YIGF CAMBODIA

The Foundation of

Web Security

Hello! I’m Vannkorn

- Full-stack Web Developer

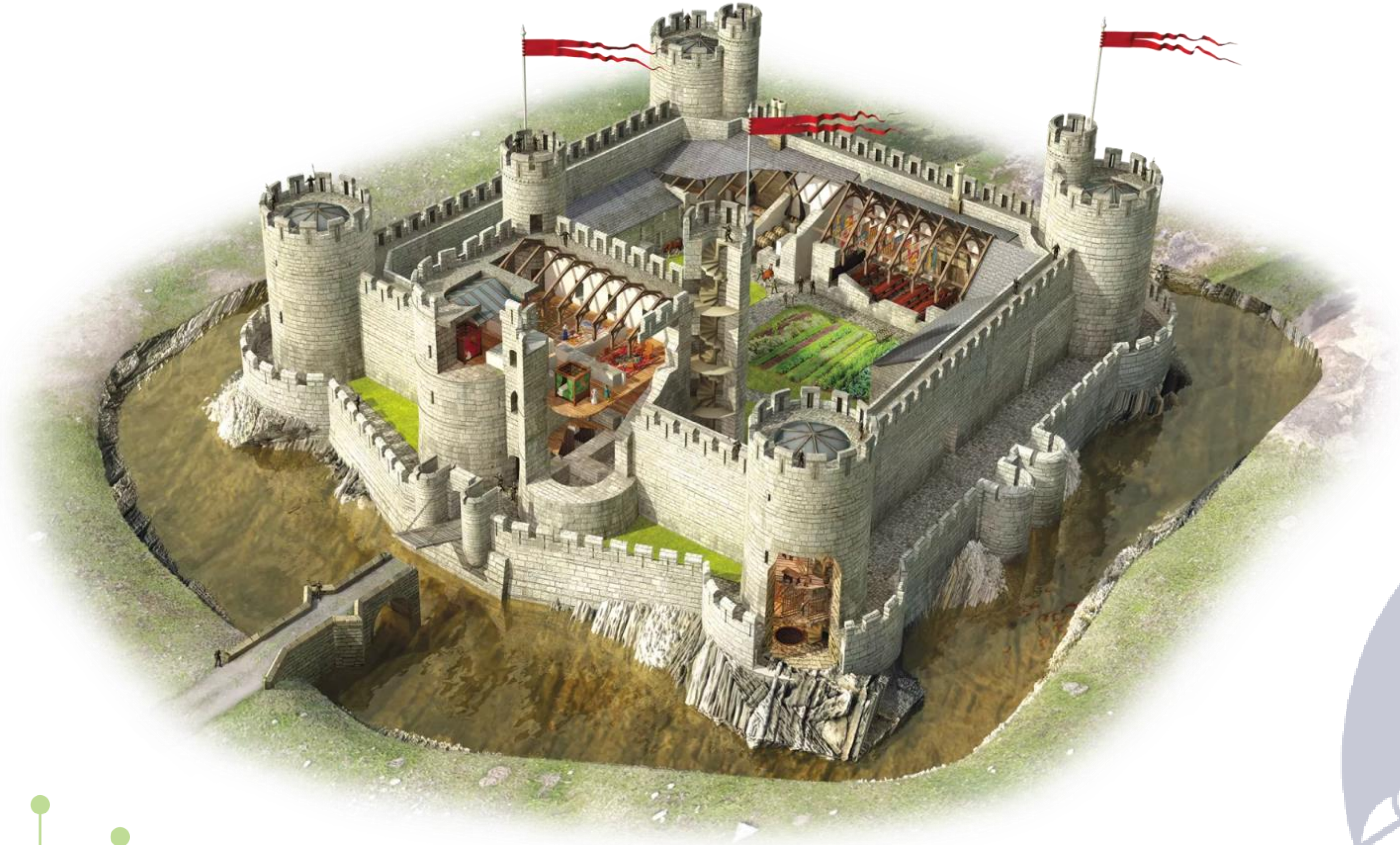
  Specialize in **WordPress** for:

  - eCommerce
  - SMEs
  - NGOs
  - News Agencies, …

Security Overview

- **Security** is not optional.
- **Security** cannot be after-thought.
- Without a **firm grounding**, it can be easy to make mistakes and leave you vulnerable.
- **Security** is an essential skill for all web developers.

Your opinion, what is **Security**?



Security rule of thumb

Security = Awareness + Adequate Protection

- Security is both of the State of being protected and the measures we take to protect.
- However, Total security is unachievable.

Why **Security** Matters?

- As the site **incorporate new features**, it increases complexity and gain security issues.
- Hackers write code that does the scanning and hack for them.
- Maybe they want to make changes to the website, to steal data, or to take complete control of the server.

Security Principles #1

Least Privilege

Least Privilege

The principle of least privilege applies to every program, as well as every user. As such, they can be applied to:

- APIs
- System resources
- Database Access
- Software version control
- Public-Facing web pages

Least Privilege

Always think of:

- Control access to systems and resources.
- You do that by Granting as little access as possible.
- It’s also important to have procedures in place to remove access when it’s no longer needed.

Least Privilege

Jerome Saltzer once said *"Every program and evey privileged user of the system should operate using the least amount of privilege necessary to complete the job."*

Security Principles #2

Simple is more Secure

Simple is more secure

When programming, there are several techniques you can use to reduce complexity, yet increase security.

- Giving clear names to functions and variables
- White code comments
- Built-in functions are better than Custom functions
- Remove Cruft
- Disable features you don’t intent to use
- Breaking long sections of codes into smaller functions
- Don’t Repeat Yourself (DRY)

Security Principles #3

Never Trust Users

Never Trust Users

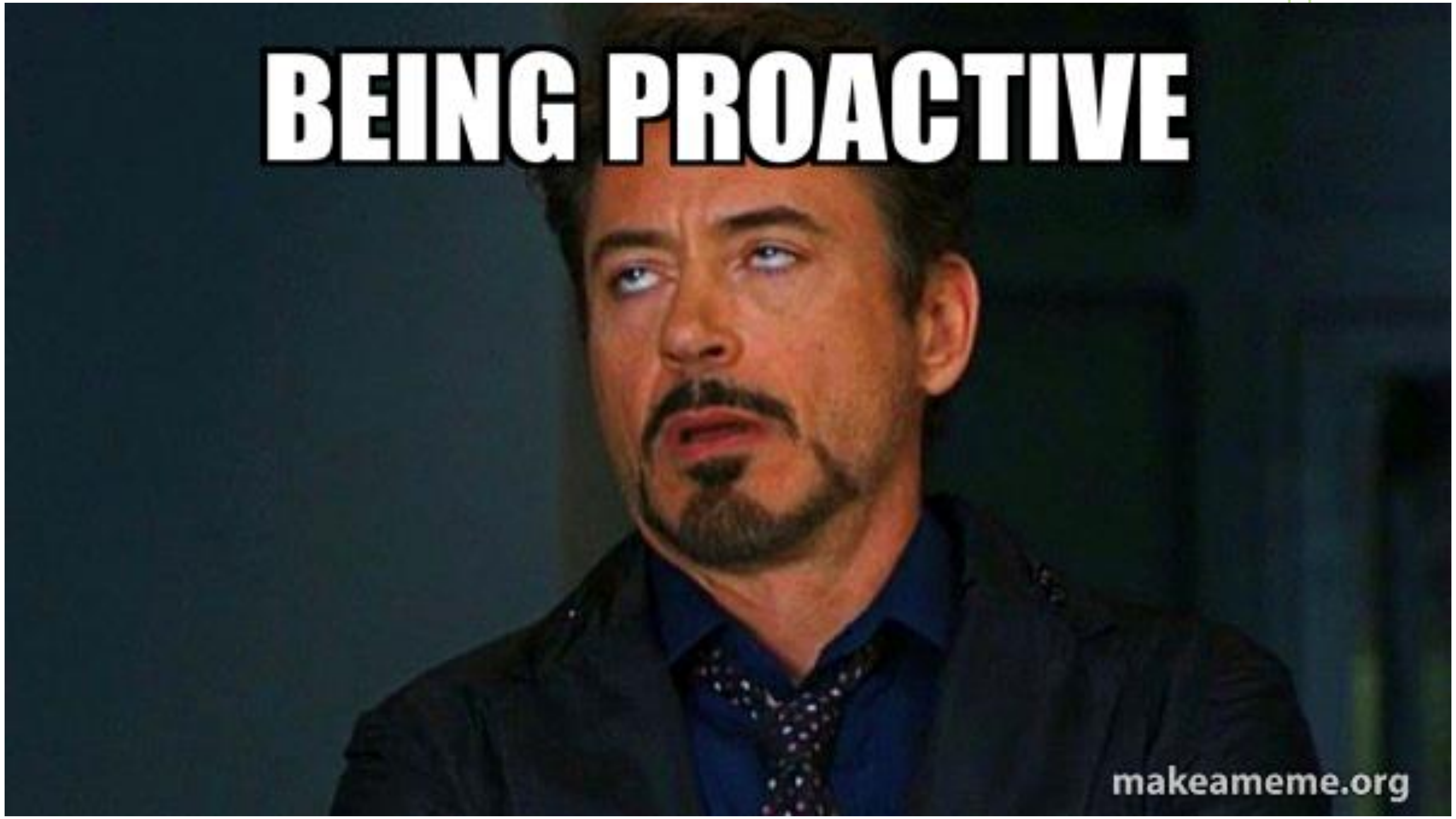
- Every user can be a potential hackers and they can be tricked.
- An accidental click can delete an important file, typo can break the configuration.
- Therefore apply the **Principle of Least Privilege** to every user.

Security Principles #4

Expect the Unexpected

Expect the Unexpted

- Be proactive not reactive
  - What if a user enters no text?
  - What if they enter too much text?
  - What if they paste the formatted texts from their clipboard?
  - Or what if they enter symbols?
  - What if they enter emojis or other ascii characters?


BEING PROACTIVE
makeameme.org

Security Principles #5

Defense in Depth

Defense in Depth

- Defense in depth decreases your reliance on any one defensive measure while at the same time geometrically increasing the difficulty of making a successful attack.
- There are **3** main categories of defenses to consider:
  - Physical
  - Technical
  - Administrative

Physical

Technical

Administration

Thank you!