100 多套 HW+安全岗位面试题合集

收集整理：潇湘信安（3had0w）　　整理时间：2023 年 4 月

注：资源均收集整理自网络，如有侵权请联系删除！！！

2023 年 HW 马上就要开始了，抽空将网上大家发的各大厂商 HW 面试题整理了下，共搜集 20 几份 HW 面试题，涉及十余家 HW 厂商，部分有答案，也做了些补充。

另外还搜集整理了近 100 份网络安全岗位面试题，适合准备从事安全/攻防研究员、安全服务/渗透测试/红队攻防工程师等岗位的师傅，用于查漏补缺、巩固知识短板。

这份文档算是一个简单的汇总吧，以后可能也会不定期更新，如果各位师傅有补充的面试题也可以联系我（WX：S_3had0w），最后祝大家都能找到一份满意的工作。

目录

扫码关注潇湘信安

加我微信私下交流

一、天融信

天融信-1

1、HW 经历（取得的成果）、主要负责什么
实话实说：不然就编

2、溯源和应急（参考 GitHub 上应急响应思维导图）
通常看日志记录情况，日志详细的情况，ip、时间、事件(恶意流量或者恶意访问日志)、作用，被攻击的地方即使修复，清理后门
https://mp.weixin.qq.com/s/SHfN5UpMaaayOIDBwmf5yQ

3、擅长 web 还是内网，然后谈谈
实话实说

天融信-2

1、谈谈 HW 经历
实话实说
2、谈谈挖洞和渗透印象较深的两次，过程、方法，获取了什么权限
3、谈谈内网流量如何出来
https://www.cnblogs.com/Xy--1/p/13475299.html
4、使用过哪些溯源平台
微步情报中心等

二、漏洞盒子

1、印象最深的渗透经历，技术关键点
答：（根据自己经历，讲重点）

2、是否在漏洞平台有提交过漏洞，以及排名情况
答：实话实说

3、平时挖洞的情况，平台提交漏洞和渗透测试方面
答：实话实说

三、长亭

长亭-1

1、谈谈作为蓝队护网过程使用过厂商的设备，
建议去了解一些各大厂商的设备，比如蜜罐，态势感知等

2、如何查看系统内存 shell

先判断是通过什么方法注入的内存马，可以先查看 web 日志是否有可疑的 web 访问日志，如果是 filter 或者 listener 类型就会有大量 url 请求路径相同参数不同的，或者页面不存在但是返回 200 的，查看是否有类似哥斯拉、冰蝎相同的 url 请求，哥斯拉和冰蝎的内存马注入流量特征与普通 webshell 的流量特征基本吻合。通过查找返回 200 的 url 路径对比 web 目录下是否真实存在文件，如不存在大概率为内存马。如在 web 日志中并未发现异常，可以排查是否为中间件漏洞导致代码执行注入内存马，排查中间件的 error.log 日志查看是否有可疑的报错，根据注入时间和方法根据业务使用的组件排查是否可能存在 java 代码执行漏洞以及是否存在过 webshell，排查框架漏洞，反序列化漏洞。
详细：https://www.cnblogs.com/lcxblogs/articles/15238924.html

3、Linux 的登录日志查看文件
linux 日志文件说明

```
/var/log/message  系统启动后的信息和错误日志，是 Red Hat Linux 中最常用的日志之一
/var/log/secure  与安全相关的日志信息
/var/log/maillog  与邮件相关的日志信息
/var/log/cron  与定时任务相关的日志信息
/var/log/spooler  与 UUCP 和 news 设备相关的日志信息
/var/log/boot.log  守护进程启动和停止相关的日志消息
/var/log/wtmp  该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件
```

4、获得文件读取漏洞，通常会读哪些文件，Linux 和 windows 都谈谈
敏感信息配置文件

Windows：

```
C:\boot.ini  //查看系统版本
C:\Windows\System32\inetsrv\MetaBase.xml  //IIS 配置文件
C:\Windows\repair\sam  //存储系统初次安装的密码
C:\Program Files\mysql\my.ini  //Mysql 配置
C:\Program Files\mysql\data\mysql\user.MYD  //Mysql root
C:\Windows\php.ini  //php 配置信息
C:\Windows\my.ini  //Mysql 配置信息
```

Linux：

```
/root/.ssh/authorized_keys  //如需登录到远程主机，需要到.ssh 目录下，新建 authorized_keys，并 id_rsa.pub 内容复制进去
/root/.ssh/id_rsa  //ssh 私钥，ssh 公钥是 id_rsa.pub
/root/.ssh/id_ras.keystore  //记录每个访问计算机用户的公钥
/root/.ssh/known_hosts  //ssh 会把每个访问过计算机的公钥(public key)都记录在~/.ssh/known_hosts。当下次访问相同计算机时，OpenSSH 会核对公钥。如果公钥不同，OpenSSH 会发出警告，  避免你受到 DNS Hijack 之类的攻击。
/etc/passwd  // 账户信息
/etc/shadow  // 账户密码文件
/etc/my.cnf  //mysql 配置文件
/etc/httpd/conf/httpd.conf  // Apache 配置文件
/root/.bash_history  //用户历史命令记录文件
/root/.mysql_history  //mysql 历史命令记录文件
/proc/self/fd/fd[0-9]*(文件标识符)
/proc/mounts  //记录系统挂载设备
/porc/config.gz  //内核配置文件
/var/lib/mlocate/mlocate.db  //全文件路径
/porc/self/cmdline  //当前进程的 cmdline 参数
```

长亭-2

1、谈谈 IDS 和 IPS

https://zhuanlan.zhihu.com/p/96942352

2、php 和 Java　反序列化的原理
https://www.jianshu.com/p/4060bb2e24cb
https://blog.csdn.net/weixin_44677409/article/details/93884388

3、谈谈自己常用的中间件漏洞
https://blog.csdn.net/bylfsj/article/details/102683791

4、Windows 和 Linux 的系统日志文件放在哪里
答：一、Windows 系统日志：事件查看器，Windows 系统日志都是在“事件查看器”下面的。我的电脑->右键管理->计算机管理->系统工具->事件查看器-> Windows 日志；

二、Linux 系统日志：/var/log

长亭-红队

面试难度：中
面试感受：由于面试习惯了，面试不带紧张。面试的攻击手法其实也就这些，懂了就 ok！

问：打点一般会用什么漏洞
答：优先以 java 反序列化这些漏洞像 shiro，fastjson，weblogic，用友 oa 等等进行打点，随后再找其他脆弱性易打进去的点。因为 javaweb 程序运行都是以高权限有限运行，部分可能会降权。

问：平常怎么去发现 shiro 漏洞的
答：登陆失败时候会返回 rememberMe=deleteMe 字段或者使用 shiroScan 被动扫描去发现

完整：
1.未登陆的情况下，请求包的 cookie 中没有 rememberMe 字段，返回包 set-Cookie 里也没有 deleteMe 字段
2.登陆失败的话，不管勾选 RememberMe 字段没有，返回包都会有 rememberMe=deleteMe 字段
3.不勾选 RememberMe 字段，登陆成功在返回包 set-Cookie 会有 rememberMe=deleteMe 字段，但是之后的所有请求中 Cookie 都不会有 rememberMe 字段
4.勾选 RememberMe 字段，登陆成功的话，返回包 set-Cookie 会有 rememberMe=deleteMe 字段，还会有 rememberMe 字段，之后的所有请求中 Cookie 都会有 rememberMe 字段

问：shiro 有几种漏洞类型
答：shiro 550、shiro 721

问：weblogic 权限绕过有没有了解
答：好像是用./进行绕过的
https://blog.csdn.net/weixin_45728976/article/details/109512848

问：fastjson 漏洞利用原理
答：在请求包里面中发送恶意的 json 格式 payload，漏洞在处理 json 对象的时候，没有对@type 字段进行过滤，从而导致攻击者可以传入恶意的 TemplatesImpl 类，而这个类有一个字段就是_bytecodes，有部分函数会根据这个_bytecodes 生成 java 实例，这就达到 fastjson 通过字段传入一个类，再通过这个类被生成时执行构造函数。
具体：https://www.cnblogs.com/hac425/p/9800288.html

问：weblogic 有几种漏洞
weblogic 就好多了，基于 T3 协议的反序列化；基于 xml 解析时候造成的反序列化，还有 ssrf，权限绕过等等

问：IIOP 听说过吗，和什么类似
java RMI 通信，也就是远程方法调用，默认是使用 jrmp 协议，也可以选择 IIOP。

问：这几个漏洞不出网情况下怎么办
答：让这几个漏洞回显

问：拿到 webshell 不出网情况下怎么办
答：reg 上传去正向连接，探测出网协议，如 dns，icmp

问：dns 出网协议怎么利用
答：将域名解析指向自己的 vps，然后设置 ns 记录等等，不记得了

问：横向渗透命令执行手段
答：psexec，wmic，smbexec，winrm，net use 共享+计划任务+type 命令

问：psexec 和 wmic 或者其他的区别
答：psexec 会记录大量日志，wmic 不会记录下日志。wmic 更为隐蔽

问：Dcom 怎么操作？
答：通过 powershell 执行一些命令，命令语句比较复杂，不记得了

问：抓取密码的话会怎么抓
答：procdump+mimikatz 转储然后 mimikatz 离线读取，Sam 获取然后离线读取

问：什么版本之后抓不到密码
答：windows server 2012 之后（具体我也忘记了）

问：抓不到的话怎么办
答：翻阅文件查找运维等等是否记录密码。或者 hash 传递、或者获取浏览器的账号密码等等。

问：域内攻击方法有了解过吗
答：MS14-068、Roasting 攻击离线爆破密码、委派攻击，非约束性委派、基于资源的约束委派、ntlm relay

问：桌面有管理员会话，想要做会话劫持怎么做
答：提权到 system 权限，然后去通过工具，就能够劫持任何处于已登录用户的会话，而无需获得该用户的登录凭证。

终端服务会话可以是连接状态也可以是未连接状态（这里当时没答上来，觉得有点鸡肋。我也不知道是不是这个意思）

四、安恒

1、基础漏洞
十大漏洞讲讲

(1) 注入
(2) 失效的身份认证和会话管理(使用别人会话 id,包含身份信息信用卡)
(3) XSS 跨站（存储、反射、dom）
(4) 不安全的对象直接引用(如?id=89 改成?id=90,可以看到 id=90 的信息)
(5) 伪造跨站请求（CSRF 可以在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点）
(6) 安全误配置
(7) 限制 URL 访问失败（缺少功能级访问控制）
(8) 未验证的重定向和转发
(9) 应用已知脆弱性的组件
(10) 敏感信息暴

2、溯源和应急响应
https://mp.weixin.qq.com/s/SHfN5UpMaaayOIDBwmf5yQ

五、未知厂商

1、讲一下使过的中间件漏洞
答：https://blog.csdn.net/bylfsj/article/details/102683791

2、getshell 后如何维持权限
答：https://blog.csdn.net/anquanzushiye/article/details/105502079

3、隧道、流量代理方面
答：https://www.freebuf.com/articles/web/170970.html

六、青藤

1、自我介绍
2、设备出现了误报如何处置（日志）
答：要确认设备是否误报，应当先去查看设备的完整流量日志等信息。在护网过程中如果确实存在异常流量应当及时进行上报，确认是误报后做好事件记录

3、如何查看区分是扫描流量和手动流量
答：扫描的数据量大，请求流量有规律可寻，手动流量请求少 间隔略长

4、被拿 shell 了如何处理
答：PDCERF 模型，简答排查、清除、看看可有即使修复的可能，不得已就关站

- Prepare（准备）：准备用来检测的工具和人
- 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
- 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
- Eradication（根除）
- Recover（恢复）
- 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

5、如何分析被代理出来的数据流

看特征：各个隧道之间的流量特征

https://blog.csdn.net/u012206617/article/details/114012822

七、奇安信

奇安信-1

1、请求方式几种

目前常用八种请求方式，分别是 GET、POST、HEAD、PUT、DELETE、OPTIONS、TRACE、CONNECT，get 和 post 最常用

2、域名解析记录对应工具

nslookup、万能 ping

3、web 十大漏洞

(1) 注入
(2) 失效的身份认证和会话管理(使用别人会话 id,包含身份信息信用卡)
(3) XSS 跨站（存储、反射、dom）
(4) 不安全的对象直接引用(如?id=89 改成?id=90,可以看到 id=90 的信息)
(5) 伪造跨站请求（CSRF 可以在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点）
(6) 安全误配置
(7) 限制 URL 访问失败（缺少功能级访问控制）
(8) 未验证的重定向和转发
(9) 应用已知脆弱性的组件
(10) 敏感信息暴

4、溯源和反制

溯源关键点别人挂了代理怎么办

https://mp.weixin.qq.com/s/SHfN5UpMaaayOIDBwmf5yQ

5、windows 提权

https://xz.aliyun.com/t/2519

https://www.cnblogs.com/zpchcbd/tag/特权提升/

6、Linux 提权，排查思路

看账号、进程、流量、日志、木马

7、各种函数

主要指 php 漏洞函数 serialize 和 unserialize,MD5 compare,is_numeric,extract()变量覆盖，命令执行函数 system、exec，文件包含 require()、require_once()、include()、include_once()，提权、加固、后门

8、分析日志工具

ELK，日志 IP，时间，恶意流量，攻击方式，攻击哪里

奇安信-红队

1、xss 怎么 getshell

答：1.xss 打管理员 cookie 进后台 getshell；2.xss+浏览器漏洞 getshell

2、sqlsever 怎么在 xpcmd 禁用的情况拿 shell

答：log/差异备份、sp_OACreate、sp_makewebtask 等

3、java 的所有反序列化

4、常用中间件漏洞

(一) IIS（php 中间件）

1) IIS 6 解析漏洞
2) IIS 7 解析漏洞
3) PUT 任意文件写入漏洞
4) IIS 短文件名漏洞
5) IIS 溢出漏洞
6) HTTP.SYS 远程代码执行（MS15-034）

(二) Apache（php 中间件）

1) AddHandler 解析漏洞
2) APache HTTPD 换行解析漏洞(CVE-2017-15715)
3) 未知扩展名解析漏洞
4) 目录遍历

(三) Nginx（php 中间件）

1) 配置文件错误导致的解析漏洞
2) 文件名逻辑漏洞（CVE-2013-4547）
3) 目录遍历
4) CRLF 注入
5) 目录穿越

(四) Tomcat（java 中间件）

1) 任意文件写入（CVE-2017-12615）
2) 远程代码执行（CVE-2019-0232）
3) 弱口令+war 后门文件部署

(五) jBoss

1) JBoss 5.x/6.x 反序列化漏洞（CVE-2017-12149）
2) JBoss JMXInvokerServlet 反序列化漏洞
3) JBoss EJBInvokerServlet 反序列化漏洞
4) JBoss <=4.x JBossMQ JMS 反序列化漏洞（CVE-2017-7504）
5) Administration Console 弱口令
6) JMX Console 未授权访问

（六）WebLogic（java 中间件）

1) 反序列化漏洞（CVE-2017-10271 & CVE-2017-3506）
2) wls9_async_response,wls-wsat 反序列化远程代码执行漏洞（CVE-2019-2725）
3) WLS Core Components 反序列化命令执行漏洞（CVE-2018-2628）
4) 任意文件上传漏洞（CVE-2018-2894）
5) SSRF 漏洞 （CVE-2014-4210）
6) 弱口令+后台部署 war 包 getshell

具体：https://blog.csdn.net/weixin_44288604/article/details/121568508

6、手工注入怎么写 shell

八、360

360-1

1、基础知识，注入函数，PHP 系统执行命令函数

答：sql 注入函数：https://blog.csdn.net/qq_44204058/article/details/113706867

PHP 系统执行命令函数：https://www.cnblogs.com/ps-blog/p/6944936.html

2、如何响应，溯源

上面已回答，https://mp.weixin.qq.com/s/SHfN5UpMaaayOIDBwmf5yQ

3、成功拿到系统 shell 后，你回去看哪些文件

主要是一些配置文件

360-2

1、溯源、态势感知、安全设备

2、基础的漏洞原理 ssrf xxe、Redis 几种利用方式

答：Redis 利用方式，https://www.cnblogs.com/hk-ss/p/14943691.html

答：CSRF 和 XSS 和 XXE 原理

XSS 学习：https://blog.csdn.net/weixin_39934520/category_9973431.html

XSS 是跨站脚本攻击，用户提交的数据中可以构造代码来执行，从而实现窃取用户信息等攻击。修复方式：对字符实体进行转义、使用 HTTP Only 来禁止 JavaScript 读取 Cookie 值、输入时校验、浏览器与 Web 应用端采用相同的字符编码。

CSRF 是跨站请求伪造攻击，XSS 是实现 CSRF 的诸多手段中的一种，是由于没有在关键操作执行时进行是否由用户自愿发起的确认。修复方式：筛选出需要防范 CSRF 的页面然后嵌入 Token、再次输入密码、检验 Referer.

XXE 是 XML 外部实体注入攻击，XML 中可以通过调用实体来请求本地或者远程内容，和远程文件保护类似，会引发相关安全问题，例如敏感文件读取。修复方式：XML 解析库在调用时严格禁止对外部实体的解析。

CSRF、SSRF 和重放攻击有什么区别？

- CSRF 是跨站请求伪造攻击，由客户端发起
- SSRF 是服务器端请求伪造，由服务器发起
- 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

360-3

1、谈谈工作 HW 经历
2、代码分析，根据面试方发来的代码进行分析
(1) weblogic 反序列化代码
(2) 一个 PHP 的 exp，分析哪个版本，并分析 exp 上各参数的作用

九、极盾科技

1、webshell 如何响应
PDCERF 模型

- Prepare（准备）：准备用来检测的工具和人
- 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
- 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
- Eradication（根除）
- Recover（恢复）
- 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

webshell 检测思路
https://blog.csdn.net/u011066706/article/details/51175971
webshell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。

黑客通过浏览器以 HTTP 协议访问 Web Server 上的一个 CGI 文件，是一个合法的 TCP 连接，TCP/IP 的应用层之下没有任何特征，只能在应用层进行检测。黑客入侵服务器，使用 webshell，不管是传文件还是改文件，必然有一个文件会包含 webshell 代码，很容易想到从文件代码入手，这是静态特征检测；webshell 运行后，B/S 数据通过 HTTP 交互，HTTP 请求/响应中可以找到蛛丝马迹，这是动态特征检测。

静态检测
静态检测通过匹配特征码，特征值，危险函数函数来查找 webshell 的方法，只能查找已知的 webshell，并且误报率漏报率会比较高，但是如果规则完善，可以减低误报率，但是漏报率必定会有所提高。

优点是快速方便，对已知的 webshell 查找准确率高，部署方便，一个脚本就能搞定。缺点漏报率、误报率高，无法查找 0day 型 webshell，而且容易被绕过。

静态检测配合人工

一个检查工具：https://github.com/he1m4n6a/findWebshell

动态检测

Linux 下就是 nobody 用户起了 bash，Win 下就是 IIS User 启动 cmd，这些都是动态特征。再者如果黑客反向连接的话，那很更容易检测了，Agent 和 IDS 都可以抓现行。Webshell 总有一个 HTTP 请求，如果我在网络层监控 HTTP，并且检测到有人访问了一个从没反问过得文件，而且返回了 200，则很容易定位到 webshell，这便是 http 异常模型检测，就和检测文件变化一样，如果非管理员新增文件，则说明被人入侵了。

缺点也很明显，黑客只要利用原文件就很轻易绕过了，并且部署代价高，网站时常更新的话规则也要不断添加。

日志检测

使用 Webshell 一般不会在系统日志中留下记录，但是会在网站的 web 日志中留下 Webshell 页面的访问数据和数据提交记录。日志分析检测技术通过大量的日志文件建立请求模型从而检测出异常文件，称之为：HTTP 异常请求模型检测。

语法检测

实现关键危险函数的捕捉方式

统计学检测

webshell 由于往往经过了编码和加密，会表现出一些特别的统计特征，根据这些特征统计学习。 典型的代表：NeoPI -- https://github.com/Neohapsis/NeoPI

防范 webshell

https://blog.csdn.net/nohaoye/article/details/46987587

防范的措施大概有三种，第一种的思路是将专门存放上传文件的文件夹里面的脚本类型文件，解析成其他类型的文件，服务器不会以脚本类型来执行它。第二种是匹配文件夹里的脚本类型文件，将其设置为无法读取及操作。第三种是将文件上传到一个单独的文件夹，给一个二级的域名，然后不给这个虚拟站点解析脚本的权限，听说很多网站都用这种方式。

2、系统被 shell 如何响应，Linux 被 shell 后进程命令（ps）被禁了，如果操作
答：恢复配置文件，然后执行进程查看命令，杀进程

3、拿到 shell 后，你会去看哪些文件
答：主要是一些配置文件

十、国誉网安

1、谈谈工作和 HW 经历
答：实话实说

2、谈一下现在有一台 windows server2008 如何提权
答：https://blog.csdn.net/weixin_45427650/article/details/105553105

3、windows 系统常见漏洞编号
答：ms08-067、ms12-020（3389）、ms15-034(针对 iis 中间件)、心脏滴血（还就是针对 https443 的...）、ms17-010（smb445）、震网三代（美国攻击伊朗核电站，可还记得）、CVE-2019-0708（3389）、CVE-2020-0796（445）
具体：https://www.cnblogs.com/dazhu-secure/p/13849242.html

十一、阿里

1、谈谈 OOB（利用 NETBIOS 中一个 OOB （Out of Band）的漏洞而来进行的，它的原理是通过 TCP/IP 协议传递一个数据包到计算机某个开放的端口上(一般是 137、138 和 139），当计算机收到这个数据包之后就会瞬间死机或者蓝屏现象，不重新启动计算机就无法继续使用 TCP/IP 协议来访问网络。）

2、谈谈 IDS（IntrusionDetection Systems 入侵检测系统）
答：https://zhuanlan.zhihu.com/p/96942352

4、谈谈 IDR（敏感数据发现与风险评估系统 Insightfor Discovery and Risk）
答：https://www.nsfocus.com.cn/html/2019/208_0926/21.html

HW 初级面试题

1. SQL 注入原理，函数，常见防御手段，getshell 方法
2. xss 注入原理，利用方式
3. csrf 注入原理
4. 应急响应流程
5. 渗透测试过程中安全工具使用过那些
6. 遇到木马了怎么进行排查
7. 域知识，黄金票据白银票据
8. 系统相关的问题，一些常用命令
9. 一些中间件漏洞
10. 给你一个网站如何进行渗透测试
11. linux，windows 提权手法有哪些，讲一讲
12. 挖过那些漏洞
13. 怎么学习中间件漏洞的
14. 了解过 waf 吗，说说一些绕 waf 的手段 15.文件上传漏洞绕过的方法
15. 了解过 xxe 吗?

HW 中级面试题

1. 你今年毕业了吗?
2. 你现在在 xx（在哪里）吗?
3. 我看你简历上写了你学过的一些内容，你能说下你的学习方向吗?

4. 你参加过护网吗?
5. 你参加过蓝队的护网吗?
6. 你知道哪些设备呢?
7. HFish 蜜罐是开源的，你有用过吗?
8. 你有过应急响应的经验吗?
9. 我看你简历上写着你学过内网渗透，你能说下当你拿到一台域内的主机之后，怎么进行域渗透吗?
10. 你简历上写了你会用 webshell 管理工具，蚁剑、菜刀什么的你都用过吧?
11. 能说下 webshell 管理工具的流量特征吗?
12. 问你一个最简单最基础的问题吧，内网的 IP 地址有哪些?
13. 你会用什么办法溯源攻击方的个人信息呢
14. CDn 负载均衡你知道吧?如果攻击方使用的是一个有挂了 CDn 负载均衡的服务器来攻击你，你要怎么溯源到目标的真实 IP 地址呢?
15. 你知道红队经常用于攻击的漏洞是什么吗?
16. 反序列化漏洞你了解过哪些?
17. shiro 反序列化你有复现过吗?
18. 你要怎么通过流量分析知道对方使用的 shiro 攻击是否成功呢?
19. 和甲方上报 IP 地址，你要上报哪些地址呢?
20. 怎么通过流量分析，判断出对方攻击成功了?
21. 如果攻击的回显有延迟或者说攻击生效需要一定的时间，你不能很快看见，那该怎么通过流量分析判断出攻击是否生效了?

2023 护网面试题

1、应急响应查找内容

分析服务器上的安全问题，你关注哪些数据？ 进程，日志，告警信息，威胁情报，文档编辑时间，启动项，路由管理，防火墙，最后登录时间，CPU 带宽，内存，代码安全，用户账户，隐藏文件等。

2、你有没有毕业？

已经毕业，正在工作（实习）

3、护网预计在五月份，时间问题？

没有问题

4、简历有护网经历，你能谈谈护网的情况吗

根据简历，以及掌握的知识，大胆的说，角色为防守方，工作位监控组，主要使用 ips，ids 等设备做流量监控与日志分析工作

5、你能大概说一下，比如数据包或者日志，你的分析思路是什么，以及你会用到哪些工具或者那些网站进行查询？

用流量监测的安全设备，比如天眼，查看报文，分析报文里和 host 和网站目录路径，查看是否可疑，使用微步查询 host 是否为恶意，使用 wireshark 对数据包深度分析看一下请求的网站路径，源 IP 与目的 ip 地址，host 字段的值以及发包内容等。工具有 wearshark，网站的话微步在线等

6、文件上传和命令执行，有看过相关日志吗
文件：可能在系统有上传功能或者有文本编辑器，看一下保重是否有 base64 加密或者 url 加密，解码验证一下是否有恶意代码
系统日志：有没有 web 容器做了一些危险行为，比如 bash 反弹 shell 等
网络应用日志：有没有异常的网站文件，类似 webshell 等，就有可能是命令执行

7、文件上传攻击特征？
能够上传文件的接口，应用程序对用户上传文件类型不校验或者校验不严格可绕过，导致任意类型文件上传，攻击者可上传 webshell。

8、用过 Nmap 扫描工具吗
用过，具体见信安面试，nmap 扫描基础命令

9、常见命令注入漏洞？php? Strust2 ？
见常见攻击告警分析以及 strust2 漏洞

10、你在分析数据包的时候，这个地址是一个互联网的地址，你会做一些什么样的排查或者说对 IP 地址进行什么样的处理呢？
把这个域名或者 ip 放到微步上检测一下，看一下是不是恶意链接

11、你有用过微步吗？
去了解一下微步在线

12、你做过渗透测试的工作吗？
有做过，具体看面试 50 题之 2，渗透一个网站需要步骤

13、你能说明文件上传的原理吗？
常见的攻击告警，文件上传部分

14、文件上传加固方法？
同上

15、暴力破解加固方法？
1） 添加强度较高的验证码，不易被破解。
2） 修改密码设置规则，提高用户的密码强度。
3） 同一账号登陆次数锁定，生成锁定日志。
4） 定期排查弱口令。

16、Sql 注入加固措施？
常见的攻击告警，sql 注入部分

17、你对应急和溯源有过一些了解吗？
详见：溯源的思路、文档，https://mp.weixin.qq.com/s/SHfN5UpMaaayOIDBwmf5yQ

18、一台主机在内网进行横向攻击，你应该怎么做？

确定攻击来源，是不是员工内部误操作，比如询问运维是否有自动化轮训脚本，如果没有，确定是攻击，结合时间点，根据设备信息，看一下安全事件，进程，流量，找到问题主机，开始应急响应流程：准备，检测，遏制，根除，恢复，跟踪，具体的操作要交给现场运维去处理。

19、你能说说护网的流程吗？

护网流程参考一下链接：https://zhuanlan.zhihu.com/p/536702187

20、你还用过其他态势感知的产品吗？

Ips，ids，hids，堡垒机等

21、平时 windows，linux 用的多吗，Linux 应用端口，比如常用数据库接口？

- 25：SMTP 简单邮件传输服务器端口
- 23：telnet 的端口，telnet 是一种可以远程登录并管理远程机器的服务
- 22：ssh 端口，PcAnywhere 建立 TCP 和这一端口的连接可能是为了寻找 ssh，这一服务有许多弱点
- 53：dns 端口
- 3306：MySQL 的默认端口
- 1433：SQLServer 的默认端口
- 3389：远程桌面登录
- 7001：Freak88,Weblogic 默认端口，Weblogic 是一个 application server,确切的说是一个基于 JAVAEE 架构的中间件
- 445：是一个毁誉参半的端口他和 139 端口一起是 IPC$入侵的主要通道
- 139：属于 TCP 协议，是为 NetBIOS Session Service 提供的，主要提供 Windows 文件和打印机共享以及 Unix 中的 Samba 服务

22、命令行工具用的什么比较多？

Xshell、SecureCRT、Finalshell、MobaXterm

23、应急响应流程

准备，检测，遏制，根除，恢复，跟踪，报告一般是从第二步到第五步的过程，截图等

- 准备：信息收集，工具准备
- 检测：了解资产情况，明确影响，尝试进行攻击路径溯源
- 遏制：关闭端口，服务，停止进程，拔网线
- 根除：通过杀毒软件，清除恶意文件，进程
- 恢复：备份，恢复系统正常
- 跟踪：复盘全貌，总结汇报

24、什么是跨域，JSONP 与 CORS

跨域：指的是浏览器不能执行其它网站的脚本，它是由浏览器的同源策略造成的，是浏览器的安全限制！

同源策略：域名、协议、端口均相同。浏览器执行 JavaScript 脚本时，会检查这个脚本属

于那个页面，如果不是同源页面，就不会被执行。
JSONP 跨域：只支持 GET 请求，不支持 POST 等其它请求，也不支持复杂请求，只支持简单请求。

CORS 跨域：支持所有的请求，包含 GET、POST、OPTOIN、PUT、DELETE 等。既支持复杂请求，也支持简单请求。

JSONP 与 CORS 的使用目的相同，并且都需要服务端和客户端同时支持，但 CORS 的功能更加强大。

JSONP 和 CORS 的优缺点

1) JSONP 主要优势在于对浏览器的支持较好；虽然目前主流浏览器都支持 CORS，但 IE9 及以下不支持 CORS。
2) JSONP 只能用于获取资源（即只读，类似于 GET 请求）；CORS 支持所有类型的 HTTP 请求，功能完善。
3) JSONP 只会发一次请求；而对于复杂请求，CORS 会发两次请求。

应用场景

- 如果需要兼容 IE 低版本浏览器，无疑，JSONP。
- 如果需要对服务端资源进行操作，无疑，CORS。
- 其他情况的话，根据自己的对需求的分析来决定和使用。

25、如何检测 webshell

静态检测

静态检测通过匹配特征码，特征值，危险函数函数来查找 webshell 的方法，只能查找已知的 webshell。

动态检测

webshell 传到服务器了，黑客总要去执行它吧，webshell 执行时刻表现出来的特征，我们称为动态特征。

日志检测

使用 Webshell 一般不会在系统日志中留下记录，但是会在网站的 web 日志中留下 Webshell 页面的访问数据和数据提交记录。

语法检测

语法语义分析形式，是根据 php 语言扫描编译的实现方式，进行剥离代码、注释，分析变量、函数、字符串、语言结构的分析方式，来实现关键危险函数的捕捉方式。这样可以完美解决漏报的情况。但误报上，仍存在问题。

26、三次握手与四次挥手

三次握手（three-way handshaking）

1. 背景：

TCP 位于传输层，作用是提供可靠的字节流服务，为了准确无误地将数据送达目的地，TCP 协议采纳三次握手策略。

2. 原理：

1) 发送端首先发送一个带有 SYN（synchronize）标志地数据包给接收方。

2) 接收方接收后，回传一个带有 SYN/ACK 标志的数据包传递确认信息，表示我收到了。
3) 最后，发送方再回传一个带有 ACK 标志的数据包，代表我知道了，表示’握手‘结束。

四次挥手（Four-Way-Wavehand）
1) 第一次挥手：Client 发送一个 FIN，用来关闭 Client 到 Server 的数据传送，Client 进入 FIN_WAIT_1 状态。
2) 第二次挥手：Server 收到 FIN 后，发送一个 ACK 给 Client，确认序号为收到序号+1（与 SYN 相同，一个 FIN 占用一个序号），Server 进入 CLOSE_WAIT 状态。
3) 第三次挥手：Server 发送一个 FIN，用来关闭 Server 到 Client 的数据传送，Server 进入 LAST_ACK 状态。
4) 第四次挥手：Client 收到 FIN 后，Client 进入 TIME_WAIT 状态，接着发送一个 ACK 给 Server，确认序号为收到序号+1，Server 进入 CLOSED 状态，完成四次挥手

27、http 状态与无连接
(1) 无连接
1) 每一个访问都是无连接，服务器挨个处理访问队列里的访问，处理完一个就关闭连接，这事儿就完了，然后处理下一个新的
2) 无连接的含义是限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接

(2) 无连接
1) 协议对于事务处理没有记忆能力
2) 对同一个 url 请求没有上下文关系
3) 每次的请求都是独立的，它的执行情况和结果与前面的请求和之后的请求是无直接关系的，它不会受前面的请求应答情况直接影响，也不会直接影响后面的请求应答情况
4) 服务器中没有保存客户端的状态，客户端必须每次带上自己的状态去请求服务器

28、什么是路由表
在计算机网络中，路由表（routing table）或称路由择域信息库（RIB, Routing Information Base），是一个存储在路由器或者联网计算机中的电子表格（文件）或类数据库。路由表存储着指向特定网络地址的路径（在有些情况下，还记录有路径的路由度量值）。路由表中含有网络周边的拓扑信息。路由表建立的主要目标是为了实现路由协议和静态路由选择。

每个路由器中都有一个路由表和 FIB(Forward Information Base)表：路由表用来决策路由，FIB 用来转发分组。路由表中有三类路由：
1) 链路层协议发现的路由（即是直连路由）
2) 静态路由
3) 动态路由协议发现的路由。

29、非 sql 数据库
Zookeeper，HBase、Redis、MongoDB、Couchbase、LevelDB

30、Linux 系统安全加固需要注意的内容
1) 关闭不必要的系统服务
2) 更改 SSH 默认端口

3） 禁止 root 用户远程 ssh 登录
4） 限制用户使用 SU 命令切换 root
5） 密码复杂度策略
6） 检查密码重复使用次数限制
7） 检查是否存在空口令账号
8） 禁止同时按下 ctrl+alt+del 重启
9） 禁用 telnet 服务

31、冰蝎，蚁剑，菜刀的流量特征
冰蝎动态二进制加密 WebShell 特征分析
https://www.wangan.com/p/7fy7f66970bb76af
常见 WebShell 客户端的流量特征及检测思路
https://www.cnblogs.com/NoCirc1e/p/16275608.html

32、常见 OA 系统
通达，泛微，万户，用友，致远，蓝凌，帆软，金蝶，红帆，极限，金和，志翔等

33、横向越权漏洞的修复
- 横向越权：横向越权指的是攻击者尝试访问与他拥有相同权限的用户的资源
- 纵向越权：纵向越权指的是一个低级别攻击者尝试访问高级别用户的资源

对于纵向越权，我们可以通过设置用户角色，为不同的角色提供不同的权限来避免。为了防止横向越权，我们可以使用缓存来进行辅助，当登录成功或者进行操作时，我们在缓存中存储一对由用户名和一个唯一的数字组成的数据（token），然后返回放入的唯一数据。在重置密码时我们的参数不仅需要用户名和密码还需要前面生成的唯一数字，根据用户名在缓存中取出对应的数字，如果取出的数字和参数中传入的想等，则证明重置的当前用户的密码，否则不是，且不予以重置。

34、挖矿病毒
https://www.ahstu.edu.cn/wlzx/info/1137/1992.htm
https://www.ahstu.edu.cn/wlzx/info/1137/1948.htm
https://www.ahstu.edu.cn/wlzx/info/1137/2416.htm
https://web.scut.edu.cn/2022/0413/c32211a467486/page.htm
https://web.scut.edu.cn/2022/0413/c32211a467487/page.htm

95 套安全面试题

以下面试题来源于@pen4uin 师傅 Github，一部分是他自己的，另一部分收纳整理自于互联网，但原项目已被删除：https://github.com/pen4uin/Security_Service_Interview

一、我的实习 & 校招

2020 实习 安全服务工程师(驻场)
1.挖过的一些漏洞（举例说明）
2.渗透测试的思路（结合自己的经验）
3.安全工具的使用（xray,sqlmap,awvs 等）

4.owasp top 10
- 记住是哪 10 个
- 知道漏洞原理
- 知道防御姿势

5.owasp top 10 中自己熟悉/经常挖到的漏洞
6.sql 注入
- 漏洞几种类型
- 漏洞成因
- 防御方法

7.编程能力(写一些小脚本，改一些 poc 等)

2020 实习 安全研究/技术支持(实战攻防)

0.自我介绍
1.实习经历
2.hw 经历
3.对红蓝对抗的看法
4.发展方向和规划
5.挖过哪些洞?追问原理
6.挖过最有意思/最难的一个洞
7.sql 注入写 shell
8.内网渗透
9.域渗透
10.Java 反序列化基础
11.跟过哪些 nday，怎样一个思路
12.shiro 反序列化
13.怎样对一个站去挖 nday
14.挖到过 0day 吗
15.代码审计
16.实战有没有遇到 xxe，oracle 注入，mssql 注入，ssrf，csrf
17.一些逻辑漏洞
18.app 渗透经历
19.会不会二进制/逆向
...

 # 小结

只记得当时技术面结束后，面试官和我说：你后面还有很多基础需要补啊！

2022 校招 红队攻防工程师

1.sql 注入的报错函数
2.dom 型 xss
3.ssrf 利用点
4.sql 注入点，空表如何利用
5.mvc 代码审计流程
6.看你简历有在挖洞，说一下你挖过的洞
7.Redis 利用姿势及环境差异
8.fastjson 回显
9.jndi 注入及原理
10.端口 389
11.Java 回显
12.泛微 oa xstream 的回显(jdk1.8 和 1.7 的差异)
13.shiro 限制 payload 长度
14.Java 回显的通用思路以及不同版本 jdk 的差异
15.文件上传白名单利用
16.00 截断的原理
17.判断域控的几种方式
18.工作组横向
19.域内横向

20.Windows 认证协议
21.白银票据黄金票据
22.判断是否在域内
23.hash 传递原理
24.权限维持
25.横向移动的各种姿势及原理
26.凭证获取(姿势/常用/原理/对抗)
27.如何对抗杀软加后门用户

Chrome dump 密码的原理，如果让你写个工具，思路是什么(或者别人工具的实现原理)

2021 实习 安全研究员

主要是两大块：Java 反序列化和内网

Java 反序列化

1.有哪些 CC 链是有回显的
2.Java 反序连化相关的协议
3.熟悉的 Java 的漏洞，选一个来深入问，shior 系列，550，721 原理，key 对了无法反序列化，不是无链的原因

内网

1.有一台 Windows 机器你会做些什么
2.有明文密码，密文密码你会做些啥。
3.有个基于 webshell 的，但 TCP 不出网，不会怎么做。
4.PTH
5.DCsync 原理，DCsync 是那个协议
6.有台 Windows 域内机子，你怎么打域控

2022 校招 攻防研究员(应用安全)

 # 基础

1. http 状态码，502，503，501
2. http 请求方式及各自作用
3. 计算机网络的分层及分别有哪些协议

 # owasp top 10

1. xss 如何执行代码
2. xss 常用哪些标签
3. http only
4. 怎样判断是否存在注入
5. sql 注入无回显怎么办
6. 延时注入除了 sleep 的其他姿势(mysql)
7. dnslog 的实现原理
8. sql 注入，单引号被拦截，如何绕过
9. sql 注入，写 shell 的语句，除了 into outfile 还有什么 mysql 的特性可以 getshell
10.redis 的利用，如何 shell,相关命令
11.ssrf 的原理即后利用，怎么执行命令，常搭配使用的协议

 # PHP 安全相关

1. 审计流程
2. 命令执行函数
3. 文件上传函数
4. 代码执行函数
5. vender 目录
6. phpunit
7. php 可以构造无文件 shell 吗

 # Java 安全相关

1. 挖过的通用洞，你会怎么利用(组合)

2. 命令的函数或包
3. java 哪些框架，审过哪些框架，它们常出现的问题是什么
4. 审计流程，你一般关注哪些洞，或擅长挖哪种类型
5. tomcat 做回显
6. 内存马的实现

 # 其他
- 写 poc/exp 的经历和心得
- 复现的一些漏洞
- Linux 提权的姿势
- Linux 下有哪些文件进行渗透时比较关注的，及文件权限问题
- dirty cow 的时间及其修复版本(哪年后就没法用了)
- 你觉得什么是你自己比较擅长的而我没有问到的

 # 小结
这个岗位主要是搞漏洞挖掘和利用以及原理分析，Web 方面就是 JAVA 和 PHP 的安全研究，比如 JAVA 下的流行框架，组件和服务器应用的安全问题。没有问内网!!!

2022 秋招 渗透测试工程师
1. 自我介绍
2. 印象深刻的一次渗透
3. 渗透测试的流程
4. SQL 注入原理，及常用 payload(手写-爆表名)
5. SQL 注入空格不能使用如何绕过
6. SQL 注入防御，延申预处理不能预防哪些注入
7. 同源策略
8. a.baidu.com 和 b.baidu.com 是否同源
9. SSRF 原理，利用
10. 攻击 redis 的方式（手写 payload）
11. CSRF 的原理及防御
12. 一种特殊的 CSRF 场景：后端只解析 json 格式的时候如何利用 CSRF(非更改 Content-Type)
13. SameSite
14. DNS Rebinding
15. Fastjson 反序列化及如何修复
16. 子域名枚举用过那些工具，原理是什么，如果出现了任意子域名都返回 200 是什么原因？
17. Java 学到哪种程度了？

2022 校招 安全研究员(SAST 方向)
一面
1. 自我介绍
2. 根据简历问(主要是挖洞方面)
3. 对 SAST 的理解
4. 对 IAST 的理解
5. 污点分析
6. 对 DevSecOps 的理解
7. 对 SDL 的理解
8. 后面的发展规划(学习方向)
9. 目前掌握的语言栈怎么样？愿意去学习新的语言吗？
10. 对 SAST 和 IAST 中哪个更感兴趣
11. 讲讲白盒审计的思路
12. 有写过相关的自动挖掘工具吗

 # 小结
体验很好，感觉双方更像是在探讨。

二面
1. Java 反序列化
2. 了解哪些白盒审计的工具，知道原理吗

3. 域控的攻击方式
4. MS14-068 的原理
5. 黄金和白银票据的利用及其效果，原理层面
6. IAST
7. 污点跟踪
8. 候选人的语言栈：java 和 go

 # 小结
估计凉凉，说让我去提前实习，我说想拿正式 Offer

2022 校招 高级安全工程师(代码审计/安全评估)

渗透基础
0.自我介绍
1. SQL 注入 写 Shell
   mysql & mssql & oracle
2. 登录框攻击面
3. getshell 的姿势
4. 文件上传点，黑名单限制，如何利用
5. SQL 注入后利用
6. 讲一个你觉得有趣的漏洞案例
7. 前段时间蓝凌 OA 的洞
8. DNS 重绑定，利用
9. Php 和 Java 的文件包含区别
10. Redis 的利用

PHP
1. 常见漏洞对应函数（挨个问）
- 命令执行
- 代码执行
- 文件包含
- 文件上传
- 文件删除
- SSRF
- ...
2. PHP 安全特性有关注吗
3. 代码审计(mvc/非 mvc)

Java
1. Java 执行命令的几种方式
2. Java 反序列化的原理
3. 讲讲 yso 的链
4. Shiro 反序列化原理
5. 反射，代理，类加载这些熟悉吗
6. 代码审计

Python
1. 是否写过非脚本的工具
2. Web 框架(flask/django)
3. 代码审计

漏洞挖掘(重点关注)
1. 简历上的通用洞挨个问
2. 漏洞利用研究的理解
3. 漏洞利用研究的案例

内网(偏实战问题)
1. disable function bypass
2. webshell 提权(低权限 -> 高权限)
3. 已经拿到 webshell，说说你的内网思路

4. 不允许扫描，如何横向
5. 存在杀软，不允许 exe 落地，怎么办
6. 常用的提权姿势
7. 内网代理，详细问了 frp

某互联网 500 强甲方红队攻防研究员面试题

职位：攻防对抗研究员

1、免杀
2、php5/7 区别
3、log4j 原理如何检测 绕过 不出网
4、fastjson 不出网
5、java 内存马
6、apk 双向认证如何绕过
7、php 反序列化 和 java 反序列化 .net
8、逻辑漏洞
9、除了 web 和社工其他方式渗透方法
10、对抗 EDR
11、隐藏流量特征 怎么和把 ip 地址变成可信
12、jwt 认证机制
13、k8s 集群
14、云渗透
15、容器逃逸
16、mysql 在哪里情况下可以直接执行系统命令
17、域攻击
18、redis 获得 shell 方法
19、小程序的攻击方法
20、域内 有什么方法能拿到黄金票据
21、二进制逆向
22、二进制漏洞
23、爱加密和梆梆壳怎么脱
24、无线渗透怎么去做
25、spring4shell 原理以及如何检测
26、bypass uac

二、同行师傅们的实习 & 校招 & 社招

01 套

1、常见的 SQL 注入类型有哪些？并写出 sqlmap 检测 SQL 注入的命令？SQLMAPAPI 怎么使用
2、Mongodb、redis、websphere、rsync 服务简介和默认运行端口
3、写出你知道的逻辑漏洞
4、列举 Linux 的反弹 shell 的一些方法
5、针对 SQL 注入，写出你所知道的 Bypass WAF 的可能的方式
6、写出任意一种漏洞检测代码，用 python 实现
7、简述 XXE 的基本原理，以及如何去检测或者判断 Blind XXE 的存在
8、简述针对一个网站的渗透测试思路
9、针对 Web 扫描器的爬虫，你怎么看
10、简述 PHP 中造成任意文件下载漏洞的常见函数，以及造成漏洞的原因

02 套

1、介绍一下自认为有趣的挖洞经历
2、你平时用的比较多的漏洞是哪些？相关漏洞的原理？以及对应漏洞的修复方案？
3、php/java 反序列化漏洞的原理?解决方案?
4、如果一台服务器被入侵后,你会如何做应急响应
5、你平时使用哪些工具?以及对应工具的特点?
6、遇到 waf 如何进行 sql 注入/上传 Webshell？请写出曾经绕过 WAF 的经过(SQLi，XSS，上传漏洞选一)
7、如何判断 sql 注入，有哪些方法
8、介绍 SQL 注入漏洞成因，如何防范？注入方式有哪些？除了数据库数据，利用方式还有哪些？

9、为什么有的时候没有错误回显
10、宽字符注入的原理？如何利用宽字符注入漏洞，payload 如何构造
11、CRLF 注入的原
12、mysql 的网站注入，5.0 以上和 5.0 以下有什么区别？
13、php.ini 可以设置哪些安全特性
14、php 的%00 截断的原理是什么？
15、webshell 检测，有哪些方法
16、php 的 LFI，本地包含漏洞原理是什么？
17、说说常见的中间件解析漏洞利用方式
18、mysql 的用户名密码是存放在那张表里面？mysql 密码采用哪种加密方式？
19、Windows、Linux、数据库的加固降权思路，任选其一
20、你使用什么工具来判断系统是否存在后门
21、如何绕过 CDN 获取目标网站真实 IP，谈谈你的思路？
22、如果给你一个网站,你的渗透测试思路是什么？在获取书面授权的前提下。
23、谈一谈 Windows 系统与 Linux 系统提权的思路？
24、列举出您所知道的所有开源组件高危漏洞(十个以上)
25、反弹 shell 的常用命令？一般常反弹哪一种 shell？为什么？
26、CMD 命令行如何查询远程终端开放端口
27、服务器为 IIS+PHP+MySQL，发现 root 权限注入漏洞，讲讲你的渗透思路
28、请写出 Mysql5 数据库中查询库’helloworld’中’users’表所有列名的语句
29、udf 提权
30、SQL 头注入点
31、php 中命令执行涉及到的函数
32.、SSRF 漏洞的成因 防御 绕过
33、mysql 写 shell 有几种方法
34、Metasploit 打开反向监听的命令
35、有哪些反向代理的工具?
36、有什么比较曲折的渗透经历
37、怎么查找域控
38、PHP 作为弱类型语言，在底层它是怎么判断变量的类型的
39、ARP 攻击的原理（讲出具体的流程），如何发现并防御 ARP 攻击
40、渗透大企业简单还是小站点简单，为什么
41、内网如何反弹 shell，反弹的 shell 流量如何隐蔽
42、除了 TCPIP 协议，如何将内网数据传递出来（内网环境有着严格防御与审查）

03 套

1、什么是同源策略
2、XSS 能用来做什么
3、XSS 的三种类型，防御方法
4、存储型 xss 原理
5、你怎么理解 xss 攻击
6、如何快速发现 xss 位置
7、Dom xss 原理/防范
8、DOM 型 XSS 与反射型 XSS 区别
9、如何使得前端 referer 为空
10、cookie 参数，security 干什么的
11、如果 SRC 上报了一个 XSS 漏洞，payload 已经写入页面，但未给出具体位置，如何快速介入
12、XSS， CSRF， CRLF 比较容易弄混，说说三者的原理，防御方法
13、csrf 如何不带 referer 访问
14、CSRF 成因及防御措施；如果不用 token 如何做防御
15、Xss worm 原理
16、Cookie 的 P3P 性质
17、CSRF 有何危害

04 套

1、渗透测试流程
2、描述渗透项目，做了什么
3、xss 漏洞类型、详情、修复方案
4、SQL 注入原理、类型，waf 绕过，写 shell，提权，修复方案

5、终端的渗透经验
6、了解什么比较新的漏洞
7、企业内部安全

05 套

1、算法？了解过什么排序？
2、爬虫
3、页面存在很多 js 的时候，用什么
4、爬虫的待爬取 URL 量级比较大的时候，如何对其去重
5、多线程 异步 协程 多路复用 用哪一个最快 为什么
6、浏览器的常用编码
7、web 常用的加密算法有什么
8、有没有内网渗透的经验？怎么渗透？如果拿下了边界层的某一个机器，如何对内网其他进行探测？
9、mysql 中 like 查询会会非常缓慢，如何进行优化
10、做了 cdn 的网站如何获取真实 IP
11、渗透的时候如何隐藏自己的身份
12、主机疑似遭到入侵，要看哪里的日志
13、SQL 注入漏洞怎么修复

06 套

1、病毒和蠕虫的区别
2、DNS 欺骗
3、DDOS 有哪些，CC 攻击是什么，区别是什么，什么协议
4、land 攻击
5、存储型的 xss 的危害和原理
6、渗透测试流程
7、移动端的调试经验 apk,ipa 包分析
8、对于云安全的理解
9、虚拟机逃逸的理解

07 套

1、owasp top10 漏洞
2、xss 如何盗取 cookie
3、渗透测试的流程
4、xss 如何防御
5、xss 有 cookie 一定可以无用户名密码登录吗？
6、SSL Strip(SSp)攻击到底是什么？
7、中间人攻击——ARP 欺骗的原理、实战及防御
8、会话劫持原理
9、CC 攻击
10、添加时间戳防止重放攻击
11、HTTPS 中间人攻击与证书校验
12、什么是 HttpOnly?
13、dll 文件是什么意思，有什么用？DLL 劫持原理
14、Rootkit 是什么意思
15、手工查找后门木马的小技巧
16、SSRF 漏洞

08 套

1、渗透测试简要流程
2、绕过 WAF 常用方法
3、SQL 注入常见 Payload
4、XSS 种类、弹窗函数、绕过方法
5、XXE 漏洞原理
6、列举 OWASP TOP10
7、SQL 注入常用函数
8、.XSS 和 CSRF 的区别
9、常见的中间件

10、文件上传怎么绕过
11、反序列化的原理
12、数据库预处理怎么突破
13、httponly
14、SQL 注入如何拿 GetShel
15、oracle、mysql、sqlserver 默认端口
16、SSRF
17、常见 Web 安全漏洞
18、MYSQL 注入 5.0 以上和 5.0 以下有什么区别
19、get 传参和 post 传参的区别

09 套

1、讲一下你所了解的 web 漏洞
2、你在 SRC 挖掘中遇到最多的漏洞是什么
3、SQL 注入分为几种
4、详细讲一下 SQL 注入
5、XSS 有几种，详细讲一下
6、XSS 除了获取 cookie，还有别的用处吗
7、讲一下渗透测试的流程
8、讲一下信息收集都收集那些信息
9、看你简历有写内网渗透，简单讲一下
10、获取 shell 之后，你是怎么提权的
11、怎么通过数据库获取 shell
12、数据库的提权有接触过吗
13、进入到内网之后，怎么去维持权限
14、讲一下黄金票据
15、讲一下 APP 渗透
16、如果抓不到包，是因为什么
17、讲一下 HTTP 双向认证
18、了解 APT 吗

10 套

1、HTTP 的请求方式
2、具体说说这些请求方式
3、sqlmap 怎么跑 post 请求
4、SSRF 的危害
5、怎么他测内网，怎么访问敏感文件文件
6、oracle 数据库端口号
7、怎么防范 CSRF
8、linux 系统中 etc/password 文件和/shadow 文件的区别
9、了解 struct 框架吗，说一说

11 套

1、SQL 注入的防护方法有哪些？
2、永恒之蓝的漏洞原理是什么？怎么做到的？
3、命令注入有哪些？
4、给你一个目标网站，你该如何进行测试？
5、给你一个后台登陆地点的网站，你能从中发现那些问题？
6、给你一千台服务器和交换机，你会如何进行扫描？
7、内网渗透了解多少？
8、中间件有哪些？
9、中间件有哪些已知的漏洞？

12 套

1、SQL 注入盲注的方法
2、如何防范 SQL 注入
3、xxs 有哪些和绕过方式以及防护方式
4、同源性法制你了解吗

5、csrf 可以干什么怎么防护
6、逻辑漏洞有哪些
7、文件包含以及变量覆盖
8、SQL 注入如何写 shell
9、内网渗透

13 套

1、简历上面写的几个漏洞，逐个问一遍
2、怎么判断目前是否是 cms
3、后台扫描用什么工具
4、御剑有自己的包吗
5、burp 会哪些模块，
6、越权以及逻辑漏洞问题
7、我听你上面说的都是小面积的测试，你有没有大面积测试过一个网站呢？
8、如果不能用 awvs 和 appscan 你还能怎么办
9、会哪些 bypass 的手法
10、SQL 注入怎么拿到最高权限？
11、写 shell 需要什么权限吗？你怎么判断存在写入权限
12、如果没有写入权限，你还能有什么办法吗
13、怎么利用说 SQL 注入来读取文件吗
14、怎么获得绝对路径呢？没有报错呢？不能读取文件呢
15、xss 里面的牛头你会用吗？xss 你知道除了可以盗取 cookie 还能干什么，xss 平台你用的是上面
16、msf 用过吗？
17、msf 的木马你知道吗？免杀是怎么做的？
18、内网提权方面你土豆你知道原理吗？
19、怎么找到域控机？
20、webshell 你会利用哪些办法来写绕过
21、mssql 的提权你能说一下吗？
22、那其他数据库的 SQL 注入呢？
23、怎么分辨数据库类型
24、做过黑产吗？

14 套

1、sql 注入原理
2、xxe 攻击
3、sql 注入都有哪些
4、Windows 怎么提权
5、文件上传绕过
6、代码审计
7、逻辑漏洞有哪些
8、验证码绕过有哪些方法
9、csrf 原理
10、不用工具的情况下 如何搜集子域名

15 套

1、有没有实习过？在哪实习的？
2、cnvd 那的都是什么证书？
3、给你一个登录窗口你会怎么利用？
4、怎么去绕过验证码？
5、我看你简历上说会绕 waf？
6、以后的发展？
7、多久能学会？
8、那你都复现过什么漏洞，在哪里跟进漏洞？

16 套

1、平时怎么做渗透，说一下渗透测试步骤
2、渗透测试过程中如何信息收集，说一下渗透测试信息收集方法
3、工作中用过那些扫描器，这些扫描器有那些优点缺点？

4、burp 如何破解 md5 加密密码或 base64 加密密码
5、常见的 http 方法有那些，他们之间的区别是什么
6、常见状态码你知道吗？分别说一下 200、201、301、302、500、503 的含义？
7、常见请求消息头的作用，分 别说一下 cookie、referer、user-Agent 的作用
8、响应消息头的作用，分别说一下 Location、Access-Control-Allow-Origin、WWW-Authenticate
9、Cookie 响应消息头的 secure 和 HttpOnly 分别作用是什么？
10、在渗透过程中常用的编码有那些？
11、静态 动态语言区别
12、常用的脚本语言和数据库有那些
13、系统、脚本语言、中间件如何组合
14、渗透测试过程如何判断对方操作系统是什么操作系统
15、你是怎么知道对方网站使用了那些常用 cms 系统搭建的（指纹信息是什么）
16、给你一个网站你是如何信息收集的

17 套

1、注入攻击原理是什么？如何找注入点？如何判断注入点？
2、注入分为几类及提交方式是什么
3、注入攻击一般所支持的类型有那些
4、mysql 数据库帐号和密码存放在那个库和表里面
5、如何寻找网站物理路径
6、分别写出 mysql 及 mssql 数据库写入 webshell 的方法
7、请说出 mysql5.0 以下与 5.0 以上的区别
8、sql 注入对服务器文件读写操作需要那些条件
9、分别说出 sqlmap -u -r -v -p —level —risk —tables —coiumns -T —tamper 参数的含义
10、注入漏洞防范方法
11、xss 攻击原理及出现的原因
12、xss 分为那几类
13、xss 的危害，可能存在的地方
14、xss 漏洞测试方法
15、xss 如何绕过安全防范
16、分别说出 iis、apache、nginx 解析漏洞原理
17、任意文件下载攻击原理及测试方法
18、任意文件上传漏洞分几类，说出每类突破方法
19、分别文件包含漏洞攻击原理及分类
20、如何快速挖包涵漏洞
21、包涵漏洞具体能做什么，怎么绕过你能说说吗
22、ssrf 漏洞攻击原理、用途
23、说说你是如何挖掘 ssrf 漏洞
24、说说 ssrf 绕过及防范方法
25、csrf 攻击原理是什么及一般你用什么工具进行检测
26、你是如何挖掘 ssrf 漏洞的及防范方法
27、说说 xxe 漏洞攻击原理是什么，如何找 xxe 漏洞及攻击方法
28、xxe 攻击在无回显的时候你是如何突破的
29、你是如何防范 xxe 漏洞的
30、你挖洞影像最深的是什么？
31、你认为你的渗透水平在国内大概是什么水平，能给自己打多少分
32、说说你以前在你公司主要做什么安全工作？如每天、每月、每年做些什么安全工作
33、你在各大漏洞平台挖过漏洞吗，能说说吗？
34、你写过什么好的安全漏洞文章发布过吗，是否可以说说？

18 套

1、自我介绍
2、拿到一个待检测的站，你觉得应该先做什么（一个网站的渗透测试思路，流程）
3、判断出网站的 CMS 对渗透有什么意义？
4、一个成熟并且相对安全的 CMS，渗透时扫目录的意义？
5、常见的网站服务器容器。
6、目前已知哪些版本的容器有解析漏洞，具体举例。
7、简述 SQL 注入，XSS，CSRF 漏洞的原理和渗透手法等
8、如何手工快速判断目标站是 windows 还是 linux 服务器？

9、为何一个 mysql 数据库的站，只有一个 80 端口开放？
10、3389 无法连接的几种情况
11、如何突破注入时字符被转义？
12、拿到一个 webshell 发现网站根目录下有.htaccess 文件，能做什么？
13、请写出突破 Waf 的方法
14、提权时选择可读写目录，为何尽量不用带空格的目录？
15、审查上传点的元素有什么意义？
16、目标站禁止注册用户，找回密码处随便输入用户名提示：“此用户不存在”，怎样利用？
17、目标站发现某 txt 的下载地址为.do?file=/upwdown/1.txt，有什么思路？
18、目标站，已知根目录下存在/abc/目录，并且此目录下存在编辑器和 admin 目录，思路
19、在有 shell 的情况下，如何使用 xss 实现对目标站的长久控制？
20、后台修改管理员密码处，原密码显示为*。你觉得该怎样实现读出这个用户的密码？
21、目标站无防护，上传图片可以正常访问，上传脚本格式访问则 403.什么原因？
22、审查元素得知网站所使用的防护软件，你觉得怎样做到的？
23、demo.do?DATA=AjAxNg==，这个链接存在 sql 注入漏洞，对于这个变形注入，你有什么思路？
24、发现 demo.jsp?uid=110 注入点，你有哪几种思路获取 webshell，哪种是优选？
25、CSRF 和 XSS 和 XXE 和 SSRF 有什么区别，以及修复方式？
26、说出至少三种业务逻辑漏洞，以及修复方式？
27、sqlmap，怎么对一个注入点注入？
28、nmap，扫描的几种方式
29、sql 注入的几种类型？
30、报错注入的函数有哪些？
31、延时注入如何来判断？
32、盲注和延时注入的共同点？
33、如何拿一个网站的 webshell？
34、sql 注入写文件都有哪些函数？
35、owasp 漏洞都有哪些？
36、网络安全事件应急响应
37、你提交的漏油
38、说说你的其它优势（如：对安全新兴技术的研究、个人博客、比赛、在校经历等）

19 套

1、自我介绍
2、提交过什么漏洞
3、常用的漏洞扫描工具有哪些
4、owasp top10
5、mysql 数据库，写入一句话木马所需权限
6、xss 分类，区别
7、xxe 漏洞
8、比较成功的渗透经历
9、app 渗透测试吗？
10、宽字节注入的原理
11、写过工具没
12、mysql 数据库的右向偏移

20 套

1、中间件
2、SQL 注入怎么写入，用的什么函数
3、越权问题有哪些，实战
4、文件上传
5、mqsql 提权有哪些
6、XSS（绕过）
7、CSRF 与 XSS 的区别
8、SSRF
9、Java 反序列化
10、URL 跳转漏洞
11、平时怎么绕 waf
12、Sqlsever 利用思路
13、盲注

21 套

1、XSS 的标签
2、说说大学这几年最自豪的事请
3、SQL 注入
4、偏移注入
5、CTF 你都做哪些题型
6、遇到的比较困难的 web 题型的 ctf 题目
7、XXE
8、反序列化
9、Bypass 说说
10、假如，让你设计一个 Waf，你会怎么设计
11、内网渗透与提权
12、平常都挖掘哪些 SRC
13、有没有写过一些脚本
14、说说 SQL 注入手工怎么爆出所有库名字

22 套

1、为什么做这一行
2、有哪些项目经验
3、会不会逆向 APK，会不会嵌入式
4、正则能不能写
5、JAVA 能不能上手
6、渗透测试的基本流程
7、如何创建一个用户并且提权
8、数据库表名 test 字段名 user,password 写出查询语句
9、linux 如何查看当前权限
10、Apach IIS Nginx 的解析漏洞
11、谷歌排行第一的 CMS 有 1000 个旁站，问怎么日(面试题)
12、是否有在国外抓过肉鸡，有没有做黑产的朋友
13、使用谷歌语法查询指定域名的子域名 并且搜索他的后台登陆
14、能否接受驻场
15、最得意的一次渗透测试
16、是否有写过 tamper

23 套

1、自我介绍
2、SQL 注入原理、修复建议、如何彻底杜绝 SQL 注入
3、渗透流程
4、XSS 的种类，修复建议
5、渗透过哪些网站，请举几个例子，印象最深的
6、漏洞平台的贡献是多少，排名是多少
7、代码审计的时候你比较关注的漏洞是哪些
8、对 linux 了解吗？linux 内核漏洞有没有分析过？
9、你说你对堆栈溢出有了解，那玩过 pwn 吗？
10、说说在 kali 上，最常用的几个工具？
11、ARP 欺骗的方法有哪些？说说原理
12、对 https 了解吗？讲一下加密和解密流程？
13、都破解过哪些软件？如果给你一个产品，你能提出安全加固建议吗？

24 套

1、如何进行信息搜集，用过哪些工具
2、对没有挂到 DNS 上的网站如何进行入侵
3、有哪些常见的中间件，相关漏洞
4、端口扫描时，都关注哪些端口，分别代表什么
5、针对 PHP 的弱类型，有哪些漏洞
6、代码审计方面，有过对大型 CMS 的审计吗，发现过哪些漏洞
7、针对 PHP 的语言特点，说几个常见的漏洞
8、SQL 注入，如何写入文件

9、SQL 注入，如果注入点在 union 或 order by 之后，怎么办
10、陈述一下缓冲区溢出
11、如果对方开启了 ASLR 和 DEP，要如何绕过

25 套

1、渗透测试流程
2、SQL 过滤单引号怎么注入
3、宽字节原理
4、CSRF 和 SSRF 区别 和 作用
5、如何绕 waf
6、命令执行有哪些函数
7、OWASP TOP10
8、隐藏马
9、端口号及对应服务
10、Java 的反序列化漏洞
11、有什么优势
12、文件包含 include()与 require()的区别
13、内网渗透相关问题

26 套

1、三分钟自我介绍
2、Web 安全，SQL 注入安全修复建议/XSS form 框限制长度的绕过
3、说说白盒检测漏洞的思路
4、说说静默挖矿行为检测
5、说说 webshell 检测
6、Python 装饰器
7、python 类方法、静态方法、对象方法区别
8、你的能力栈
9、你的能力模型
10、说一个你觉得做的比较好的项目？在项目上你比业界的优势在哪儿？
11、期待做什么样的工作？宽度 or 广度？你对工作的选择？
12、说说水平权限优化这块儿的工作
13、怎么看待深度和广度的点
14、你的职业规划
15、工作意愿
16、期望工作城市

27 套

1、order by 注入 limit 注入 后面跟的函数有什么不同
2、order by 含义
3、MYSQL 注入
4、基于 css 的 XSS
6、基于 flash 的 XSS 原理
7、过滤了单引号、into outfile 是否还能利用
8、除了 script ,html 事件之外还有哪些存在 XSS 的地方
9、IIS 拒绝服务原理
10、SSRF 除了探测主机外如何进一步进行攻击
11、uname -a 、 '-a'参数可控，如何执行多条指令
12、MYSQL /MSSQL 注入原理，分类，盲注
13、文件上传 & 文件包含、分类、原理
14、CSRF 和 XSS 原理、分类
15、SSRF & XXE 细节，绕 waf ，渗透测试流程

28 套

1、SQL 注入的成因、代码层防御方式
2、XSS 的成因、代码层防御方式、写出 3 条 xsspayload
3、Jsonp 劫持漏洞的原理、利用方式、防御方法
4、XXE 漏洞的原理、危害、防御方法

5、getshell 的姿势（SQL 注入、文件包含、文件上传、命令执行、后台 getsehll 等）
6、在 SRC、补天、盒子、乌云等都提交了哪些高中危漏洞，说说挖这些漏洞的方法。
7、说明电商系统的加车、下单、支付过程中，常见的逻辑漏洞有哪些，如何挖掘
8、APP 常见任意密码重置漏洞的挖掘方法
9、挖掘过哪些逻辑漏洞，请说明挖洞方法
10、SSRF 漏洞的成因、利用方法、防御方式
11、挖掘过哪些 APP 的 web 漏洞（非逆向），如何挖掘的
12、利用的过的通用漏洞有哪些？包括 CMS、web 中间件、操作系统、DB 等
13、同源策略，有什么作用？同源策略中 Access-Control-Allow-Origin 的作用是什么
14、CSRF 的成因、利用方式、哪些功能容易有 CSRF，防御方法
15、挖掘 Web 漏洞的流程和思路，是当完成信息收集之后，开始挖洞的思路
16、获取 Web shell 后，是否做过内网渗透，你用哪些正向代理、反向代理工具，这些工具如何使用
17、写出 Mysql 导出 php 一句话木马的命令

29 套

1、自我介绍
2、渗透测试流程，有没有打过内网
3、SQL 注入，报错
4、XSS，反射/DOM 型，怎么利用
5、Redis 的利用
6、应急响应能力怎么样，处置流程思路
7、无态势感知，安全设备，怎样手动发现 shiro 反序列化漏洞进来都攻击
8、平时有分析研究漏洞吗，编写 exp，熟悉什么开发语言
9、关于 hook 了解
10、ATT&CK 框架了解吗、到什么程度，是否有过应用

30 套

1、如何做的样本分析，思路是什么
2、如何用 linuxgdb 分析一个简单样本
3、再举一个你的其他应急的例子(我举的是挖矿病毒)
4、日志你看的是什么日志，web 服务器日志嘛
5、某些命令被替换了，如何发现
6、rpm 有个参数就可以校验命令是否被替换，是什么
7、是否做过 APT 相关的研究
8、如何分析 windows，linux，web 一些常见的漏洞
9、内网突破到内网漫游的思路
10、如何横向、IPC 了解过嘛，横向原理
11、权限提升（windows，linux）

31 套

1、常见的端口问题
2、SQL 注入中的报错函数
3、渗透测试的基本流程
4、Redis 数据库的利用手法
5、CSRF 的原理 & 利用
6、对于 webshell 执行命令或者木马.exe 被杀软拦截，如何 bypass
7、XSS 的原理、最大化利用
8、Fastjson 的某个版本漏洞成因、漏洞的入口点在哪
9、Java 反序列化的原理

32 套

1、自我介绍
2、渗透测试的流程
3、熟悉什么语言，有无开发经历
4、自动化挖洞了解过吗？曾经刷过什么漏洞？怎么刷的？
5、前期信息搜集你是怎么做的
6、印象深刻的一次漏洞挖掘？
7、从浏览器输入 URL 到页面回显的过程中，经历了哪些协议

8、HTTP 和 HTTPS 网站的注入用 sqlmap 是否有区别，状态码为 401 或者其他时如何与成功的页面区分
9、AWVS，比如如何防御对于类似工具的扫描，能否针对一个服务比如 ASP.NET 进行扫描
10、CSRF 和 SSRF 的区别
11、SSRF 对输入做了 ipv4 的正则过滤，有什么 bypass 方式？
12、一个 ip 可以有多个站点，服务器是怎么知道我们访问的是哪个站点的？

33 套

1、Dnslog 的原理
2、内网渗透如何判断 tcp 是否有出口限制
3、iptables 的三张表分别的作用，如何查看详细登陆日志
4、如何查看是否有进程调用敏感文件执行命令，例如：攻击者把木马注入到主进程里，如何发现木马所在的子进程的进程号并杀死木马进程?
5、线程，协程的原理以及相关的效率问题
6、你觉得你的优势是什么
7、来到这里你想学到什么
8、php 反序列化
9、你了解的 redteam 是什么
10、未来的学习计划

34 套

1、go 语言免杀 shellcode 如何免杀？免杀原理是什么？
2、windows defender 防御机制原理，如何绕过？
3、卡巴斯基进程保护如何绕过进行进程迁移？
4、fastjson 不出网如何利用？
5、工作组环境下如何进行渗透？详细说明渗透思路。
6、内存马的机制？
7、不出网有什么方法，正向 shell 方法除了 reg 之类的，还有什么？
8、什么是域内委派？利用要点？
9、shiro 漏洞类型，721 原理，721 利用要注意什么？
10、护网三大洞？
11、天擎终端防护如何绕过，绕过思路？
12、免杀木马的思路？
13、jsonp 跨域的危害，cors 跨域的危害？
14、说出印象比较深刻的一次外网打点进入内网？
15、rmi 的利用原理？
16、域内的一个普通用户（非域用户）如何进行利用？
17、宝塔禁止 PHP 函数如何绕过？
18、证书透明度的危害？
19、内网渗透降权的作用？
20、webshell 有 system 权限但无法执行命令，怎么办？

35 套

1、网站信息收集
2、怎么寻找真实 IP（cdn 绕过）
3、常见漏洞原理和防范
4、sql 怎么找注入点、盲注
5、叙述一下时间盲注原理以及用到的各种函数
6、sleep 函数被过滤怎么办？
7、sql 注入能拿 shell 么，需要什么权限
8、怎么获得网站的绝对路径？
9、web 服务器解析漏洞了解么？
10、Nginx 安全配置相关
11、PHP 审计流程
12、php 怎么防注入
13、php 安全配置了解么
14、web 渗透流程
15、http 了解么、长连接还是短连接、谈谈对 http 无状态的理解。
16、bp 抓 https 包的原理
17、https 实现过程

18、防御 csrf 的方式？token 防御 csrf 的原理？

36 套

1、讲一讲同源策略，以及有哪几种跨域方式？就你所说的哪几种跨域方式，都会出现哪些漏洞知道吗？
2、cors 跟 csrf 漏洞的区别？
3、cookie 的 same-site 熟悉吗？
4、httponly 的话，怎么绕？
5、你对 xxe 漏洞的理解？
6、windows 的 ntlm 跟 ker 协议有了解？
7、说几种 sql 报错注入的方式？
8、你有挖掘过什么漏洞吗？众测也好、src 也好？
9、如果给你一个站点，你是怎么做这个整个的流程，给你一个主域名？
10、你有什么搜集子域的方式？爆破的话怎么判断是存活？如果没有 web 站点的话呢？
11、有针对你这些漏洞挖掘的过程，有想过自动化的开发吗？
12、说一个代码审计一个有趣的例子吗？
13、有写过一些安全工具吗？
14、搞内网搞的多吗？自己有学过一点这一块的知识吗？现在看了哪些？
15、讲一个你最近分析过多一个有趣的漏洞吧？
16、java 的代码审计熟悉吗？
17、php 的反序列化的原理大体说一下？java 的反序列化这块呢？
18、redis 的弱口令，有哪几种获得 shell 的方法？
19、mysql 有一个 sql 注入点，怎么拿 shell？写文件的函数？mysql 的提权方？sqlserver 的执行命令的函数是哪个？需要什么权限？

37 套

1、说说你知道的解析漏洞
2、文件上传绕过 waf 思路
3、mysql 延时注入除了 sleep 函数,还有什么
4、PHP 中常见危险函数
5、说说 eval 和 system 区别
6、Mysql 写入木马条件,如何得到网站物理路径
7、说说 php 反序列化理解
8、getshell 后发现不出内网,如何判断哪些协议能出网,哪些端口能用,对应工具用什么
9、如何定位域控

38 套

1、为何一个 MYSQL 数据库的站，只有一个 80 端口开放
2、成熟并且相对安全的 CMS，渗透时扫目录的意义
3、在某后台新闻编辑界面看到编辑器，应该先做什么？
4、审查上传点的元素有什么意义？
5、CSRF、XSS 及 XXE 有什么区别，以及修复方式？
6、3389 无法连接的几种情况
7、列举出 owasp top10 2017
8、说出至少三种业务逻辑漏洞，以及修复方式？
9、目标站无防护，上传图片可以正常访问，上传脚本格式访问则 403，什么原因？
10、目标站禁止注册用户，找回密码处随便输入用户名提示：“此用户不存在”，你觉

39 套

1、owasp top10 有哪些
2、ssrf 原理，出现在什么场景，应用，防范
3、csrf 简单说一下
4、说一下 jsonp 跨域劫持
5、讲一下自己挖掘的漏洞，挑一个出来详细说
6、之前提到短信轰炸漏洞，讲解一下怎么绕过服务端的限制
7、使用 Java 或者 Python 开发过什么
8、了解 windows 下的日志文件吗
9、给一个场景，怎么来分析日志文件
10、Apache 解析漏洞

11、tcp 三次握手
12、ping 属于什么协议，除了 ping 之外还有什么能判断网络存活（差不多这意思，记不太清了）
13、Linux 查看进程命令有哪些
14、windows 一些网络命令

40 套

1、CS 流量如何修改/隐藏
2、低权限注入点如何提权
3、SQLserver 删除了 xp_cmdshell，如何恢复
4、Java 反序列的利用过程/原理

41 套

1、自我介绍
2、sql 注入用过哪些函数
3、ATP 攻击步骤
4、sql 注入的原理是什么，怎么防范
5、挖掘 src 的主要是什么漏洞
6、参加过哪些 ctf 比赛
7、有没有自己写过工具
8、还有没有想问的
9、对哪些方面比较熟悉
10、你是 XX 人，为什么投递到南昌？
11、有没有过 app 测试的经历

42 套

1、SQL 注入如何读写文件，二次注入，防御方式
2、XSS 有哪几种，如何防御
3、CSRF 和 XSS 区别，如何防御
4、文件上传的前后端的绕过，防御方式
5、IIS6、0，Apache，Nginx 的文件解析漏洞讲一下
6、XXE 和 SSRF 简单讲一下
7、RCE 讲一下，PHP 函数 eval 和 system，popen 的区别
8、Python 的迭代器和装饰器讲一下
9、缓冲区溢出原理和防御
10、内网渗透经验有没有
11、多线程和进程讲一下，线程通信以及进程通信方式
12、渗透测试流程讲一下，信息收集都有哪些方面
13、有没有实际渗透经验，讲一下
14、有没有了解过系统漏洞，windows 方面的，比如 MS08-06715、你是如何学习渗透的，哪些方式
15、虚函数的底层实现
16、反射的底层实现
17、满二叉树和完全二叉树
18、Python 和 Java 的垃圾回收讲一下
19、SQL 手工注入流程
20、Java 框架的控制反转怎么实现的
21、进程通讯有哪些
22、消息队列的原理
23、经典老问题访问百度，重点说一下涉及到的所有协议
24、常见的 web 漏洞有哪些
25、Burpsuite 的功能有哪些
26、说一下所有的排序算法，哪些是不稳定的
27、图的遍历方式有哪些，基于什么数据结构
28、如何实现一个 HTTP 代理，原理是什么

43 套

1、常用的 nmap 命令是什么
2、常用的漏洞扫描工具有哪些
3、了解 owasp top10 吗？有哪些

4、xss
5、http 协议吗？有什么字段？
6、xxe
7、挖过 src 吗
8、了解逆向吗，对二进制熟悉吗
9、sql 注入的原理是什么
10、宽字节注入的原理是什么

44 套

1、Java 反序列化漏洞的原理和利用方式
2、xss 的原理和防护措施
3、内网渗透做过没有
4、信息收集的方法
5、谷歌语法使用
6、正则的作用，用过的正则符号
7、其他抓包软件，比如 wireshark 用过
8、说出你完成的一次渗透，遇到的困难，解决的方式。
9、tcp/ip 协议，http 协议
10、jdk,jre,jvm 的关系
11、开发过程中写过的项目，最长有多少行代码。
12、ptyhon 会不会用，能不能代码审计
13、说一说 java 的反射机制
14、有没有密码字典，字典的规则是什么

45 套

1、简单做个自我介绍，说说职业规划。
2、说说 webshell 检测的项目，从源码侧做的检测？
3、说说常见的 Web 漏洞？
4、说说渗透里有意思的点？
5、如果说做一个 fuzz 平台，应该怎么做？
6、堆溢出、栈溢出？原理和防护？
7、插桩有了解吗？
8、有没有了解一些二进制的东西？
9、C 语言申请空间？
10、你常用的 Python 框架？异步框架？
11、Python 异步 sink 这些有什么了解吗？
12、Java 的设计模式？
13、你平时的信息流？
14、webshell 检测？流量、编码
15、流量检测有没有做过其他攻击的尝试
16、红蓝对抗例子？内网？渗透测试流程
17、当前的攻防演练你觉得思路应该怎么样
18、你自己的职业规划方向
19、你怎么看待 Web 安全
20、说一下你最擅长的三个方向
21、你提到的程序分析？污点追踪了解吗

46 套

1、了解哪些漏洞
2、文件上传有哪些防护方式
3、用什么扫描端口，目录
4、如何判断注入
5、注入有防护怎么办
6、有没有写过 tamper
7、3306 1443 8080 是什么端口
8、计算机网络从物理层到应用层
9、有没有 web 服务开发经验
10、如何向服务器写入 webshell
11、有没有用过 xss 平台

12、网站渗透的流程
13、mysql 两种提权方式
14、常见加密方式
15、ddos 如何防护
16、有没有抓过包，会不会写 wireshark 过滤规则
17、清理日志

47 套

1、sql 注入会用到哪些函数
2、sqlmap 爆出当前库名的参数是什么
3、namp 探测系统的参数是什么
4、namp 的小写 o 与 a 是干嘛的
5、布尔型盲注的具体语句是什么
6、宽字节的原理
7、python 有没有反序列化
8、get 传参与 post 传参的区别
9、Http 有哪些请求方式
10、如何判定 cdn 与 cdn 的作用
11、如何确认服务器的真实 IP
12、栅栏密码的原理
13、oracle 的默认端口
14、如果 substr()函数被禁用，有多少替换函数
15、redis 如何拿下，哪个端口，具体语句，具体操作
16、同源策略
17、ssrf 有哪些危害
18、如何防御 ssrf
19、MSF 框架稍微问的深入了一些
20、web 容器（中间件）有哪些解析漏洞与原理
21、如何防范 sql 注入

48 套

1、首先根据简历提问
2、我的一个项目完成的怎么的样
3、Java 基础怎么样，
4、有没有自己动手写过一些工具
5、有没有想过自己以后要写一下扫描器
6、sql 注入的简单原理及其如何防御
7、有没有了解过反序列化 尤其是 Java 方向的
8、数据结构还记得多少
9、src 主要挖掘一些什么类型的漏洞
10、了解的 MSF 框架怎么样
11、数据库主要了解的哪些，主要学的什么数据库
12、ssrf 的原理及其防御

49 套

1、自我介绍
2、owasp top10 漏洞你最熟悉那些
3、请下 sql 注入原理 ，盲注常用那些函数，绕 waf 的手段有那些
4、XXE 原理，XXE 实现过程，XXE 页面没有回显怎么解决，XXE 可以 getshell 不
5、完整的渗透思路
6、你知道 Nmap 那些参数 （三次握手是用哪个参数）
7、BURP 常用的模块
8、知道内网渗透吗？拿到 webshell 入侵内网第一步该干什么
9、sql 如何写 shell
10、知道那些提权的方式，怎么提权的
10、命令执行常用函数
11、反序列化函数，java 反序列化 用那些类
12、CSRF 原理 怎么防御 ，渗透思路 平时怎么挖漏洞的

50 套

1、udf 提权
2、命令执行与代码执行的区别
3、文件包含利用姿势
4、漏洞复现
5、sqlserver 的注入相关
6、预编译怎么进行 sql 注入
7、内网的正向代理和反向代理
8、mimikatz 的使用
9、目标出不了内网咋办
10、如何绕过 disable_function
11、mysql 进行写 shell 的方法
12、redis 的漏洞利用相关
13、sqlmap 的 os-shell 写了哪些文件
14、最近在研究啥
15、免杀
16、java 的相关的反系列化

51 套

1、CDN 绕过
2、站库分离判断，站库分离渗透思路
3、floor 报错注入原理
4、sqlmap os-shell 原理
5、tamper 脚本写过吗
6、Linux　root 无法写 shell
7、mssql 注入
8、oracle 盲注，dnslog 注入
9、绕 waf 有没有研究过
10、如果没有 union select，怎么进行写文件
11、如果不能使用 into outfile，又该如何写 webshell?
12、burp 中数据包参数加密如何爆破
13、文件上传
14、ssrf 绕过
15、验证码绕过，对应后端代码可能是怎么实现的
16、App 测试中证书校验，代理检测如何抓包
17、App 客户端测试方法了解吗
18、App 动态调试了解过吗
19、udf 提权原理，前提
20、Linux 提权
21、免杀研究过吗
22、蚁剑有自己尝试过改装吗
23、常见组件目录位置和敏感配置文件位置有自己总结过吗
24、redis：无写权限如何利用、主从复制 RCE、写入定时任务无法执行可能是什么原因
25、ssrf+redis 禁用 gopher 如何利用
26、内网渗透思路流程 域渗透-非域渗透
27、内网渗透快速判断网络拓扑
28、后渗透工具用的熟练吗
29、java 写的多吗
30、PHP 反序列化，魔术方法
31、ThinkPHP
32、PHP 代码审计：审计工具，审计思路流程
33、有实际审计过什么 cms 吗
34、写过什么小工具吗
35、复现过什么漏洞吗，举例
36、SRC/CTF/实际渗透经历
37、中间件问题

52 套

1、根据简历上来问
2、MVC 框架详细说一下
3、详细介绍一下 sql 注入，原理、条件、分类等等
4、xss 与 csrf 的区别
5、csrf 的原理以及如何防范
6、还有什么你擅长的但是没有问道
7、讲一下 xxe 的原理
8、xxe 会用到哪些函数
9、文件上传
10、常见的 web 容器有哪些
11、apache 7、0 文件上传黑名单怎么绕过，详细说说
12、htaccess 文件绕过、win 文件流绕过（隐写）
13、密码学的对称密码与非对称密码有哪些
14、md5 是不是对称加密
15、apache 可以执行 php 文件吗
16、了解哪些数据库
17、说说反序列化的原理
18、xxe 有没有实战过
19、java 的多线程
20、python 有过哪些项目，写过什么东西
21、python 学到什么程度

53 套

1、sql 注入基于利用方式而言有哪些类型？
2、sql 注入写马有哪些方式？
3、oracle 注入除了注入数据之外有哪些直接利用的方式？，sqlserve 获取 shell 的方法？
4、xss 的利用方式
5、同源策略的绕过方式
6、完整的渗透测试流程思路
7、如何绕过基于语义检测的 waf，比如雷池，阿里云 waf 等(不是太理解语义这东西，说了一些我知道的绕过场景)
8、问了预编译场景下是否存在 sql 注入
9、编程问了个多线程和协程的区别。
10、黄金票据和白银票据的区别？
11、pth 中 LM hash 和 NTLM hash 的区别
12、CDN 的绕过方式
13、waf 的绕过方式

54 套

1、SQL 注入有哪几种方式
2、那你会绕 SQL 注入的 WAF 吗
3、除了 MySQL，对其他的数据库了解吗
4、XSS，分类
5、反射型和 DOM 型的区别
6、CSRF 和 SSRF 的区别
7、CSRF 有什么应用场景？怎么防御？
8、SSRF
9、XXE
10、写过小工具吗？用的什么语言？
11、你了解过代码审计吗？

55 套

1、jsonp 原理，防御，怎么利用的，什么位置什么功能点
2、cors 原理，防御，怎么利用
3、同源策略，举个例子
4、sql 注入 5、0 之前和 5、0 之后有什么区别
5、sql 注入写 shell 条件
6、csrf 原理，防御，利用

7、csrf 防御为什么要 check refer 字段
8、xss 分为几种类型，具体是什么
9、dom 型原理
10、xss 蠕虫
11、怎么手动判断一个网站是用的什么操作系统(不用工具)
12 常见的请求方式有哪些
13、get 和 head 请求有什么区别
14、常用的扫描器用过那些？有他们也会用 get 或者 head
15、refer 字段是干啥的

56 套

1、内网环境如果只有 cmd 和目标服务器的账号密码，如何确认目标服务器是否能登陆
2、对于 MySQL+PHP+Windows 的环境，如果存在注入，如何提高注入效率
3、mimikatz 是从哪个进程抓的 hash
4、如何在内网环境中找到域控(至少 10 种方法)
5、已知一公司环境存在域控，如果不在域环境内,如何寻找域控
6、内网渗透横向扩展有那几种方法(至少 5 种)
7、内网中，如果拿到一台机器或者多台机器的 hash,如果 hash 没有解出来，还有别的利用方法吗
8、除了通过 445,3389，21，22，23，80，8080，3306 端口上部署的服务拿权限外，还可以通过什么端口什么服务拿到目标机的权限
9、mssql 开启 xpcmd 无法写文件，还有什么方法可以 getshell
10、mysql 的 mof 提权原理
11、udf 提权原理和条件
12、fastjson 利用过
13、黄金票据是

57 套

1、自我介绍
2、工作经历
3、什么时候开始学习网络安全
4、印象深刻的渗透流程（每个 HR 都问）
5、struct2 或典型漏洞原理分析
6、ThnkPHP5、*代码执行有无断点调试
7、XSS 种类及其原理
8、CSRF 防御
9、sql 注入防御代码层面
10、判断服务器处于工作组还是域环境
11、真实渗透过程
12、后渗透了解吗
13、反序列化漏洞
14、非关系型数据库和关系型数据库有哪些

58 套

1、SQL 的存储引擎
2、SQL 注入写 shell 的条件，用法
3、GPC 是什么？开启了怎么绕过
4、Mysql 一个@和两个@什么区别
5、IIS 解析漏洞，不同版本有什么漏洞，还有什么容器解析漏洞
6、wireshark 抓包，数据报经过三层交换机、路由的变化，NAT 协议描述，地址进入内网怎么变化
7、linux 计划任务，黑客隐藏自己的计划任务会怎么做。windows 计划任务怎么设定
8、挖过最难的漏洞是什么

59 套

1、Burpsuit 怎么去修改返回码？
2、你写过脚本吗？写过哪些？
3、PHP 代码功底怎么样？
4、你代码审计的思路是怎么样的？
5、什么是 DNS 注入？

6、常见的中间件解析漏洞？
7、项目上做过哪些方面的渗透？
8、会写 exp 吗？
9、会写 JS 调试 PHP 吗？
10、有后渗透实战经验吗？如何进行后渗透?（注意一下渗透岗必问，面了几家都问了）
11、mysql,正则匹配过滤 in 后怎么注入?
12、怎么查看真实 ip？怎么绕过云 cloud 邮件服务器。
13、mysql 5、5 版本和 5、0 版本的区别
14、怎么绕 waf？有哪些方法去饶 waf?哪些分块传输能绕 waf，有什么优势。
15、怎么识别 ORACLE 数据库的注入？
16、文件包含和 ssrf 会同时存在吗？
17、有没有分析过最新的漏洞，调试过相应的代码？
18、php 伪协议了解多少？
19、mysql 执行盲注 sleep4s 为什么回显回来是 20s
20、了解 fastjson 相关漏洞吗？
21、apache 最新的解析漏洞是什么？
22、mysql 报错注入有哪些常用的函数？
23、什么是 SSRF，怎么去判断这个点有 SSRF 漏洞？SSRF 有哪些利用方法？
24、什么是 CRLF，怎么去利用？

60 套

1、xss 通常是用来获取 cookie,关于 cookie，你了解多少，有多少属性。
2、cookie 和 session 有什么区别
3、假设有这样一个情景，你通过 xss 可以拿到管理员 cookie，你如何知道后台在哪里
4、如果后台在内网里，你无法登录，那么你该怎么办。如何更大效率的利用这个 xss
5、HTTP 请求方式
6、擅长哪一块
7、有一个网站，存在文件包含漏洞。但是没有上传点。如果是你会怎么利用
8、网络原理，和系统原理这边你怎么样
9、tcp 三次握手，标志位

61 套

1、自我介绍
2、WAF 及其绕过方式
3、IPS/IDS/HIDS
4、云安全
5、怎么绕过安骑士/安全狗等
6、Gopher 扩展攻击面
7、Struct2 漏洞
8、UDF 提权
9、DOM XSS
10、数据库提权
11、怎么打 Redis
12、内网渗透
13、容器安全
14、k8s docker 逃逸
15、linux、windows 命令：过滤文件、查看进程环境变量
16、站库分离怎么拿 webshell

62 套

1、对一个网站进行渗透测试的流程
2、如何分辨各类中间件
3、SQL 注入原理？利用？防御方式
4、SQL 手工注入的过程
5、如何判断 id =1 中的 1 是字符型还是数字型
6、SQLmap 工具的使用?各个参数的含义？是否有完整翻译过官方文档?
7、通过 SQL 注入，我们能够做到什么？
8、Java Web 相关漏洞 反序列化漏洞讲解一下
9、SSRF 漏洞讲解一下？原理？常见漏洞出现点

10、XSS 原理？利用方式？防御方式？
11、手机 APP 渗透经验？
12、CTF 攻防战，做了什么？
13、一个登陆页面 有图形验证码 找回密码 注册功能 你该如何进行测试
14、你最得意的一个 python 脚本
15、Linux 下的命令操作 如查找某个端口的进程号 全盘查找某个特定名字的文件等
16、短信绕过具体展开讲一下
17、XXE 漏洞原理？危害？常见场景

63 套

1、自我介绍
2、主修的编程语言，脚本语言掌握程度
3、跟导师做过的项目（web 渗透，漏洞挖掘和代码审计相关，主要谈的是简历上的学习方向）
4、大致谈了谈内网渗透流程，添加路由，内网扫描，提权，横向，域控提权，后门免杀，权限维持（金票）
5、漏洞相关：sql，xss，csrf，ssrf，xxe，代码执行和命令执行区别，各类逻辑漏洞
6、同源策略，跨域访问
7、cookie 的 httponly,samestie 相关
8、复现过近期的爆出来的漏洞么,复现漏洞的利用方式，利用条件，漏洞原理
9、SQL 注入，XSS 如何绕过 waf
10、最近关注的安全事件
11、你的安全学习路线
12、谈谈对源码审计的理解
13、怎么进行源码审计

64 套

1、安全研究的方面？做过哪些渗透测试的工作？
2、只给你一个网址，如何进行渗透测试
3、SQL 注入，id=1 如何检测？order by 怎么利用？limit 语句怎么利用？盲注有什么？
4、sleep 被禁用后还能怎么进行 sql 注入
5、XSS 可以控制属性怎么利用
6、CSRF 怎么防护？
7、请求头中哪些是有危害的？
8、XXE 的危害？哪些地方容易存在 xxe？xxe 架构方面有没有了解过
9、JAVA 中间件的漏洞，举几个例子？
10、IIS 常见的漏洞
11、python 有哪些框架，其中出现过哪些漏洞
12、业务逻辑漏洞，用户任意密码重置举出有什么例子，因为什么因素导致的？
13、PHP 代码审计？开源的代码审计有没有做过？弱类型比较，反序列化漏洞这种考点在哪？
14、HTTP-Only 禁止的是 JS 读取 cookie 信息，如何绕过这个获取 cookie

65 套

1、SSRF 没有回显怎么测试
2、完整的渗透测试流程
3、具体的项目经验
4、sql 注入的类型以及流程
5、内网的提权以及代理，隧道

66 套

1、自我介绍
2、ssrf 问的比较深入
3、文件上传绕过方式
4、sql 注入的基本原理，盲注，getshell
5、存储型 xss，如果做到最大化利用
6、信息收集的流程
7、oracle 注入 getshell
8、sqlserver 的提权方式
9、xss 的绕过方式
10、php 反序列化，java 反序列化

11、redis 常见漏洞，利用等
12、代码审计的流程
13、问我有没有学过 python，语言了解哪些
14、正反向代理
15、内网渗透了解哪些

67 套

1、tcp 三次握手原理
2、xss 原理，挖掘思路
3、sql 注入扫描工具思路
4、逻辑漏洞平行越权原理，思路
5、针对网站的渗透思路
6、开头问了下专业课。
7、python 多线程，高并发，什么时候有效，什么时候没用。
8、问了个递归和迭代一定条件下是否可以替换
9、问了下二分查找的时间复杂度
10、又问了关于 sqlmap 是否研究过

68 套

1、mysql 注入，已知 information、schema 相关表在代码层中被过滤，不考虑绕过情况，还可以怎么查询表名或字段
2、mysql 注入中基于报错注入的多种方式
3、前端 xss 如果特殊字符输出被 htmlscecial 过滤如何利用
4、同源策略是啥，rerfer 检测，前端空 rerfer 防御，怎么构造
5、jsonp 是什么，怎么绕过
6、sqlmap 源码是否分析过
7、tp 漏洞复现
8、java 反序列化 rmi 原理(简历上有写)，其他类型的反序列化是什么
9、如果让你编写一个 DOM 型 xss 扫描器，你该怎么写？假如事件需要点击，比如 onclick 去点击，该怎么检测这种类型的 xss
10、内网渗透流程和方式，比如域渗透
11、windows10 上面的 pth 怎么利用
12、linux 主机留后门的各种方式
13、DNS 隧道搭建方式
14、数据结构，算法，计网基础(非计科类专业自闭)
15、知识面深入，内网探测高危服务除了端口扫描还有啥？
16、渗透方向能力目标，学习的新方向。

69 套

0、自我介绍
1、编写工具的具体思路，sql 注入，xss
2、csrf 的防御， referer 验证，referer 为空则防御(referer 是浏览器特性，为空排除特性之外的问题则做防御验证)
3、xxe 无回显探测 dns 验证，内部实体探测
4、xss 硬编码如何利用
5、java 反序列化基础
6、白盒审计能力问题
7、密码重置处的逻辑问题

70 套

0、自我介绍
1、xss 概念
2、dom xss 和反射型 xss 的区别
3、csrf 防御方法
4、sql 注入概念
5、order by 注入、limit 注入、二次注入
6、时间盲注以及不能直接延时的 bypass 方式
7、sql 注入的防御措施以及这些措施可能出现的问题，如预编译是否能防御所有攻击，可能出现什么问题

8、mysql getshell 的几种方式
9、Oracle、sql server
10、javascript 原型污染以及关于原型链的一些细节问题
11、java 反序列化
12、java 任意文件读写怎么挖掘，以及关于文件 io 的操作
13、php 反序列化，魔术方法，pop 链挖掘以及如何绕过__wakeup__
14、php 文件包含，变量覆盖（涉及的相关函数)
15、渗透测试流程
16、渗透测试过程中如何维持权限，扫描内网服务
17、如何快且准确的扫描内网服务
18、windows 主机渗透，怎么创建 Administrator 用户以及隐蔽措施
19、同源策略
20、进程和线程的区别
21、python 协程，异步操作
22、python GIL 锁
23、python 模板注入
24、django、flask 框架漏洞挖掘
25、浏览器安全
26、docker 原理
27、docker 逃逸，挖掘方法
28、信息内容安全
29、xxe 原理、利用以及无回显的利用
30、ssrf 原理，利用，bypass 方法
31、如何利用 ssrf 攻击内网服务，如 mysql 以及利用条件
32、爬虫，比如 headless browser
33、安卓客户端抓包，如捕获不到数据包怎么解决
34、mvc 模式，以及 mvc 框架应用的漏洞挖掘思路
35、src 挖掘过的漏洞
36、逻辑漏洞挖掘思路，如任意账号登陆，利用第三方认证等等
37、漏洞自动化挖掘的思路
38、漏扫和普通扫描器的区别以及开发思路
39、Padding Oracle Attack
40、对称加密和非对称加密的区别
41、Hash 技术以及常用的 hash 算法
42、HTTPS 协议

71 套

1、自我介绍
2、最近做的 CTF 赛题
3、二次注入的防御措施
4、代码审计的思路
5、如何快速定位攻击流量和漏洞利用点，以及攻击溯源
6、威胁情报
7、爬虫与反爬虫
8、应用安全测试经历，以及快速测试大量应用的解决方案
9、使用过哪些扫描器，各自优缺点

72 套

1、自我介绍
2、挖洞经历，主要工作介绍？挖掘漏洞的生命周期？在做漏洞挖掘过程中有没有什么漏洞？RCE 的利用链是怎么样的？
3、跨域有哪几种方式，JSON 跨域呢？
4、说说在漏扫平台这部分的工作？对比很多家的漏扫平台，你觉得他们的不足点在什么地方？漏洞的更新/维护方面有什么想法？
5、Python 的装饰器/生成器/迭代器
6、说说 webshell 检测
7、讲讲遇到的攻击路径还原过程入侵的利用过程
8、讲讲漏洞挖掘这部分的工作？
9、职业规划？

73 套

1、自我介绍
2、怎么排查发现自己是否被中了 webshell？
3、windows、linux 应急搞过吗？
4、有接触过二进制攻防吗？
5、内网渗透有无实战过？
6、在长亭都做些什么工作？
7、说一下你一般是怎么信息收集的？
8、你是怎么判断这个网站使用了哪个 cms 的？
9、java 学的怎么样？
10、入侵排查有没有什么思路？

74 套

1、自我介绍
2、各种 web 漏洞的原理、进攻及防御技巧
3、jquery 库里面有一个函数可以直接导致 xss 的是哪个函数？
4、一般有哪些熟悉可以导致 xss？
5、文件上传你都有什么思路？
6、做了这么多代码审计，你有什么独到的方法？都用什么工具？seay 那个工具的原理有了解过吗？
7、有想过挖洞自动化吗？
8、讲一讲同源策略，跨域都有什么方式？
9、讲一讲你对 jsonp 的了解？还有 cors 一般都会有什么漏洞？
10、csp 是干嘛的？有啥绕过姿势吗？
11、给你一个网站，你一般是怎么做渗透测试的？一般会挖什么类型的漏洞？
12、那对于甲方来说，你觉得怎么来对一个网站做好防护准备？
13、平时会对一些新的漏洞进行跟进甚至分析吗？

75 套

1、自我介绍
2、讲一讲同源策略/SSRF/CSRF/XSS
3、反射型 XSS 和 DOM 型 XSS 的区别
4、变量覆盖漏洞涉及的主要函数
5、对 RPO 漏洞的理解
6、讲一道印象深刻的 CTF 题
7、讲一讲代码[审计]()的思路
8、讲一讲 csrf 如何防御
9、有没有做过[数据分析]()
10、https 的工作原理

76 套

1、xss 类型，具体利用方式如钓鱼怎么实施，防御
2、csrf 攻击，具体利用方式，防御
3、sql 注入攻击以及防御（最基础的那种
4、php 反序列化，常用魔术方法以及 pop 链挖掘思路
5、tcp 是怎么实现可靠传输的

77 套

1、简要做个自我介绍
2、说说白盒你做的工作？思路？检测率？误报率？
3、安全能力建设的工作？
4、webshell 检测？
5、挖矿检测？特征提取？检测模型？使用的方法？效果？实验对比？
6、白盒做的工作？
7、能力建设的工作？
8、黑盒的工作？
9、说说命令注入反弹 shell 的方式？如何绕过 HIDS？
10、代码实现黑盒命令注入？的检测思路？如何降低非预期？

78 套

1、说一下 http referer
2、sqlmap 如何扫 post 注入，如何批量扫描？
3、sql 注入了解吗？盲注流程讲一下，除了 sleep 函数还有什么？如何 getshell？
4、xss 的原理，如何防御？
5、csrf 的防御
6、ddos 的原理
7、webshell 已经上传如何禁止菜刀等工具连接
8、讲一下文件上传
9、使用过哪些漏扫工具
10、一个互联网网站端口如何防护，发现入侵如何解决？
11、渗透测试流程
12、TCP/IP 四层模型是哪四层
13、linux 查看某个服务
14、linux ssh 日志放在哪个目录
15、如何查看用户？
16、nat 常用的两种模式
17、应急响应

79 套

1、自我介绍一下
2、举一个你安服印象最深刻的例子，是怎么最后一步拿下这个网站的？
3、给你一个整个目标，你会怎么去渗透呢？
4、你拿到一个 shell，你一般会干什么？
5、讲一讲逻辑漏洞、越权问题？你会怎么去测试一个网站有这些漏洞？你有什么方法去测试这些漏洞？说一下你尝试的步骤？
6、问一下 XSS，你会怎么去测试 xss 的问题？script 过滤了咋办
7、你了解 csp 吗？绕过方式有哪些？
8、平时挖过 ssrf 的漏洞吗？防御怎么日？
9、研究过反序列化漏洞么？调用链有什么好办法去找吗？
10、做过代码审计的东西么？你一般会怎么去审计呢？
11、你擅长挖什么样的漏洞
12、反序列化搞过么
13、自己有写过什么工具么

80 套

1、自我介绍
2、分享一个挖掘漏洞的例子
3、渗透和挖掘漏洞都有接触吗
4、挖掘一个网站安全问题的思路
5、描述一下 ssrf 产生的原因和危害
6、设计一个工具自动化测试 ssrf 的思路
7、设计一下防御方案
8、测试一个系统水平越权的思路
9、分享一个最有挑战性的渗透经历
10、有没有做过代码审计的工作
11、给一个 CMS 做白盒审计的思路
12、用污点跟踪的思路挖掘 sql 注入的思路

81 套

1、自我介绍
2、你比较擅长黑盒测试还是白盒审计
3、比较擅长挖哪些漏洞
4、文件上传绕过的原理
5、介绍一下原型链污染
6、python 的模板注入的原理
7、反序列化漏洞
8、怎么防御反序列化呢

9、有没有遇到需要给出解决方案的场景
10、怎么发现那个 CMS 的后台漏洞
11、CNVD 的是什么漏洞
12、渗透经历和结果
13、通过纯代码发现漏洞的经历
14、写过什么工具或者脚本什么的
15、用什么语言写的
16、哪个语言更熟一点

82 套

1、自我介绍
2、什么时候开始学的安全？
3、刚学安全的时候觉得什么东西比较困难？现在又觉得什么东西比较困难？
4、之前的实习经历中学习到了什么？
5、在项目期间学习到了什么？（问项目）
6、SSRF 漏洞是什么？怎么修复？
7、JSONP 漏洞了解吗？怎么利用？怎么修复？
8、Java 了解吗？Golang 有反序列化漏洞吗？为什么？
9、RASP、IAST 这些了解吗？
10、打了那么多 CTF，你觉得哪些是含金量高的呢？
11、Docker 逃逸？
12、有哪些你觉得你厉害的但是我没有问到的？
13、分别介绍一下三种 xss 类型
14、怎么自动化检测 DOM XSS
15、复现过哪些 CVE，详细讲讲过程
16、开发语言主要熟悉什么？分别写过什么项目？
17、以后期望做安全研究还是产品研发？

83 套

1、自我介绍
2、怎么防御 JSONP 漏洞
3、怎么伪造 Referer 头为空？
4、富文本 xss 和 普通的 xss 在防御时有什么不同？
5、xss 的防御措施(包括减轻危害的措施)，具体展开说说。
6、SSRF 攻击 redis 的手段有哪些？
7、SQL 注入漏洞一般会怎么绕过？
8、伪随机数漏洞，能否具体说说？你是怎么伪造出和目标环境一样的 Cookie 的？
9、SSRF 在不考虑协议限制的情况下怎么去 getshell?
10、具体说说 Redis 怎么 getshell?
11、说一说怎么防御 SSRF 漏洞？
12、具体说说怎么去绕过一些 SSRF 漏洞的限制？
13、在 SSRF 漏洞的防御措施中，解析 url 的过程中会不会存在什么问题呢？
14、绕过 SSRF 的方法中畸形 URL 具体指的是哪些呢？
15、具体的说一说你了解的 xss 漏洞，包括原理、利用、以及防御等。
16、xss 的防御中一般来说会使用哪些编码方式呢？
17、浏览器的解码机制有了解过吗？知道浏览器自解码吗？
18、有了解 mXSS 吗？
19、你觉的你在 SRC 中发现的一些比较有趣的漏洞？
20、说一下你对 SQL 注入自动化检测的理解。 具体怎么去生成检测的 payload？
21、有了解过 RASP 和 SQL 注入结合吗？
22、POST json 的方式能够防止 CSRF 攻击吗？
23、具体说说 ajax 构造 POST 请求的过程

84 套

1、自我介绍
2、webshell 检测，主要做法？同源启发式检测怎么做的？深度学习怎么做的？
3、流量侧能力建设实践过什么漏洞？
4、0day 类型怎么做检测？

5、你有什么问题要问的吗？
6、介绍下渗透的思路？挖到的漏洞场景？挖到的 CVE 介绍下？
7、说一说在安全建设方面做的工作？

85 套

1、证书透明
2、Windows 的 Redis 主从 RCE
3、PTH 怎么利用和 NTML 验证端口是什么
4、git 和 svn
5、CS 怎么联动 C#来进程注入
6、Shiro 有哪些常见漏洞
7、Linux 和 Windows 有什么提权方式，Windows 令牌窃取普通用户可以利用吗，为什么不能利用
8、ThinkPHP3 有哪些漏洞，ThinkPHP5 的路由控制不严谨导致的 RCE 有没有利用过
9、有没有钓鱼经历，如果和室友同在一台路由器下，有什么横向移动方法
10、Windows/linux 权限维持
11、Windows/linux 在管理员权限和没有管理员权限下怎么实现流量代理
12、Windows/linux 提权思路
13、简述一下 windows 委派控制
14、小离发现了一个 AD target，可是 shell 是本地用户，请问小离接下来该怎么继续进行横向
15、工作组如何定位运维机器
16、域环境如何定位目标机器
17、在内网里怎么利用 dnslog 看回显
18、域控权限，目标机器没有开 445 139 3389 等共享端口如何拿下机器权限
19、域控机器有什么攻击方法
20、thinkphp rce 危险函数全禁用，不能日志包含，不能文件包含，怎么 getshell？
21、mysql 和 sqlserver 站库分离的判断方法和渗透思路分别有哪些？
22、在拿到如阿里云或腾讯云主机权限进行远程连接时如何避免触发告警？
23、一个 sa 权限注入，站库分离，而且数据库服务器为断网机，如何实现文件落地并上线？
24、一个普通权限 webshell，在无法提权但有 hash 时如何进行权限提升和内网横向渗透？
25、Mysql 注入拿到 admin 的 hash，比较复杂，没办法解开，有什么思路
26、xss 打到 cookie，但是设置了 httponly，有什么思路
27、免杀，测试过国内哪些杀软，流量加密，内存问题，有些木马能够正常上线，但是一操作就会断开
28、获取一个不在域内的机器权限，如何枚举出域内机器
29、有域管权限，怎么寻找域内用户和机器对应关系
30、拿到一台域内机器普通用户权限，如何快速拿到域控权限

86 套

1、shiro 反序列化他的那个 rember 那个字段参数被检测长度要怎么绕
2、fastjson 遇 waf 怎么绕
3、fastjson 和 log4j 有什么区别
4、内网的时候 fscan 没检测出漏洞的时候，这个时候该怎么办
5、bcel 是什么鬼
6、xp_cmd 命令执行不了是什么原因
7、各种数据库提权方式
8.、站库分离情况下 这个服务器只是数据库 假设当前是数据库 root 权限，该如何去提权？
9、shiro 反序列化爆 key 出来，但是利用链每一个都不能用可能是什么原因
10、数据库里面如何搜索有管 admin 的信息
11、xp_cmd 执行不了命令绕过
12、内网渗透思路不上线 cs msf 工具
13、横向用什么工具

更多安全岗位面试题（懒的整理了，有空再说吧！）：

- https://github.com/vvmdx/Sec-Interview-4-2023
- https://github.com/BJLIYANLIANG/Security_Service_Interview
- https://mp.weixin.qq.com/s/lBEWvz3IuWzLbHfP4i3SWA
- https://mp.weixin.qq.com/mp/appmsgalbum?action=getalbum&__biz=Mzg2NDY2MTQ1OQ==&scene=1&album_id=2309712886719365121&count=3#wechat_redirect