Common issues I start with & why

When first starting out on a program I tend to stick to what I know best and try to create as much impact as possible with my findings. Below is a list of the most common bugs I hunt for on bug bounty programs and how I go about finding them. I know you are sitting there thinking, "*wait, don't you look for every type of bug?*"and of course I look for every type of issue eventually **but when first starting out**, these are the bug types I focus on. As a hacker you also can not know absolutely everything so **never** go in with the mindset of trying every type of vulnerability possible. You may burn out & cause confusion, especially if new. My methodology is all about **spending months on the same program with the intention of diving as deep as possible** over time as I learn their web application. From my experience developers are making the **same mistakes** throughout the entire internet and my first **initial look is designed to give me a feel** for their overall view of the security throughout the web application. **The trend is your friend**.

To reiterate, on my ***first initial look I primarily look for filters*** in place and aim to bypass these**.** This creates a starting-point for me and a **'lead'** to chase. Test functionality right in front of you to see if it's secure to the most basic bug types. You will be surprised at what interesting behavior you may find! If you don't try, how will you know?

Cross Site Scripting (XSS)

Cross Site Scripting is one of the most common vulnerabilities found on bug bounty programs despite there being ways to prevent it very easily. For the beginners, XSS is simply being able to input your own HTML into a parameter/field and the website reflecting it as valid HTML. For example you have a search form and you enter <img src=x onerror=alert(0)> and upon pressing 'Search' it shows back a broken image