**Introduction to Clickjacking**

 Clickjacking is a type of web security vulnerability where an attacker tricks a user into clicking on something different from what the user perceives, potentially leading to unintended and malicious actions being performed without the user's knowledge or consent.  
  
Clickjacking can have various consequences, including stealing sensitive information, making the user perform actions they didn't intend to, or even taking control of their accounts.

**Old school defenses (weak)**

 The oldest defense is a bit of JavaScript which forbids opening the page in a frame (so-called “framebusting”).  
  
That looks like this:  
  
if (top != window) {  
  
top.location = window.location;  
  
}  
That is: if the window finds out that it’s not on top, then it automatically makes itself the top.  
  
Blocking top-navigation  
We can block the transition caused by changing top.location in beforeunload event handler.  
  
Sandbox attribute  
One of the things restricted by the sandbox attribute is navigation. A sandboxed iframe may not change top.location.  
  
So we can add the iframe with sandbox="allow-scripts allow-forms". That would relax the restrictions, permitting scripts and forms. But we omit allow-top-navigation so that changing top.location is forbidden.

**X-Frame-Options**

 The server-side header X-Frame-Options can permit or forbid displaying the page inside a frame.  
  
It must be sent exactly as HTTP-header: the browser will ignore it if found in HTML <meta> tag. So, <meta http-equiv="X-Frame-Options"...> won’t do anything.  
  
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**

 The samesite cookie attribute can also prevent clickjacking attacks.  
  
A cookie with such attribute is only sent to a website if it’s opened directly, not via a frame, or otherwise.