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

OWASP 中国
The Open Web Application Security Project

- 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

金融行业安全现状

OWASP 中国
The Open Web Application Security Project

- 2014年经国内安全监管机构研究发现：
- 154家银行的官方网站，发现35家存在高危漏洞，占总数的23%；35家存在中危漏洞，占比23%。
- 存在中危及高危漏洞的银行数量占检测总数比为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

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

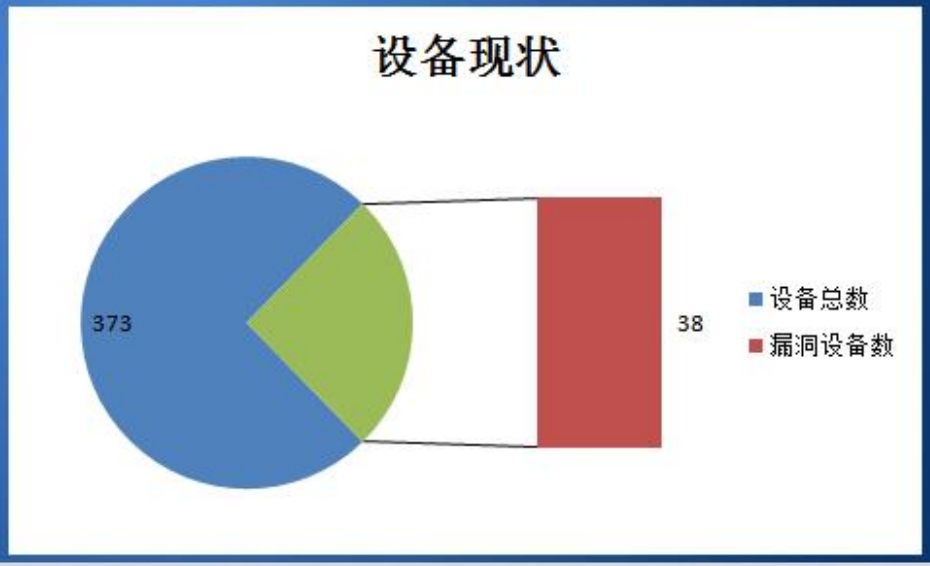
厂商分布

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



金融行业安全现状

- 问题根源

一.漏洞动态增加

新产品、新技术迭代加速，新的安全漏洞随时可能出现。每一项新产品、新技术，都可能带来新的安全威胁；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漏洞

问题根源

- 问题根源

二.攻击技术持续进化

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

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- **现有解决方案缺陷**
- 一.依赖防火墙解决？防护手段滞后

现有的应用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。

性能限制：防火墙延迟不能超过100毫秒，意味着难以进行复杂的双向数据流分析。

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- 现有解决方案缺陷
- 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：
- 需要登录系统
- 移动app的接口
- 具备复杂的交互逻辑的应用

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- 现有解决方案缺陷
- 三.依赖安全检测服务？

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。

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- 现有解决方案缺陷
- 四.不可预知的风险

- 网络环境变更
- 由于业务需求，仓促上线新的应用
- 新人在研发、运维上未遵守规范
- ……

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- 现**有解决方案缺陷**
- 五.技术局限:0Day

防御(检测)技术 在时间上 滞后于攻击技术。

现有解决方案缺陷

OWASP 中国
The Open Web Application Security Project

- 现有解决方案缺陷
- 五.技术局限:0Day

防御(检测)技术 在时间上落后于攻击技术。

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. 现有解决方案缺陷

- 4. 三位一体的解决方案
- 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

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
- 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
- 关注Web2.0自动交互 — 处理页面交互
- 防火墙绕过

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，70%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+高覆盖度

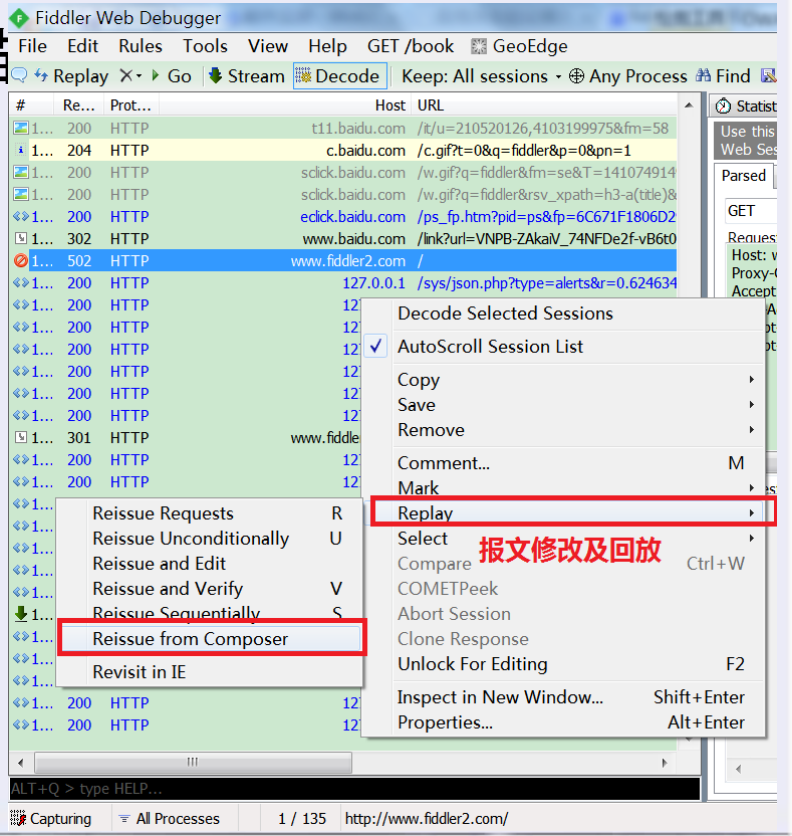
- 方法一：

- 测试过程 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

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

OWASP 中国
The Open Web Application Security Project

- 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

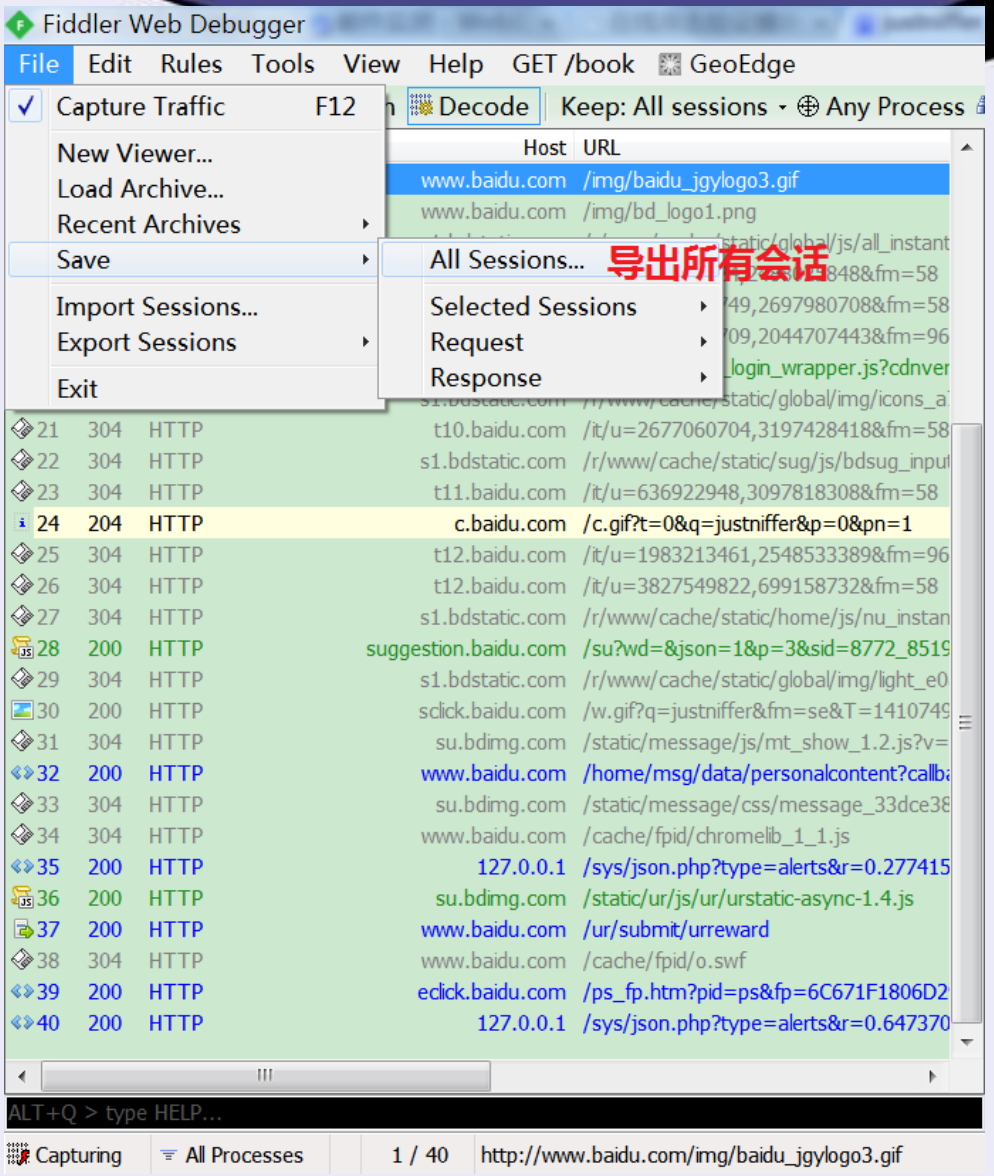
1. Fiddler的Url日志
2. 获取Apache、Nginx、Tomcat的access日志
3. 从旁路镜像中提取url日志（安全人员不用再被动等待应用的上线通知）

百度安全团队从2009起，从旁路镜像中获取url列表，高效地检出大量的漏洞。

解决方案

OWASP 中国
The Open Web Application Security Project

1. 从Fiddler2导出Url日志



解决方案

OWASP 中国
The Open Web Application Security Project

2.获取Apache、Nginx、Tomcat的access日志

Splunk：

splunk 安全

splunk_百度百科

Splunk 是机器数据的引擎。使用 Splunk 可收集、索
用程序、服务器和设备（物理、虚拟和云中）生成的
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是一
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、仪表盘以及
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：360鹰眼、jnstniffer等

360鹰眼

- 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:

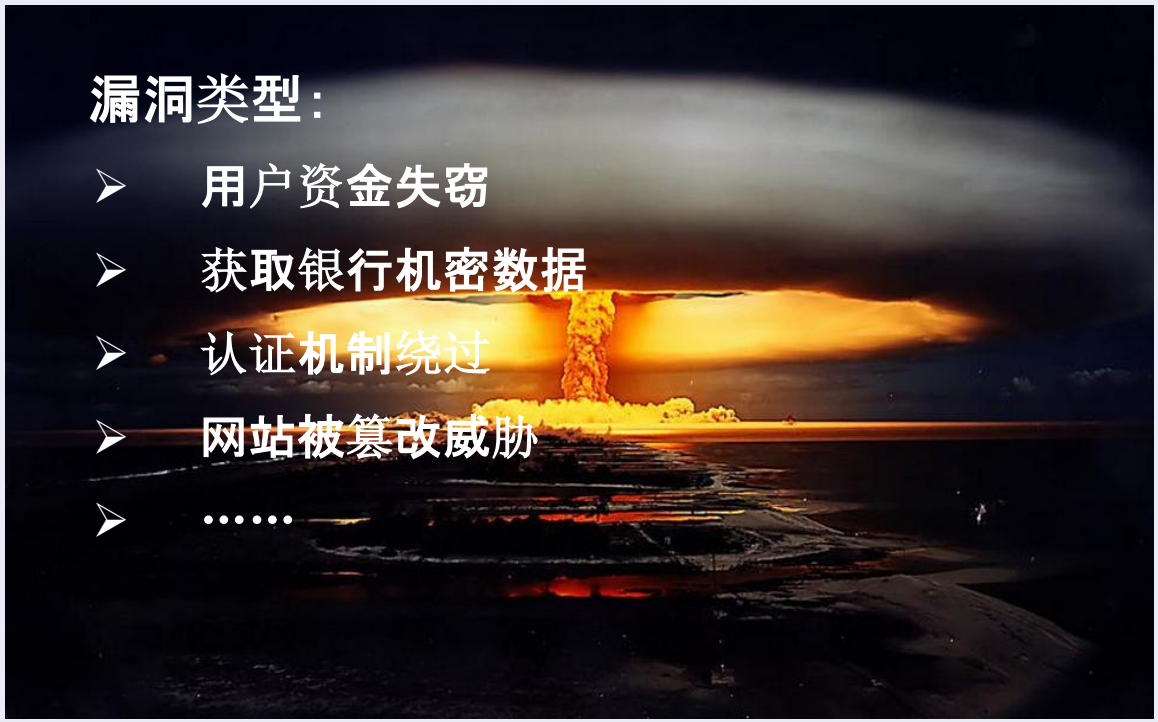
```
192.168.2.2 - - [15/Apr/2009:17:19:57 +0200] "GET /sflogo.php?group_id=205860&type=2 HTTP/1.1" 200 0 "" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko/2009032711 Ubuntu/8.10 (intrepid) Firefox/3.0.8)"

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)"
```

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+高覆盖度

- 局限
- 流量重发时，不一定能100%重现当时的业务流程及出现的bug。
- 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）
- 漏洞检测（防御）技术滞后于攻击技术，无法解决

- **解决方法：引入全被动式漏洞分析**

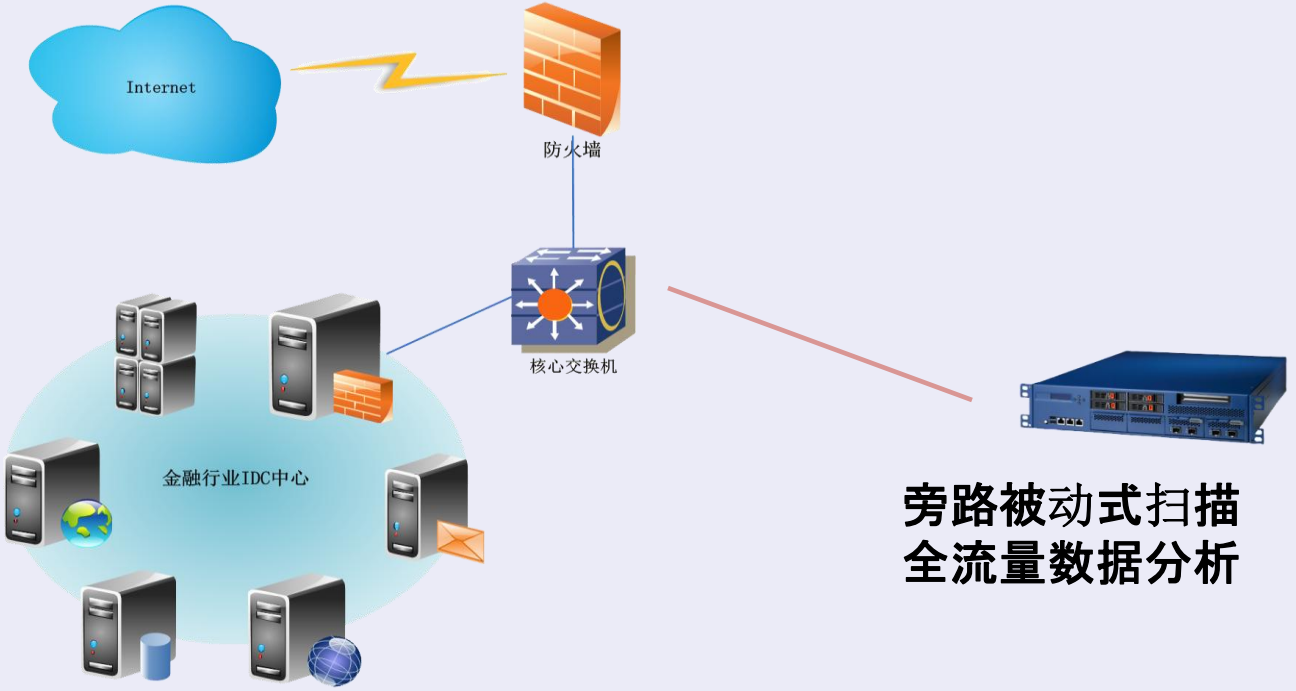
解决方案

- 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™

- 运行模式：类似IDS，但更关注Web应用及漏洞感知，而不是黑客攻击。



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

OWASP 中国
The Open Web Application Security Project

- 4.3 全被动式扫描：不发送任何数据包

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

请各位专家批评指正

谢谢