**Day 3 03 October 2023**

**Clickjacking**

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause a user to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Clickjacking is for clicks, not for keyboard.

IntersectionObserver is that one that looks at solving the clickjacking problem.

**Old School defense**

Old defense is a bit of JavaScript which forbids opening the page in a frame (so called gramebusting). To me, a lot of writing defensive JavaScript is simply putting up logical safeguards to protect your code from input you might not expect, but will accept.

**X-Frame-Options**

X-Frame-Options can permit or forbid displaying the page inside a frame.

The header may have 3 values:

Deny

Never ever show the page inside a frame.

SAMEORIGIN

Allow inside a frame if the parent document comes from the same origin.

Allow-From domain

Allow inside a frame if the parent document is from the given domain.

**SameSite Cookie Attribute**

Cookies are small strings of data that are stored directly in the browser.

The samesite cookie attribute can also prevent clickjacking attacks.