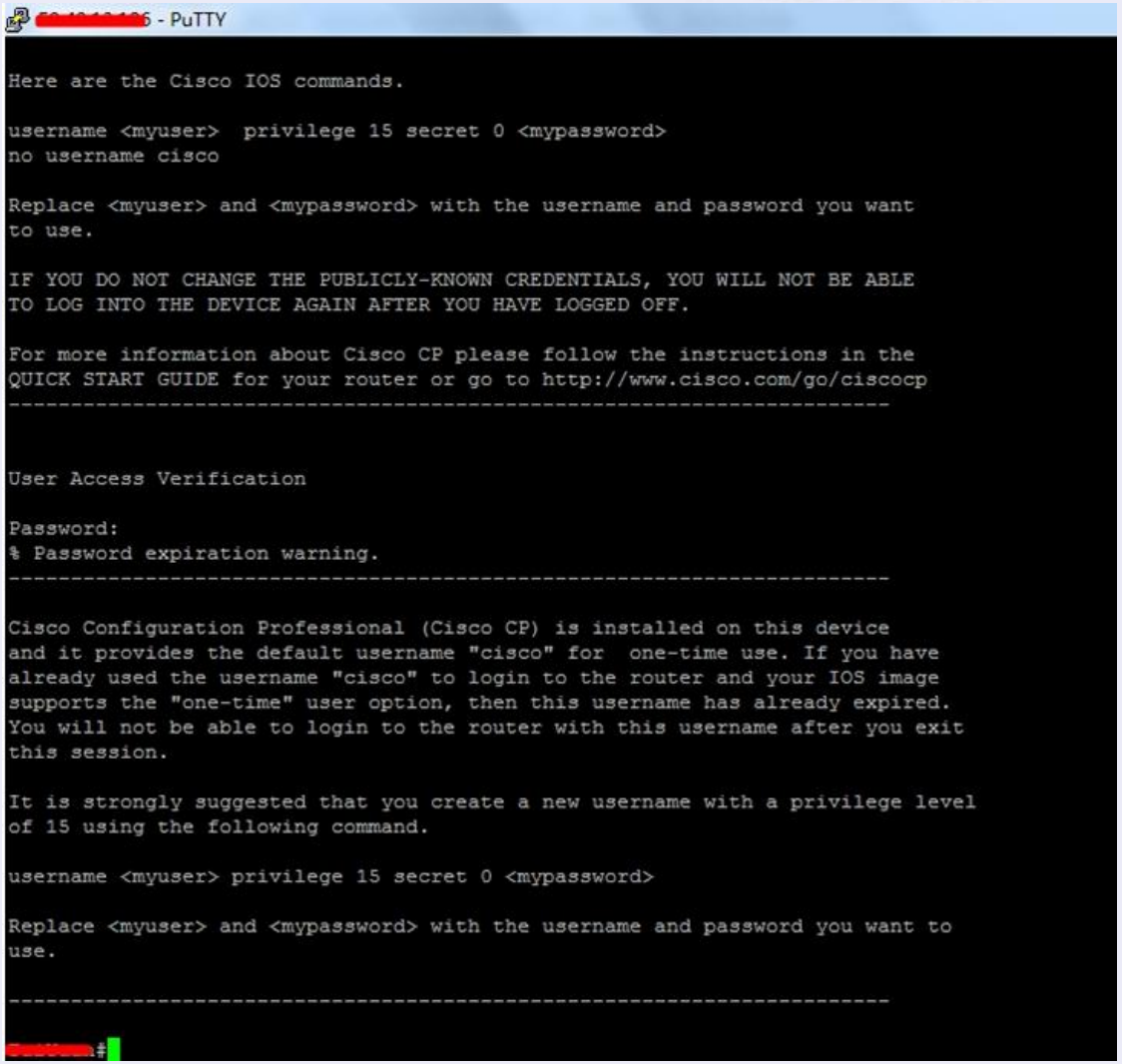
- 数十台网络设备存在漏洞



思科路由器

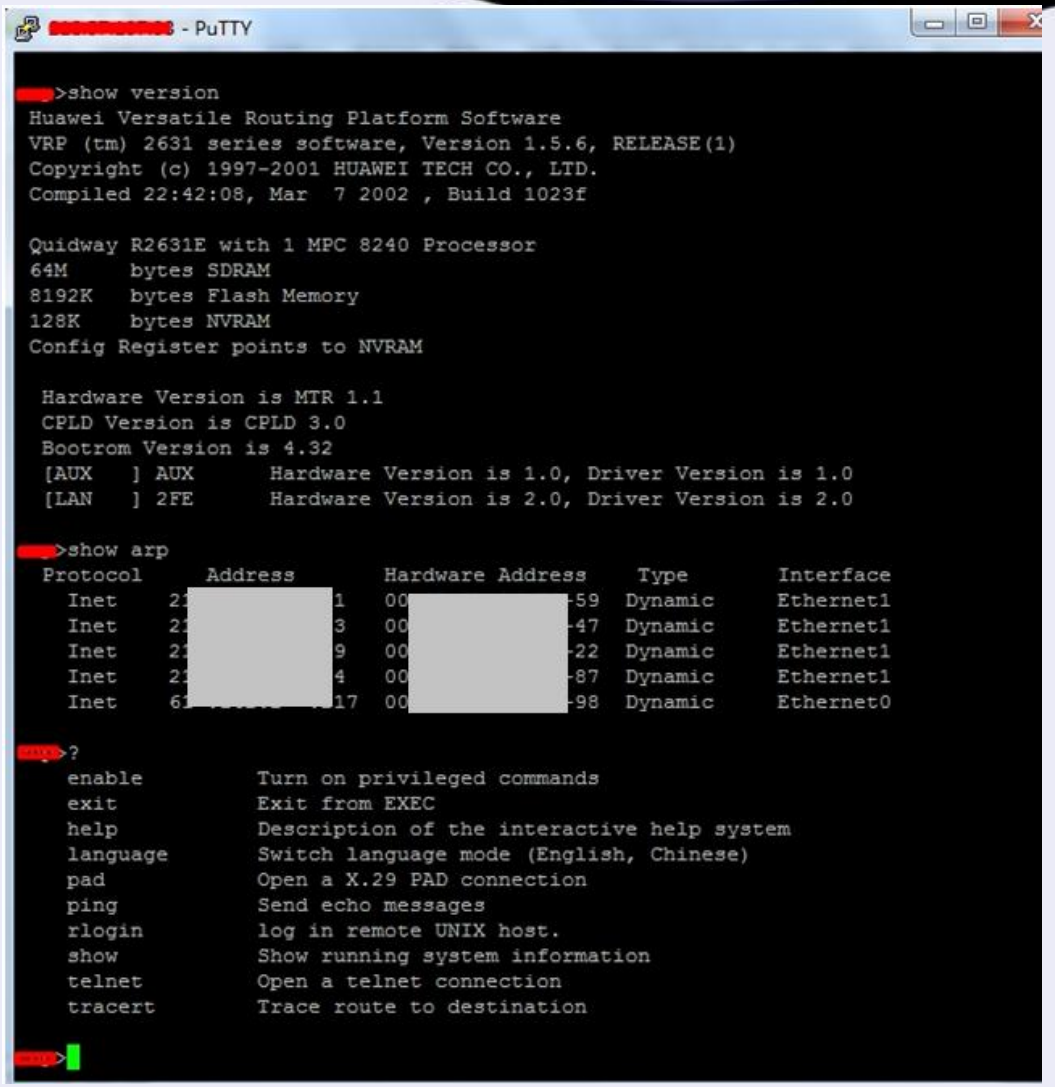
OWASP 中国
The Open Web Application Security Project

- 思科路由



华为路由器

- 华为路由器


[redacted] - PuTTY
>show version
Huawei Versatile Routing Platform Software
VRP (tm) 2631 series software, Version 1.5.6, RELEASE(1)
Copyright (c) 1997-2001 HUAWEI TECH CO., LTD.
Compiled 22:42:08, Mar 7 2002 , Build 1023f
Quidway R2631E with 1 MPC 8240 Processor
64M bytes SDRAM
8192K bytes Flash Memory
128K bytes NVRAM
Config Register points to NVRAM
Hardware Version is MTR 1.1
CPLD Version is CPLD 3.0
Bootrom Version is 4.32
[AUX] AUX Hardware Version is 1.0, Driver Version is 1.0
[LAN] 2FE Hardware Version is 2.0, Driver Version is 2.0
>show arp
Protocol Address Hardware Address Type Interface
Inet Dynamic Ethernet1
Inet Dynamic Ethernet1
Inet Dynamic Ethernet1
Inet Dynamic Ethernet1
Inet Dynamic Ethernet0
>?
enable Turn on privileged commands
exit Exit from EXEC
help Description of the interactive help system
language Switch language mode (English, Chinese)
pad Open a X.29 PAD connection
ping Send echo messages
rlogin log in remote UNIX host.
show Show running system information
telnet Open a telnet connection
tracert Trace route to destination

- 植入永久性木马、控制骨干节点
- 这种rootkit一旦被植入，将长期潜伏，难以检出，更难以置换设备

我们面对的

OWASP 中国
The Open Web Application Security Project

- 45%的银行官方网站存在中高危险漏洞
- 20%的防护体系可以被穿透
- 15%的基础网络设施存在漏洞

目录

OWASP 中国
The Open Web Application Security Project

OWASP 中国
The Open Web Application Security Project

- 问题根源

一. 漏洞动态增加

二. 攻击技术动态发展、持续进化

金融行业安全现状

OWASP 中国
The Open Web Application Security Project

一.漏洞动态增加

每一项新产品、新技术的升级迭代，都会引进新的安全漏洞。每一项新的业务类型，都会有新的风险模型；业务变更和应用升级也有可能带进新的漏洞。

如：

- Struts的每一次产品升级，都带来了新的安全风险。
- Nosql、XML、移动app漏洞
- 移动支付、二维码支付

二.攻击技术动态升级

黑客技术不断发展，每天都可能有新的攻击技术出现，给应用带来新的威胁。

如：

防火墙绕过技术

目录

OWASP 中国
The Open Web Application Security Project

目录

OWASP 中国
The Open Web Application Security Project

- **常见解决方案难以解决的问题**

1. 防火墙
2. 全自动扫描器
3. 安全检测服务
4. 不可预知的风险
5. 技术局限：0Day

难以解决的问题

- 一. 防火墙？
- 1. 现有的防火墙防护体系是基于已知签名的，无法应对新的漏洞和新的攻击手段，随时可能面临被突破及穿透的风险。
- 2. 延迟限制：防火墙延迟不能超过100毫秒，意味着难以进行复杂的特征匹配或正则匹配。
- 3. cpu性能、内存、硬盘容量等限制：意味着难以进行复杂的双向数据流分析及安全建模。

难以解决的问题

OWASP 中国
The Open Web Application Security Project

- **二.依赖全自动扫描器？**

只能达到70~80%的覆盖面，难以应对Web及移动App应用复杂的操作逻辑。

- 如：
- 孤岛页面
- 需要登录系统
- 移动app的接口
- 具备复杂的交互逻辑的应用

难以解决的问题

OWASP 中国
The Open Web Application Security Project

- **三.依赖安全检测(安全评估)服务？**

- **周期**间隔过长;难**以**应对**未知攻**击;
- 测试**方案**难**以达到**100%**的覆盖面。**

- **四.不可预知的风险**

- 网络环境变更，如核心路由出现漏洞；
- 由于业务需求，仓促上线新的存在漏洞的应用
- 新人在研发、运维上未遵守编码规范、配置规范等

- **五.技术局限:0Day**

防御(检测)技术 在时间上 滞后于攻击技术。

目录

OWASP 中国
The Open Web Application Security Project

- 1. 金融行业安全现状
- 2. 问题根源
- 3. 现有解决方案面临的难题
- **4. 三位一体的漏洞分析方法**
- 4.1 主动式（全自动）：Web2.0、交互式漏洞扫描
- 4.2 半自动式漏洞分析：业务重放+url镜像，实现高覆盖度
- 4.3 被动式漏洞分析：应对0Day和孤岛页面

解决方案

OWASP 中国
The Open Web Application Security Project

- 4.1 主动式(全自动)Web扫描
- 使用常见的漏洞扫描器
- 自动fuzz，填充各种攻击性数据
- 业务逻辑混淆，导致服务出错

解决方案

OWASP 中国
The Open Web Application Security Project

- 4.1 主动式(全自动)Web2.0扫描-金融方向的难点:
- Web2.0自动交互 — 处理页面交互
- 防火墙绕过

产品实践:

- 国外:WVS、Appscan
- 国内:绿盟、安恒、知道创宇、安赛AIScanner

解决方案

OWASP 中国
The Open Web Application Security Project

- 4.1 主动式(全自动)Web2.0扫描
- **局限:**
- 难以处理高交互式应用
- 只能发现暴露给用户(搜索引擎)的链接，难以覆盖100%的业务链接

- **解决方法:引入半被动式漏洞分析方法**
- 在人工参与的情况下，50%以上的Web金融应用系统存在高危漏洞

解决方案

OWASP 中国
The Open Web Application Security Project

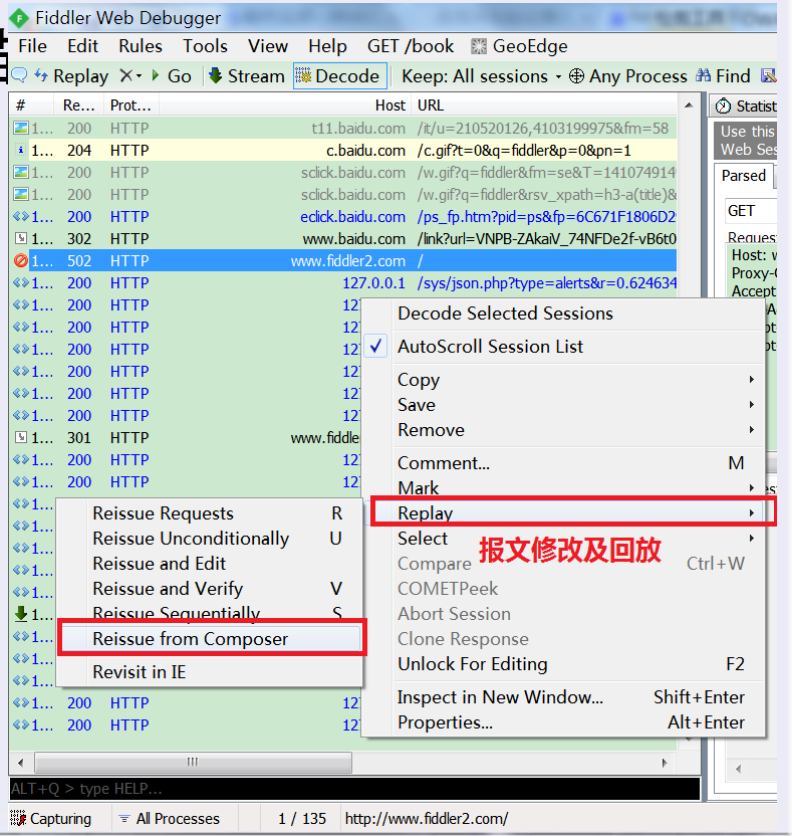
- 4.2 半自动式漏洞分析：业务重放+url镜像，实现高覆盖度

- 方法一：业务重放
- 测试过程使用 burpsuite、fiddler (www.fiddler2.com)：

1. HTTP(S)业务流量录制与重放扫描
2. 手工修改业务数据流
3. 对手机APP也适用

检测逻辑漏洞：

- 水平权限绕过
- 订单修改
- 隐藏域修改



解决方案

- 4.2 半自动式漏洞分析:业务重放+高覆盖度

- 方法二:

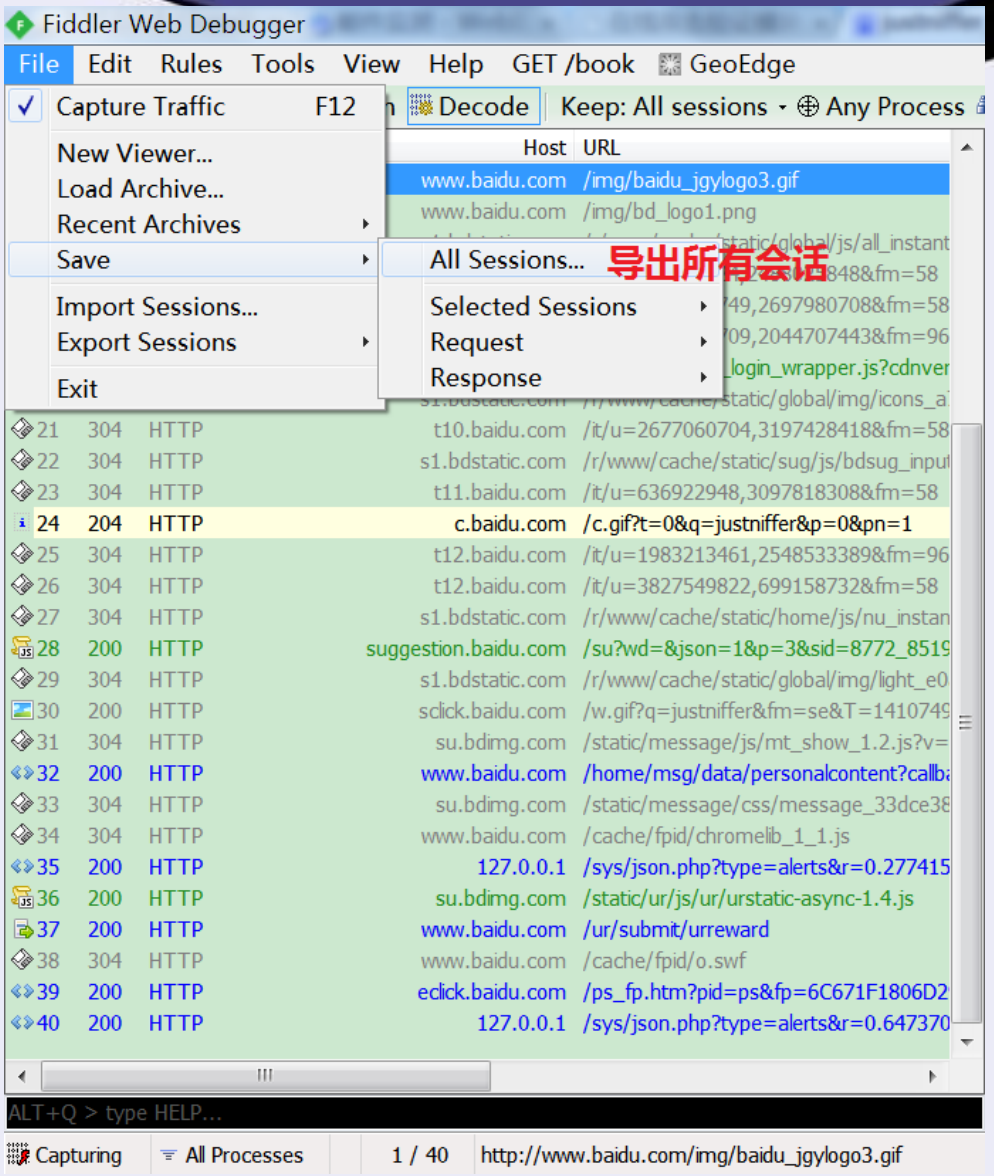
- 从日志中获取url记录

1. Fiddler的Url日志
2. 获取Apache、Nginx、Tomcat的access日志
3. 从旁路镜像中提取url日志（安全人员不用再被动等待应用的上线通知）

解决方案

OWASP 中国
The Open Web Application Security Project

1. 从Fiddler2、burpsuite导出Url日志
再导入到漏洞扫描器扫描



解决方案

OWASP 中国
The Open Web Application Security Project

2.获取Apache、Nginx、Tomcat的access日志

* 360-日志宝
* Splunk
* 各种日志审计系统

splunk 安全

splunk_百度百科

Splunk 是机器数据的引擎。使用 Splunk 可收集、
用程序、服务器和设备（物理、虚拟和云中）生成
机数据 。从一个位置搜索并分析所有实时和历史.
功能特性 产品导览 版本比较 独特优势
baike.baidu.com/ 2014-08-29

Splunk推出面向未来的安全情报产品_软件与服务_比特网

2013年5月6日 - Splunk Enterprise和Splunk App for Enterprise Security是
通过现成内容发现未知威胁的安全信息平台,其中包括新的搜索、仪表盘以
soft.chinabyte.com/482... 2013-05-06 - 百度快照 - 评价

解决方案

OWASP 中国
The Open Web Application Security Project

3. 从旁路镜像中提取url日志（安全人员不用再被动等待应用的上线通知）

如：jnstniffer、360鹰眼、各大IT公司等

- http://justniffer.sourceforge.net/
- Network TCP Packet Sniffer
- Reliable TCP Flow Rebuilding
- Optimized for "Request / Response" protocols.
- Can rebuild and save HTTP content on files

Example 1 Retrieving http network traffic in access_log format

```
$ justniffer -i eth0
```

output:

```
192.168.2.2 - - [15/Apr/2009:17:19:57 +0200] "GET /sflogo.php?group_id=205860&type=2 HTTP/1.1" 200 0 "" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko/2009032711 Ubuntu/8.10 (intrepid) Firefox/3.0.8)"

192.168.2.2 - - [15/Apr/2009:17:20:18 +0200] "GET /search?q=subversion+tagging&ie=utf-8&oe=utf-8&aq=t&rls=com.ubuntu:en-US:unofficial&client=firefox-a HTTP/1.1" 200 0 "" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko/2009032711 Ubuntu/8.10 (intrepid) Firefox/3.0.8)"

192.168.2.2 - - [15/Apr/2009:17:20:07 +0200] "GET /sflogo.php?group_id=205860&type=2 HTTP/1.1" 200 0 "http://justniffer.sourceforge.net/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko/2009032711 Ubuntu/8.10 (intrepid)Firefox/3.0.8)"
```

旁路提取url

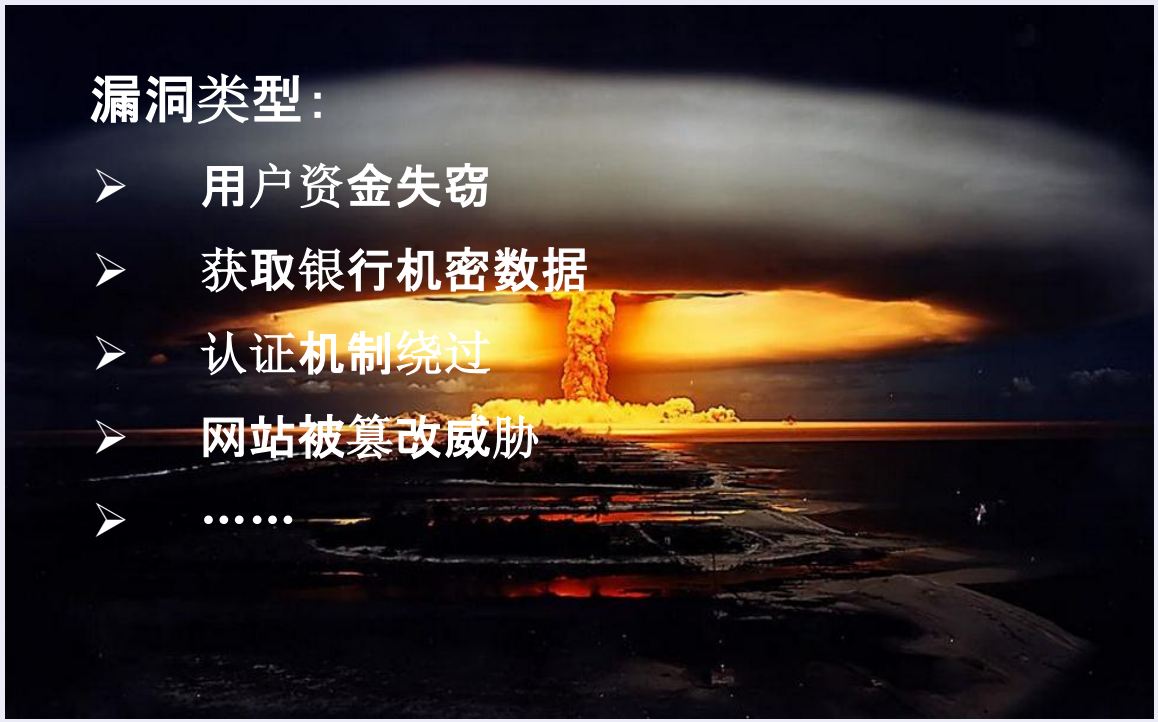
OWASP 中国
The Open Web Application Security Project

- 这种方法目前在各大IT公司都在使用
- 从旁路镜像中获取url列表，能高效地检出大量的漏洞，不需要运维人员通知，便可以获知业务系统的上线情况并执行漏洞扫描任务。

半自动检测实践

OWASP 中国
The Open Web Application Security Project

对国内20多家网上银行系统进行了半自动安全测试，发现不少存在高危漏洞，通过这些漏洞，能对系统造成非常严重的危害。



两个经典案例

- 逻辑缺陷
- 大量数据泄漏

解决方案

OWASP 中国
The Open Web Application Security Project

- 4.2 半自动式漏洞分析：业务重放、url镜像，高覆盖度

- **局限**

① 时间滞后/token: 流量重发时，不一定能100%重现当时的业务流程及出现的bug。

② 依然难以覆盖100%的业务链接，存在孤岛页面。（正常数据流不触发）

③ 漏洞检测（防御）技术滞后于攻击技术，无法解决0day漏洞

- **解决方法：引入全被动式漏洞分析**

解决方案

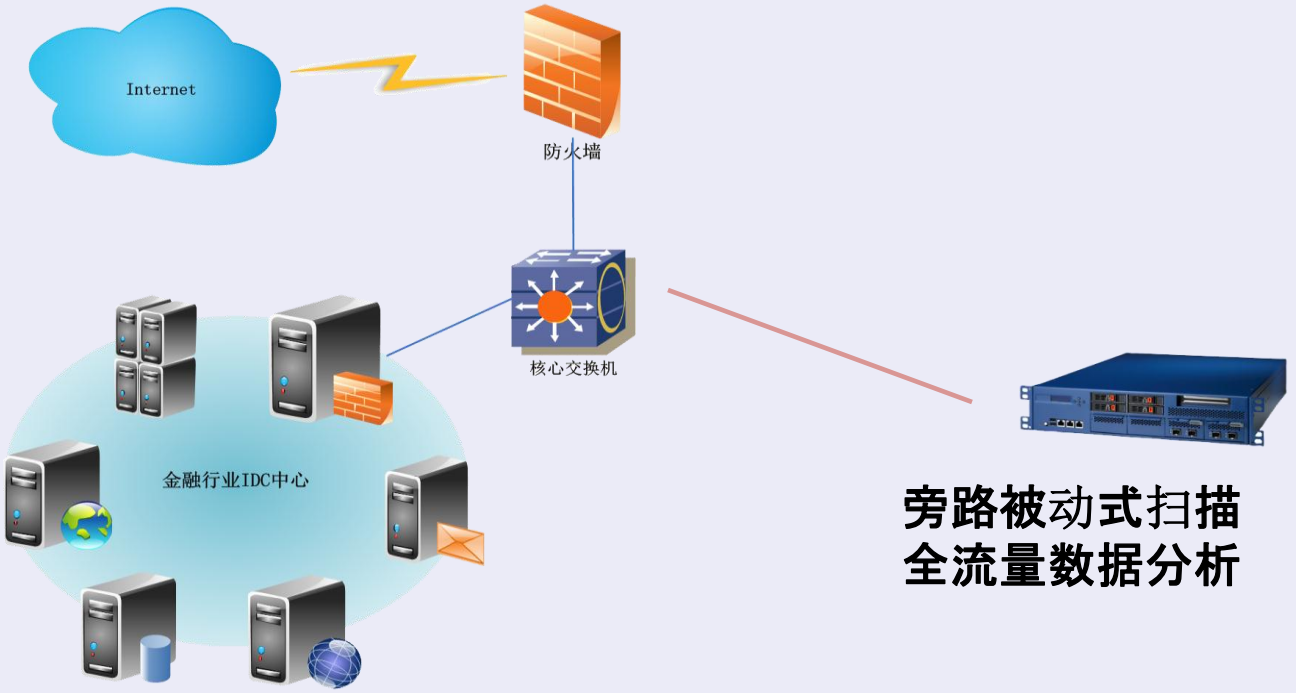
OWASP 中国
The Open Web Application Security Project

- 4.3 全被动式漏洞分析：

国外产品：Nessus PVS被动扫描

Nessus® vulnerability scanner

PVS passive vulnerability scanner™



旁路被动式扫描
全流量数据分析

解决方案

OWASP 中国
The Open Web Application Security Project

- 4.3 全被动式漏洞分析(不发送任何数据包)

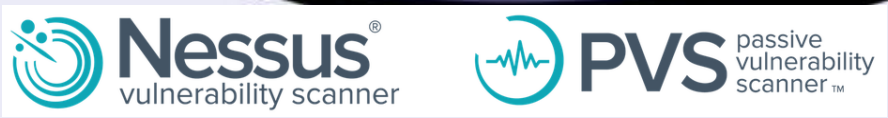
- 全被动式扫描VS主动式漏洞扫描器

相同点:都是根据双向数据包的内容，判断漏洞是否存在

不同点:

检测方式:被动式扫描不需要联网，不会主动发出url请求，也不发出任何数据包

解决方案



PVS和IDS的区别：

- 更关注漏洞感知，而不是入侵，如页面出现sql错误信息，可触发pvs报警，但不会触发ids报警。
- 报警结果不一样：pvs按照漏洞的风险等级，ids按照黑客的攻击手段报警
- 双向分析数据报文
- 更关注于web应用，OWASP TOP10的攻击手段
- 按攻击影响报警（分析双向报文），而不是按攻击手段去报警（分析单向报文）

解决方案

- Nessus的PVS只是一个思路，它专注及网络及主机漏洞，对Web应用的检测能力有限。我们需要重新设计一个针对web的PVS出来:WebPVS

解决方案

OWASP 中国
The Open Web Application Security Project

- WebPVS的优点：

- 虽然依然难以覆盖100%的业务链接，但是能覆盖100%已经发生的业务链接。
- 能与黑客同步发现各种漏洞
- 由于HTTP协议是固定，因此能够根据回包情况发现0day攻击。

OWASP 中国
The Open Web Application Security Project

总结:

- 我们介绍了金融行业的安全现状，并简单介绍了三个漏洞挖掘的思路
- 希望大家能建立起一套系统的、全面的漏洞扫描、漏洞挖掘方法。

OWASP 中国
The Open Web Application Security Project

请各位专家批评指正

谢谢