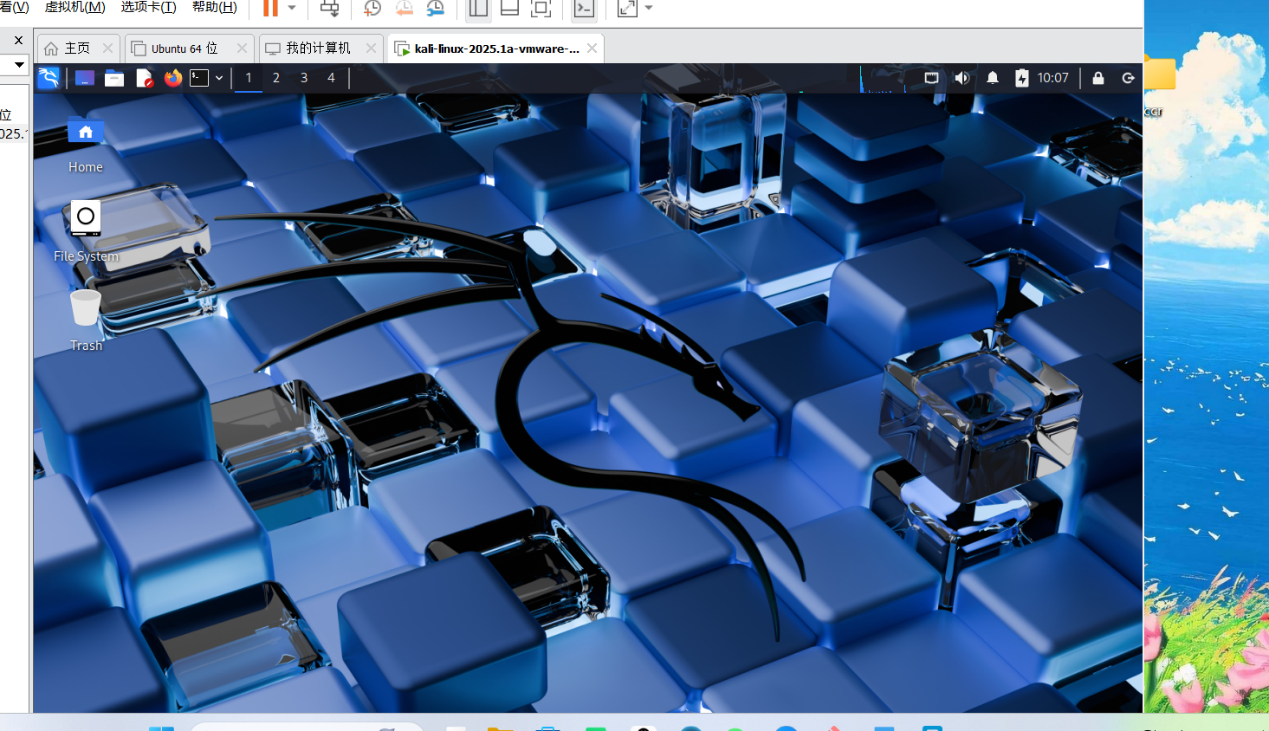
本周安装了vmware 虚拟机

下载了kali

对kali有了初步了解



了解到了xss攻击

大致的意思是

攻击者通过在网页中注入恶意脚本，当用户浏览该网页时，脚本就会执行。

1. 反射型：脚本来自URL参数等，不存储在服务器，一次交互触发。

2. 存储型：脚本存储在服务器，如留言板，危害大。

3. DOM型：基于文档对象型，通过修改DOM结

Csfr漏洞

流程

受害者登录：受害者先登录一个网站，并且此时浏览器保存了该网站的登录认证信息。

攻击者构造恶意请求：攻击者构造一个恶意网页或链接，链接中包含一个目标网站的请求（。该请求看似合法，但实际上是恶意构造的。

受害者点击链接：受害者在不知情的情况下点击了攻击者诱导的链接，或访问了包含恶意请求的网页。

伪造请求被发送：由于受害者已经登录目标网站，浏览器会自动附带上该网站的 Cookie 等身份认证信息，目标网站接收到这个伪造的请求时，认为这个请求来自合法用户，从而执行了恶意操作。

防止CSRF攻击的方法:

使用CSRF令牌：网站可以生成一个随机的CSRF令牌，并在每次用户请求时（特别是POST请求）将该令牌包含在请求中，且每次请求的令牌不同，服务器会验证该令牌是否合法。如果请求中缺少令牌或令牌不正确，服务器就拒绝执行请求。

要求用户输入验证码：对于关键操作，如更改密码或进行资金转账，可以要求用户输入验证码或进行二次身份验证，增加攻击的难度

POST请求而非GET请求：对于可能造成副作用的操作（如修改密码、转账等），尽量使用POST请求而不是GET请求，因为GET请求通常容易被恶意链接滥用。