Our logic is ALWAYS flawed, humans cannot see the future and we will not see all the vulnerabilities of the logic we implement in the code we write.

Often companies don’t keep good documentation of their software. Of course, employees of any company are constantly rotating in and out as well so if there is not good documentation chances are new devs will have a really hard time building upon existing code. Any time we see new features being added on top of existing ones, or large overhaul updates we should be looking at them very closely as these are often hot spots for these logic vulnerabilities or other types of vulnerabilities.

Another issue is when groups work together on one code base, this can often lead to logic vulnerabilities as many people are contributing to one codebase. Often these codebases are so complex devs will get confused on their own parts of the code so those points where multiple people are contributing to one feature or section of an app are great spots to look for vulnerabilities.

Just really gather as much information on our target app as possible and make it your goal to understand as much of the functionality as possible. Even if you hypothesize and make educated guesses, getting in this type of mindset will help us find bugs.