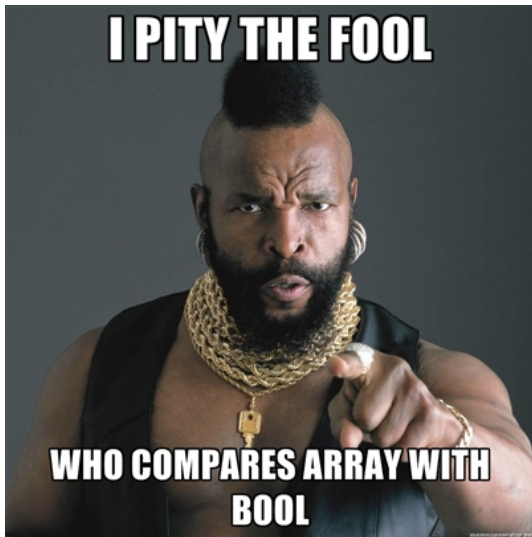




or why you won't code nice things

**I WANTED TO WRITE GOOD
PHP CODE**

**BUT THEN I TOOK AN ARRY TO THE
KNEE**



comparing things

one diamond hidden in php

- the comparison operator compares **and** converts things
 - `123456 == "123456"`
 - `"1e3" == "1000"`
 - `"61529519452809720693702583126814" == "6152951945280972000000000000000000"`
 - `array("foo", "bar") == true`
 - `array() == false`
- All of above statements are evaluated as *true*
- `'0' == false`, `0.0 == false`, `'0,0' == true`

- An example of a php book
 - ① Learn ALL the features of php
 - ② use them in examples
 - ③ and on the last page: the code in the examples isn't safe
- using obscure handlers instead of frameworks
- oop is teached the same way as your parents introduced you to your grandgrand-grand-mother
- php is often selfteached by bad examples found on strange webpages

last slide of security problems

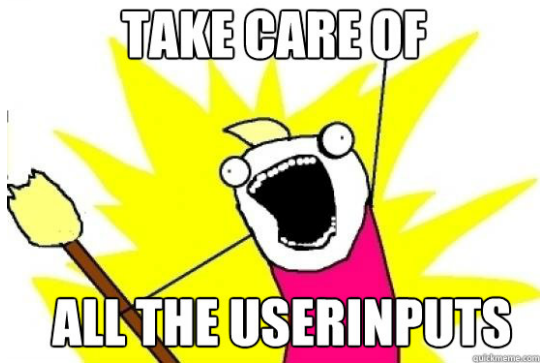
as announced on the previous slide

- the language it self (like any other) don't care about safe, secure and reliable code
- it gives you freedom: if you want to write insecure code, just go an do it
- \Rightarrow a lot of php-applications on the web are **insecure** by default
 - htmlentities
 - input filters
 - escaping the input
- all userInput is evil

last slide of security problems

as announced on the previous slide

- the language it self (like any other) don't care about safe, secure and reliable code
- it gives you freedom: if you want to write insecure code, just go an do it
- \Rightarrow a lot of php-applications on the web are **insecure** by default
 - htmlentities
 - input filters
 - escaping the input
- all **userinput is evil**



- php isn't a bad language
- yes, it has design flaws
- using frameworks will reduce problems
- **but** php makes it easy to do things wrong
- so the user must take care about what he/she/it is doing.

Questions?

don't *think* or even *assume* what php might do.
just **Read The Fucking Manual**

don't *think* or even *assume* what php might do.
just **Read The Fucking Manual**
