**①渗透测试**

通过计算机上的授权，模拟黑客攻击攻击，旨在对系统安全性进行评估。需要明确攻击范围，底线和时间，遵守道德规范和法律法规，不得对目标系统进行非法攻击或破坏

Burp Suite（Web应用程序漏洞扫描工具OpenVAS（漏洞扫描工具）Nmap(网络映射器)

目标是发现系统的弱点和漏洞、验证安全策略的有效性、评估安全防御机制的可靠性，以及提高员工的安全意识等

**②CSRF的原理和技术**

攻击者欺骗用户打开恶意页面来获取用户的身份令牌，然后自动发送请求到目标网站，利用用户的身份验证令牌进行恶意操作

通过WEB程序关闭跨域资源共享策略来限制跨域请求2**.**验证请求中的Referer值是否来自合法页**3**.每次用户执行重要操作都需要验证一个随机生成的令牌，并在服务器上验证

**③SSRF的原理和防御方法**

攻击者构造出服务器因提供从其他服务器获取数据的功能发起请求的安全漏洞，攻击者以此来控制这些功能中的发起请求的服务，将其作为跳板来攻击内网中的其他服务

**1**.限制外部请求的访问范围**2**.使用安全网关**3**.加强身份认证和授权**4.**禁用不安全的URL协议**5.**定期检查应用程序日志**6.**使用黑白名单策略7.设置超时和重试策略

**④重放攻击的原理和防御**

攻击者特定的时机重复发送录制的原发包，迫使服务器处理重复的请求，从而实现非法访问和数据篡改等目的

引入时间戳和随机数2.使用加密算法3.实施身份认证4.设置单次有效性和序列号5.采用时间窗口和过期机制

**⑤web类型的漏洞有哪些**

sql注入2.XSS跨站脚本攻击3.文件上传漏洞4.命令执行漏洞5.暴力破解漏洞6.访问控制漏洞7.XML外部实体注入漏洞（XXE）

防御：输入验证和过滤，参数化查询，输出编码，身份验证和授权，加密传输，备份和恢复

定期更新软件安全策略和漏洞库，减少高风险操作

**⑥XSS原理和防御**

攻击者通过漏洞在用户可信任的网站植入了恶意脚本代码，用户访问该页面时，隐私信息被窃取用来执行其它恶意操作

对用户输入进行验证和过滤2.设置HTTP头部中的安全策略字段3.CSP可以限制网页中能够加载和执行的内容来源

**⑦数字证书的工作原理和核心**

利用一对互相匹配的密钥对（公钥和私钥）进行加密、解密操作。

公钥加密技术确保信息在传输过程中的安全性，而身份验证机制则确保只有合法的用户才能持有有效的数字证书

**⑧密码算法相关的对称和非对称**

对称加密算法：使用相同的密钥进行加密和解密

非对称加密算法：不同的密钥进行加密和解密，一把称为公钥，另一把称为私钥

**⑨非对称加密算法RSA的数学原理**

非对称加密算法RSA的数学原理基于两个大质数的乘积难以分解。选择两个大质数p和q，并计算它们的乘积n = p × q。选择一个整数e，使得e与(n)互质，这个e就是公钥的一部分，d × e = 1 (mod (p-1) × (q-1))。这个d就是私钥。

在实际应用中还需要考虑其他因素，如**密钥长度、填充方案**等，以确保其安全性得到充分发挥。可能需要不断**增加密钥长度**来应对潜在的攻击。

**①终端BG个人数据分级分类表(L2中哪两个不能明文存储、L3类数据类型)**

L2中密码和身份验证信息，银行卡信息和支付密码不能明文储存

L3数据类型：个人生物识别信息（指纹虹膜，健康和医疗信息，个人财务信息和税务记录

**②隐私基线相关**

个人隐私保护的一系列基本原则、措施和要求

隐私保护概念：合规性，数据最小化原则，透明度，用户同意，安全性

**③安全的看法**

软件开发中，质量是核心要素，而安全是质量的重要组成部分。安全测试是软件的基石，相当于很多零前的1，如果安全测试没有通过，功能再强，性能再好也是不可靠的。

**④安全规范类的知识的例子**

网络安全（账号密码不明文储存和共享，定期更新软件和系统，收到的可疑邮件和页面弹窗要谨慎点击，）个人隐私保护（个人的身份信息不要轻易泄露，谨慎发布个人和生活地照片），工作场所安全（遵循公司的信息安全规范，如有违规立刻向有关部门或领导出申报或举报）等

**⑤学习了安全方面的新知识**

网络攻击手段和防御措施。攻击手段：XSS跨站脚本攻击，sql注入

XSS跨站脚本攻击：对用户输入进行验证和过滤，设置HTTP头部中的安全策略字段，CSP可以限制网页中能够加载和执行的内容来源 sql注入防御：尽量使用参数化语句，减小用户权限，避免将用户输入直接拼接到sql语句中。

**⑥发现过什么问题，描述下过程**

某些用户在发送包含特定表情符号的消息后，接收方无法正常显示这些表情，而是显示为乱码。初步分析时，我们以为是表情符号的编码问题或者是与接收方的设备兼容性有关。

然而，随着测试的深入，这个问题并不是在所有用户或所有设备上都会发生，它似乎与发送方的账号状态、消息发送的时间以及接收方的网络环境都有关。这让我们开始怀疑这可能是一个更为复杂的逻辑或状态管理问题。为了找到问题的根源，我们进行了大量的日志分析和场景复现。最终，我们发现这个问题是由于一个罕见的并发场景导致的。当发送方在特定时间窗口内（例如，账号状态刚刚更新后）发送包含特定表情符号的消息时，由于系统内部的状态没有同步更新，导致消息处理过程中出现了错误。解决这个问题不仅需要修复代码中的逻辑错误，还需要对系统的状态管理机制进行优化，以确保在各种并发场景下都能保持状态的一致性。这个缺陷的解决过程非常曲折，因为它涉及到多个看似不相关的因素，并且只有在特定的条件下才会触发。这也提醒我们，在软件测试中，我们需要保持开放的心态，不断尝试新的测试方法和思路，以发现那些隐藏在深处的缺陷。

**⑦怎样平衡工作与生活**

明确事情的优先级，从而制定计划，调整好自己的心态，经常和家人同事沟通，保持健康的生活方式，培养兴趣爱好

**⑧和团队同事的关系怎么样，对团队的看法和建议是什么**

和同事之间相处都是融洽和积极，对于新入职的我，大家都是有求必应，有问必答的。我们的团队是一个积极向上、富有创造力和凝聚力的团队，定期召开团队会议，分享工作进展。针对新人开展一些分享学习会就更好了

**①在渗透领域深耕些什么**

对于测试来说，安全测试是必不可少的一部分，以前偏重于功能性能，现在希望积累更深一层的安全测试理论和实践知识，让自己技能更全面

**②觉得自己的优点是什么**

善于和同事之间交流，有极强的时间观念，和对勇于接受新鲜事物

**③对未来的计划是什么**

**④有没有觉得很困难的事情或印象深刻的事情**

**⑤加班多不多，或者你觉得加班有没有必要，怎么看待加班**

不多，有必要，在完成工作的前提下，有时间学习工作相关的更多知识，有助于提高工作效率

**⑥历史工作经历、技能**