

Yeah. My style is different. I teach practical first and then give the definitions!

There are 3 major types of Exploit codes:-

- **Proof of Concepts** - Incomplete kind of exploits (think of it like long articles) that can tell you where the real flaw is. They generally will only state that the vulnerability can be exploited or not, but won't actually help you to exploit.
- **Public Exploits** - Exploits written by anyone in the community. The writer might be inexperienced and thus the exploit might be unstable and risky to use. Plus, there are often fixes required in order to make these exploits to work. I have seen exploits written in C, C++, Python, Ruby and Perl and many other programming languages.
- **Commercial Exploits** - Exploits written by trusted vendors like Rapid7 or Core Security. They do a lot of research before creating these exploits and these are also tested in multiple environments so we consider them pretty safe. We generally access them in frameworks like Metasploit from Rapid7 or Core Impact from Core Security.

