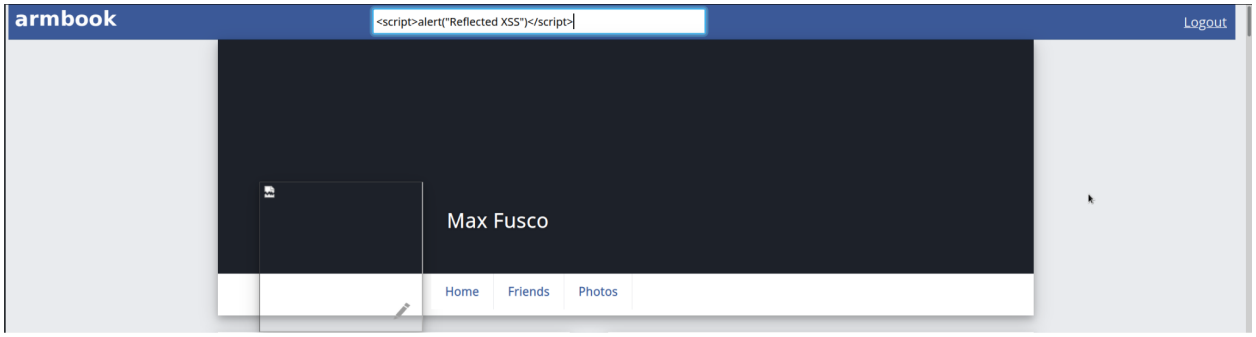
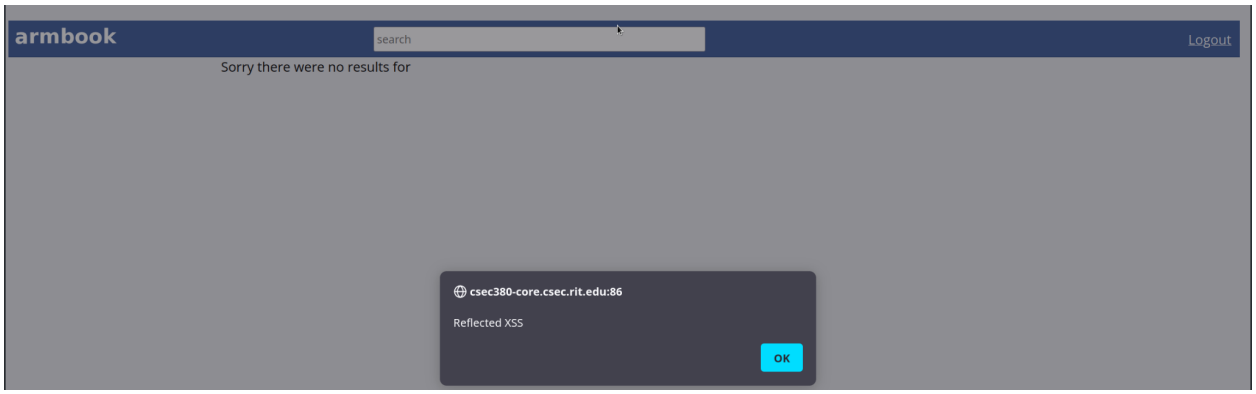
Reflected XSS

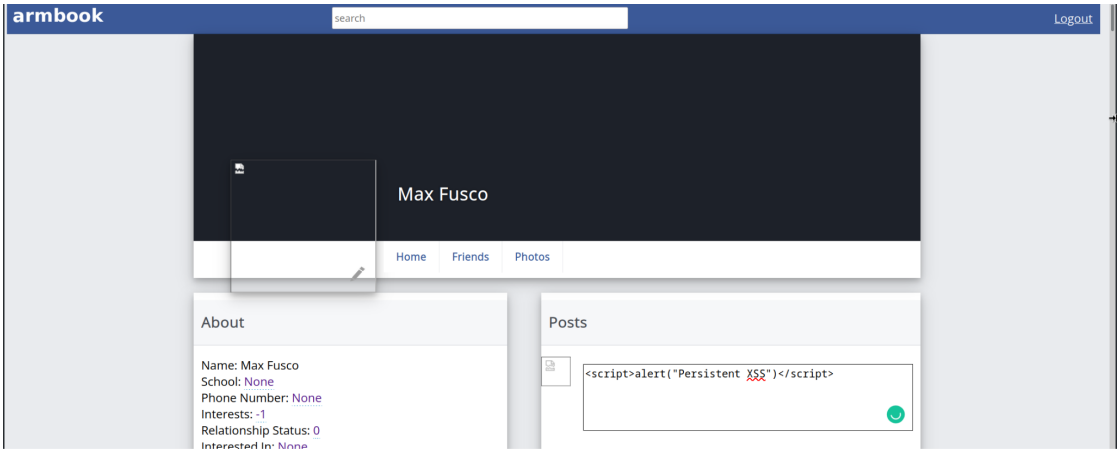


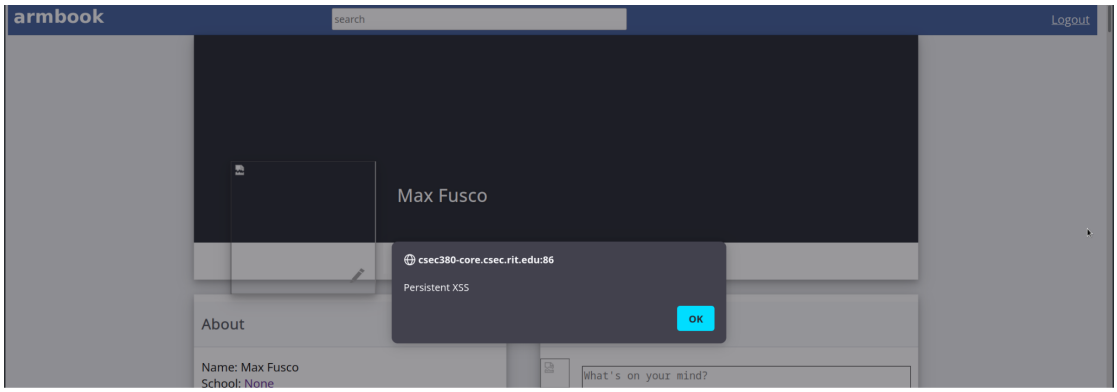


How I found it:
I saw an input field and I entered a simple XSS example and I got an alert from the XSS. I wish I could say there was some more complex thought process, but there really wasn't.

TLDR: I entered '<script>alert("Reflected XSS")</script>' in the search bar and XSS went brrr.

Persistent XSS





How I found it:
I saw that our personal pages had a comment page and figured that would be a decent enough place to perform Persistent XSS. I already had some people posting on my page, so I decided that I would get rid of previous comments. To do this I entered ‘<!--’ to comment everything out below and then proceed. All that was needed was to enter ‘<script>alert(“Persistent XSS”)’ and now it comes up on my page all the time.

Similarly I used the same concept to make my page dark mode.