maybe there's IDOR?! - And from there, **deep down the rabbit hole you go**. You naturally want to know more about this website and how it works and suddenly the hacker inside you wakes up.

If you have no developer experience at all then **do not worry**. I recommend you check through https://github.com/swisskyrepo/PayloadsAllTheThings and try to get an understanding of the payloads provided. Understand what they are trying to achieve, for example, is it an XSS payload with some exotic characters to bypass a filter? Why & how did a hacker come up with this? What does it do? Why did they need to come up with this payload? Now combine this with playing with basic HTML.

As well as that, simply getting your head around the fact that code typically takes a parameter (either POST or GET, json post data etc), reads the value and then **executes code**. As simple as that. A lot of researchers will brute force for common parameters that aren't found on the page as sometimes you can get lucky when guessing parameters and finding weird functionality.

For example you see this in the request:

```
/comment.php?act=post&comment=Hey!&name=Sean
```

But the code also takes the "&img=" parameter which isn't referenced anywhere on the website which may lead to SSRF or Stored XSS (since it isn't referenced it may be a beta/unused feature with less 'protection'?). **Be curious and just try**, you can't be wrong. The worst that can happen is the parameter does nothing.