更多资料与课程请加微信：chankeedu
前端学习交流群：22396007

1. 听说过XSS么？XSS是怎样的运行机制？用哪些方法可以规避它?

跨网站指令码简称XXS：是一种网站应用程式的安全漏洞攻击，是代码注入的一种。它允许恶意使用者将程式码注入到网页上，其他使用者在观看网页时就会受到影响。这类攻击通常包含了 HTML 以及使用者端脚本语言。

XSS的运行机制：XSS 通过修改 HTML 节点或者执行 JS 代码来攻击网站。

规避：最普遍的做法是转义输入输出的内容，对于引号，尖括号，斜杠进行转义，通过转义可以将攻击代码变成对于显示富文本来说，不能通过上面的办法来转义所有字符，因为这样会把需要的格式也过滤掉。这种情况通常采用白名单过滤的办法，当然也可以通过黑名单过滤，但是考虑到需要过滤的标签和标签属性实在太多，更加推荐使用白名单的方式。

2. 请简述下CSP,描述下它得功能与本质的意义?

内容安全策略 (CSP) 是一个额外的安全层，用于检测并削弱某些特定类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击等。无论是数据盗取、网站内容污染还是散发恶意软件，这些攻击都是主要的手段。我们可以通过 CSP 来尽量减少 XSS 攻击。CSP 本质上也是建立白名单，规定了浏览器只能够执行特定来源的代码。

3. 了解网络安全防护么？说一下CSRF与XXS的区别?

前端通常防护的是CSRF与XXS，CSRF为跨域请求伪造，是一种挟制用户在当前已登录的Web应用程序上执行非本意的操作的攻击方法。

XXS为跨网站指令码是代码注入的攻击，区别在于XSS 利用的是用户对指定网站的信任，CSRF 利用的是网站对用户网页浏览器的信任。

4.请简述一下防范CSRF可以遵循的规则?

- Get 请求不对数据进行修改
- 不让第三方网站访问到用户 Cookie
- 阻止第三方网站请求接口
- 请求时附带验证信息，比如验证码或者 toke

5.请简述出一种方法，基于前端技术对密码安全进行防护?

加盐：加盐的本质，是给原始密码添加字符串，增加原密码长度，对于密码存储来说，必然是不能明文存储在数据库中的，否则一旦数据库泄露，会对用户造成很大的损失。并且不建议只对密码单纯通过加密算法加密，因为存在彩虹表的关系。通常需要对密码加盐，然后进行几次不同加密算法的加密。但是加盐并不能阻止别人盗取账号，只能确保即使数据库泄露，也不会暴露用户的真实密码。一旦攻击者得到了用户的账号，可以通过暴力破解的方式破解密码。对于这种情况，通常使用验证码增加延时或者限制尝试次数的方式。并且一旦用户输入了错误的密码，也不能直接提示用户输错密码，而应该提示账号或密码错误 。