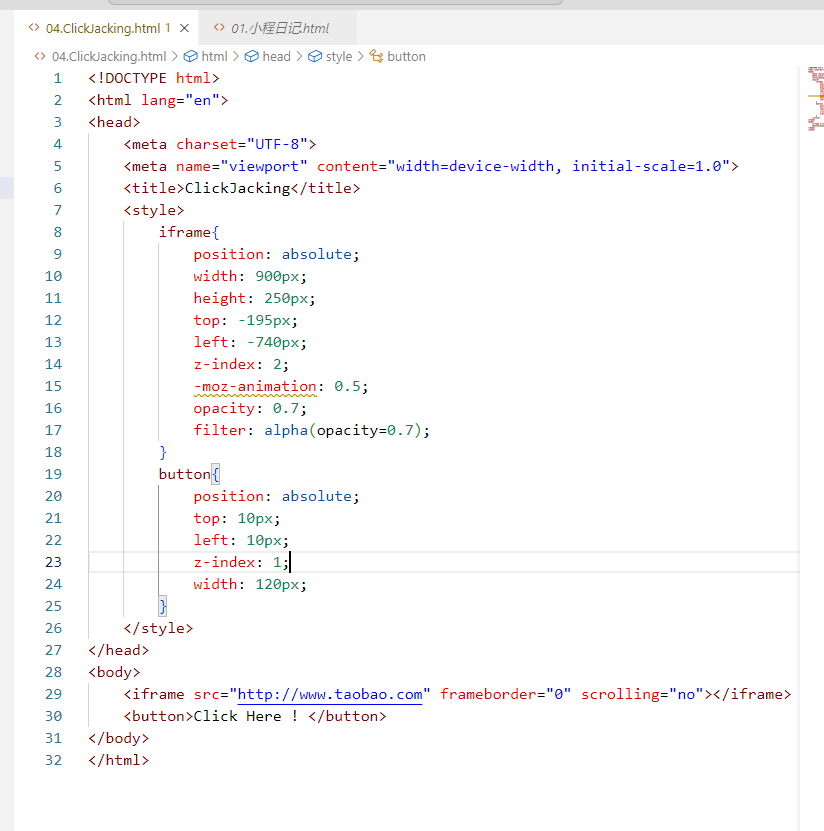
ClickJacking (点击劫持)

点击劫持是一种视觉上的欺骗手段，攻击者使用一个透明的，不可见的iframe，覆盖在一个网页上，通过调整iframe的位置，可以时受害者在不知情的情况下点击到iframe页面上的一些功能性按钮。

<iframe> HTML 内联框架元素，它能够将另一个HTML页面嵌入到当前页面之中。



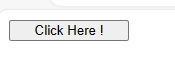
Opacity css 属性 设计元素的不透明度

z-index 设置定位元素的堆叠顺序



当用户想要点击Click按钮的时候，实际上点击了淘宝网页上的内容

只要将不透明度设为0 淘宝页面就完全不可见



点击会跳转到淘宝页面

点击劫持的本质是视觉欺骗

图片伪造也是其中

攻击者将设计好的图片覆盖在原有的图片之中

或者一些图片中设计一些文字，覆盖原有文字，达到欺骗用户的效果

拖拽劫持

触屏劫持

通过将一个不可见的ifname覆盖到当前页面，可以劫持用户的触屏操作。

防御ClickJacking

通常可以写一段js代码，以禁止ifname的嵌套

比如：

If(top.location != self.location)

Top.location = self.location

但是js代码的控制能力并不强，一个比较好的方案是使用一个HTTP头X-Frame-options