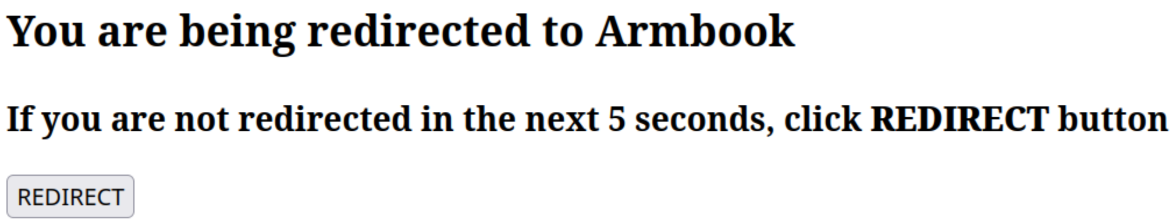
Maxwell Fusco
HW 4 Act 3 Step 2

Vulnerability
This vulnerability being utilized is called clickjacking, this is generally just making users think they are clicking something other than what they are. For the example I provided, it is a redirect page which has a nearly 0 opacity iframe for the armbook on top of the button so that when you hover over the redirect button you are actually clicking “Add Friend”

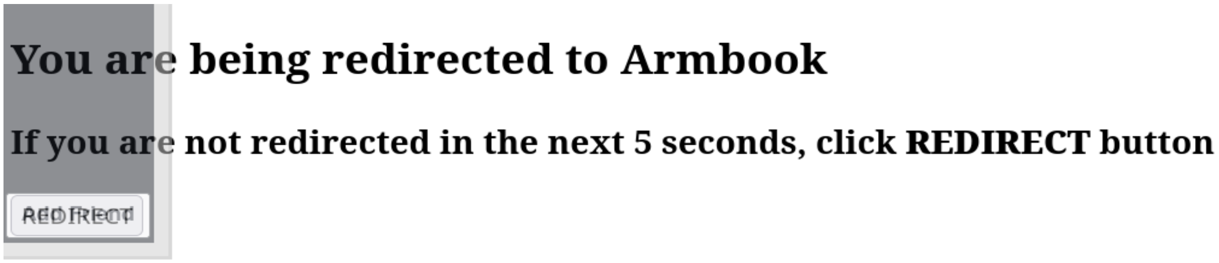
Demonstrations
How page appears:



You are being redirected to Armbook

If you are not redirected in the next 5 seconds, click REDIRECT button

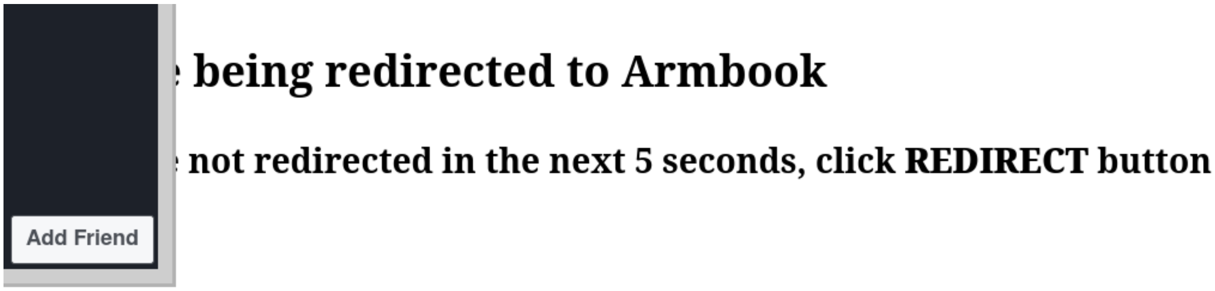
Iframe opacity at 50%:



You are being redirected to Armbook

If you are not redirected in the next 5 seconds, click REDIRECT button

Iframe opacity at 100%:



being redirected to Armbook

not redirected in the next 5 seconds, click REDIRECT button

How to fix:
There are two main ways of preventing these kinds of attacks: (1) implementation of a CSP (Content Security Policy) header or (2) implementing X-Frame-Options header. Both of these options work by preventing the use of a given site from being used in an iframe, except for a certain specified domain you allow (similar to CORS).