- weblogic漏洞
  - 任意文件上传
  - XML解析器反序列化漏洞
  - 反序列化漏洞
  - 未授权命令执行漏洞
- tomcat漏洞
  - 任意文件写入
  - 远程代码执行
  - 文件包含漏洞
  - 反序列化
  - war远程部署
- sql注入常见方式
  - union联合查询
  - 报错注入
  - 布尔盲注
  - 时间盲注
- log4j2的特征
- 任意文件上传的绕过
- windows应急----日志
- shiro特征
  - shiro 550和721
- struts2特征
- 宽字节注入原理
- 蚁剑特征
- 冰蝎特征
  - 2.0
  - 3.0
  - 4.0
- 哥斯拉特征
- 菜刀特征
- CS流量特征
- 文件上传
  - 攻击如何从流量层面判定上传成功
- java内存马和分类
- 应急响应
- DNSlog
  - 如何判断DNSlog外带是否成功
- 水坑攻击
- 钓鱼邮件
  - 钓鱼反制
- XXE----XML外部实体注入
- 破壳漏洞
- Redis未授权访问漏洞----6379端口
- XSS----跨站脚本攻击
- 日志地址
  - windows
  - linux
- 定时任务
  - windows
  - linux

weblogic漏洞

weblogic是java中间件，端口7001

任意文件上传

管理端未授权的两个页面存在任意上传jsp文件漏洞，进而获取服务器权限

XML解析器反序列化漏洞

weblogic的一个组件对外提供webservice服务，其中使用了XML解析器来解析用户传入的XML数据，在解析的过程中出现反序列化漏洞，导致可执行任意命令

反序列化漏洞

T3协议在开放WebLogic控制台端口的应用上默认开启，攻击者可以通过T3协议发送恶意的的反序列化数据，对存在漏洞的组件进行远程代码执行

未授权命令执行漏洞

未经身份验证的远程攻击者可能通过构造特殊的 HTTP GET请求，执行任意代码

tomcat漏洞

任意文件写入

因配置文件配置不当（非默认），导致可以使用PUT方法上传任意文件，但限制了jsp后缀的上传

远程代码执行

和一个java文件有关，在windows下存在这个漏洞

文件包含漏洞

Tomcat AJP协议设计上存在缺陷，导致可以读取或包含Tomcat上所有webapp目录下的任意文件

反序列化

使用了tomcat提供的session持久化功能，在会话中尝试读取session文件中的内容，进行反序列化

war远程部署

默认进入后台的密码为tomcat/tomcat，未修改造成未授权即可进入后台。有一个上传war包的地方

sql注入常见方式

union联合查询

报错注入

函数：floor()、updatexml()、extractvalue()

布尔盲注

函数：length()、substr()、ascii()

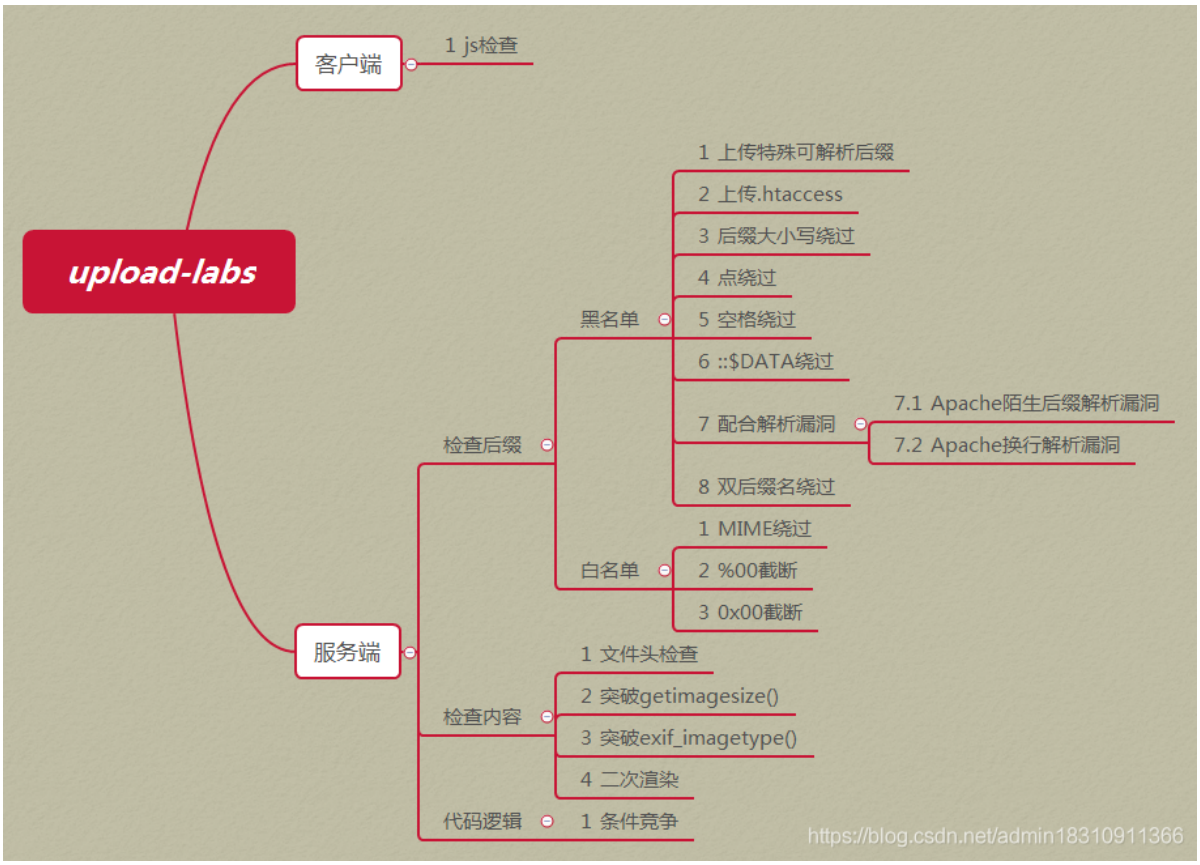
时间盲注

函数：sleep()

log4j2的特征

payload中有jndi和ldap

任意文件上传的绕过



windows应急----日志

系统日志、安全日志、应用程序日志

事件查看器

事件IP：

1. 4624----登录成功

   4625----登录失败

   4634----注销成功

   4647----用户启动的注销，当用户远程登陆，并注销时，会发生此事件

   4672----使用管理员进行登录

   4720----新建用户

   4724----更改账户密码

   4726----删除用户

登录类型：

1. 2----交互式登录

   3----网络

   4----批处理

   5----服务启动（服务登录）

   6----不支持

   7----解锁

   8----网络明文（IIS服务器登录验证）

   10----远程交互

   11----缓存域证书登录

shiro特征

返回包中有rememberMe=deleteMe字段

返回包中存在base64编码数据

shiro 550和721

struts2特征

基于java开发的框架，大多数是远程命令执行

url中会出现的特征：`.action`

请求头中有id=，context

payload解码后有%和{ }

宽字节注入原理

mysql使用GBK编码后，两个字符的前一个字符ASCII码大于128时，会将两个字符认成一个汉字

蚁剑特征

1. 加密后参数名以_0x开头，是base64加密
2. 请求体只是经过 url 编码，特征为ini_set("display_errors","0")

冰蝎特征

2.0

1. 十几个User-Agent头，每次请求时会随机选择其中的一个。如果发现一个ip的请求头中的user-agent在频繁变换，可能就是冰蝎
2. Accept值每个阶段都一样

3.0

1. content-type字段常见为application/octet-stream
2. 16个User-Agent头，每次请求时会随机选择其中的一个。如果发现一个ip的请求头中的user-agent在频繁变换，可能就是冰蝎
3. 长连接
4. 较长的base64编码请求包

4.0

1. 弱特征
    1. Content-type: Application/x-www-form-urlencoded
    2. Accept: application/json, text/javascript
2. 10种User-Agent,每次连接shell时会随机选择一个进行使用
3. 本地端口在49700左右，每连接一次，每建立一次新的连接，端口就依次增加
4. 默认使用长连接，请求头和响应头都有Connection: Keep-Alive
5. 默认连接密码rebeyond，密钥为连接密码32位md5值的前16位

哥斯拉特征

1. 请求包含pass=
2. user-agent,如果不修改的话会返回使用的jdk信息
3. Accept为text/html, image/gif, image/jpeg
4. 请求包的Cookie中最后出现分号
5. 响应包数据：md5前十六位+base64+md5后十六位

菜刀特征

1. payload在请求体中，采用url编码+base64编码，payload部分是明文传输
2. payload中有eval或assert、base64_decode这样的字符

CS流量特征

1. 下发指令：请求头中有id=
2. UA头：4.0版本的UA头是固定的，4.5及以上则会随机生成
3. 心跳包特征：间隔一定时间就会通信，请求包数据长度固定
4. ja3和ja3s：ja3和操作系统有关，ja3s和三次握手有关

文件上传

1. 服务器端后端未对上传的文件进行严格的验证和过滤，就可能造成上传恶意文件

攻击如何从流量层面判定上传成功

全流量设备有没有异常外连，上传了shell要用工具连接

java内存马和分类

1. 客户端发起的web请求会依次经过Listener、Filter、Servlet三个组件，在请求的过程中，在内存中修改已有的组件或者动态注册一个新的组件，插入恶意代码
2. 分类
    1. 细分
        1. web应用型
            1. Servlet-API 实现的动态注册内存马
        2. 框架型
        3. 中间件型
        4. agent型
        5. 其他型
    2. 大致分
        1. servlet-api型
        2. 字节码增强型

应急响应

DNSlog

dns日志，在域名解析的时候会留下域名和解析IP的记录

如何判断DNSlog外带是否成功

1. 原理
    1. 把信息放在高级域名中，传递到自己这，然后读取日志，获取信息

       通俗：通过DNS请求后，通过读取日志来获取我们的请求信息
2. 源ip与dnslog是否有外联日志

水坑攻击

攻击者观察受害者经常访问的网站，攻击网站之后，在网站上部署恶意程序，当受害者访问到时会被感染，从而获得受害者公司网络的访问权

钓鱼邮件

1. 邮件内容涉及域名、IP均都应该进行屏蔽
2. 对访问钓鱼网站的内网IP进行记录，以便后续排查溯源可能的后果

钓鱼反制

对邮件内的链接进行查询，whois，天眼ioc，附件在沙盒进行分析

1. 根据钓鱼邮件发件人进行日志回溯
2. 通知已接收钓鱼邮件的用户进行处理
    1. 删除钓鱼邮件
    2. 系统改密
    3. 全盘扫毒

XXE----XML外部实体注入

1. 应用程序解析XML输入时，没有禁止外部实体的加载，导致可加载恶意外部文件
2. 特征
    1. 请求包有<?xml，说该站点在使用XML技术，可能是base64编码
    2. 配置错误会可以导致强制应用程序解析XML数据
        1. 修改content-type头，强制输入xml格式的数据
3. 绕过
    1. 抓包改content-type为，text/xml 或者 application/xml
4. 防御
    1. 直接禁用外部实体
    2. 黑名单过滤(不推荐)过滤诸注入必须的关键词

破壳漏洞

1. 允许攻击者通过环境变量执行任意命令
2. 通过 echo bash，让系统执行命令，echo相当于python里的print，print输出什么内容，系统就执行什么内容

Redis未授权访问漏洞----6379端口

1. 没有设置密码（一般密码为空）或者密码为弱密码的情况下，没有进行有效保护措施，处于公网的redis服务就会被任意的用户未授权访问
2. 防御
    1. 修改redis.conf文件
    2. 加强redis访问密码
    3. 修改默认端口

XSS----跨站脚本攻击

1. 攻击者往 Web 页面里插入恶意脚本代码，当用户浏览该页时，嵌入 Web 里的脚本代码就会被执行
2. 分类
    1. 存储型xss漏洞----持久型XSS
        1. 把用户输入的数据存储到数据库，并显示到前端页面。攻击者可进行身份验证盗取

2. 数据会经过服务器端，会到达数据库，输入一次攻击代码会攻击多次
3. 攻击代码会直接存放到数据库

2. 反射型XSS漏洞----非持久型XSS
    1. 把用户输入的数据“反射”给浏览器。攻击者诱使用户“点击”恶意链接，就能攻击成功
    2. 数据会经过服务器端，不会到达数据库，输入一次攻击代码只会攻击一次
    3. 攻击代码输入后，在后端会直接输出到前端被触发
3. DOM型XSS----特殊的反射型XSS
    1. 输入的恶意代码不会经过服务器，在前端被js代码直接读取放置到前端的标签中
    2. 数据不会经过服务器端，不会到达数据库，输入一次攻击代码只会攻击一次

日志地址

windows

c盘windows/System32/winevt/Logs下

linux

定时任务

windows

计算机管理-->系统工具-->任务计划程序

linux

crontab

1. 命令
    1. 查看当前用户的：-l
    2. 查看指定用户的：-l -u 用户
    3. 删除当前的定时任务：-r
    4. 新增或编辑定时任务：-e