

- 1、JNI 函数在 java 中函数名为 com.didi.security.main,C 中的函数名是什么样的?  
com\_didi\_security\_mian          java.com.didi.security.main
- 2、Frida 和 Xposed 框架?
- 3、SSRF 利用方式?
- 4、宏病毒?
- 5、APP 加壳?
- 6、勒索软件 Wanacry 的特征?    蠕虫、僵尸病毒
- 7、ARM32 位指令中, 返回值和返回地址保存在哪个寄存器中?
- 8、HTTPS 握手过程中用到哪些技术?
- 9、Linux 中 PHP 环境, 已知 disable\_functions=exec,passthru,popen,proc\_open,shell\_exec,system, 请写出两种有可能实现任意命令执行的方式?
- 10、Android APP 逆向分析步骤一般是怎么样的?

一开始会问问你在工作中负责的是什么工作（如果在职），参与过哪些项目。还有些会问问你之前有没有护网的经历，如果没有的话一般都会被定到初级（技术特牛的另说）。下面就是一些技术上的问题了

#### 11、sql 注入 的分类?

Boolean 盲注、Union 注入、文件读写、报错注入{ floor 报错注入、ExtractValue 报错注入、UpdateXml 报错注入}  
、时间盲注、REGEXP 正则匹配、宽字节注入、堆叠注入、二次注入、User-Agent 注入、Cookie 注入、过滤绕过、万能密码

#### 12、sql 注入的预防?

预编译

PDO

正则表达式过滤

#### 13、序列化与反序列化的区别

序列化：把对象转化为可传输的字节序列过程称为序列化。

反序列化：把字节序列还原为对象的过程称为反序列化。

#### 14、常见的中间件漏洞?

IIS

PUT 漏洞、短文件名猜解、远程代码执行、解析漏洞

Apache

解析漏洞、目录遍历

Nginx

文件解析、目录遍历、CRLF 注入、目录穿越

Tomcat

远程代码执行、war 后门文件部署

JBoss

反序列化漏洞、war 后门文件部署

WebLogic

- 反序列化漏洞
- SSRF 任意文件上传
- war 后门文件部署
- Apache Shiro 反序列化漏洞
- Shiro rememberMe (Shiro-550)
- Shiro Padding Oracle Attack(Shiro-721)

#### 15、内网渗透思路？

- 代理穿透
- 权限维持
- 内网信息收集
- 口令爆破
- 凭据窃取
- 社工
- 横行和纵向渗透
- 拿下域控

#### 16、OWASP Top10 有哪些漏洞

- SQL 注入
- 失效的身份认证
- 敏感数据泄露
- XML 外部实体 (XXE)
- 失效的访问控制
- 安全配置错误
- 跨站脚本 (XSS)
- 不安全的反序列化
- 使用含有已知漏洞的组件
- 不足的日志记录和监控

#### 17、正向代理和反向代理的区别

正向代理，当客户端无法访问外部资源的时候（比如 Google、YouTube），可以通过一个正向代理去间接地访问。

正向代理是一个位于客户端和原始服务器(origin server)之间的服务器，为了从原始服务器取得内容，客户端向代理

发送一个请求并指定目标(原始服务器)，然后代理向原始服务器转交请求并将获得的内容返回给客户端。

反向代理，客户端是无感知代理的存在，以代理服务器来接受 internet 上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给 internet 上请求连接的客户端。此时代理服务器对外就表现为一个服务器。

#### 18、蚁剑/菜刀/C 刀/冰蝎的相同与不相同之处

- 相同：都是用来连接 Web Shell 的工具
- 不同：相比于其他三款，冰蝎有流量动态加密

#### 19、正向 SHELL 和反向 SHELL 的区别

正向 Shell：攻击者连接被攻击者机器，可用于攻击者处于内网，被攻击者处于公网的情况。

反向 Shell：被攻击者主动连接攻击者，可用于攻击者处于外网，被攻击者

处于内网的情况。

正向代理即是客户端代理，代理客户端，服务端不知道实际发起请求的客户端。

反向代理即是服务端代理，代理服务端，客户端不知道实际提供服务的服务端

## 20、Windows 提权

提权可分为纵向提权与横向提权：

纵向提权：低权限角色获得高权限角色的权限；

横向提权：获取同级别角色的权限。

## 21、Windows 常用的提权方法

系统内核溢出漏洞提权

数据库提权

错误的系统配置提权

组策略首选项提权

WEB 中间件漏洞提权

DLL 劫持提权

滥用高危权限令牌提权

第三方软件/服务提权等

## 22、Linux 提权有哪些方法

Linux 内核漏洞提权

低权限用户目录下可被 Root 权限用户调用的脚本提权（SUID）

环境变了劫持高权限程序提权

sudoer 配置文件错误提权

## 23、数据库有哪些，关系型的和非关系型的分别是哪些关系型

MySQL: 3306

SQL Server: 1433

Oracle: 1521

DB2: 5000

MongoDB: 27017

### 非关系型

Redis: 6379

Memcached: 11211

## 24、PHP 反序列化

### PHP 代码执行的危险函数

call\_user\_func()

call\_user\_func\_array()

create\_function()

array\_map()

### PHP 命令执行函数

system

shell\_exec  
passthru  
exec  
popen  
proc\_open  
putenv  
assert



安全入门到进阶学习资料

安全入门到进阶电子书籍

安全入门到放弃思维脑图

加微信获取 备注：PDF

---