WEB服务器主要做哪些安全措施转发

在浏览器端主要所做的安全措施是身份验证、输入校验

web服务器所做的安全措施为安全配置、异常处理。

应用服务器主要所做的安全措施是权限管理、安全审计。

## xss攻击（跨站脚本攻击）:

允许恶意web用户将代码植入到提供给其它用户使用的页面中。

XSS攻击的危害包括

1、盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号

2、控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力

3、盗窃企业重要的具有商业价值的资料

4、非法转账

5、强制发送电子邮件

6、网站挂马

7、控制受害者机器向其它网站发起攻击

## 短链接风险

是可通过遍历猜解、信息窃取等手段非法获取主体的访问权限标识，并冒充主体实施非法访问。

## 跨站请求伪造

CSRF，全称为Cross-Site Request Forgery，跨站请求伪造，是一种网络攻击方式，它可以在用户毫不知情的情况下，以用户的名义伪造请求发送给被攻击站点，从而在未授权的情况下进行权限保护内的操作。

具体来讲，可以这样理解CSRF。攻击者借用用户的名义，向某一服务器发送恶意请求，对服务器来讲，这一请求是完全合法的，但攻击者确完成了一个恶意操作，比如以用户的名义发送邮件，盗取账号，购买商品等等。