渗透测试初级面试题

1. 为何一个 MYSQL 数据库的站，只有一个 80 端口开放？
答:更改了端口，没有扫描出来；站库分离；3306 端口不对外开放。

2. 一个成熟并且相对安全的 CMS，渗透时扫目录的意义？
答:敏感文件、二级目录扫描；站长的误操作比如：网站备份的压缩文件、说明.txt、二级目录可能存放着其他站点。

3. 在某后台新闻编辑界面看到编辑器，应该先做什么？
答:查看编辑器的名称版本，然后搜索公开的漏洞。

4. 审查上传点的元素有什么意义？
答:有些站点的上传文件类型限制是在前端实现的，这时只要增加上传类型就能突破限制了。

5. CSRF、XSS 及 XXE 有什么区别，以及修复方式？
答: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 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。

6. 3389 无法连接的几种情况
答:没开放 3389 端口;端口被修改;防护拦截;处于内网(需进行端口转发)

7. 列举出 owasp top10 2019
答:1）注入；2）失效的身份认证；3）敏感信息泄露；4）XML 外部实体（XXE）；5）失效的访问控制；6）安全配置错误；7）跨站脚本（XSS）；8）不安全的反序列化；9）使用含有已知漏洞的组件；10）不足的日志记录和监控。

8. 说出至少三种业务逻辑漏洞，以及修复方式？
答: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；
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；
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。

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？
答:原因很多，有可能 Web 服务器配置把上传目录写死了不执行相应脚本，尝试改后缀名绕过。

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”，你觉得这里怎样利用？
答:.先爆破用户名，再利用被爆破出来的用户名爆破密码；其实有些站点，在登陆处也会这样提示；所有和数据库有交互的地方都有可能有注入。