The True Art Of Exploiting Logic Flaws - Secure Coding

By: Ahmed Belkahla

f*ck WORD
> Capture the flag <

Whoami

- Ahmed Belkahla @kahla
- CyberSecurity Consultant @ EY
- Network Engineering Student @ INSAT
- CTF Player @ Fword (https://fword.wtf)
- Technical Manager @ Securinets && Ex Vice Chair @ Securinets
- **Personal Blog:** https://ahmed-belkahla.me

ls -la

- Why Logic Flaws ?
- Demo Time
- Secure Coding Practices
- Resources

Why Logic Flaws ?

What’s The Solution ?


LETS GET
CREATIVE
memegenerator.net


HUMANS
YOU ARE THE WEAKEST LINK
imgflip.com

Demos

Can You Spot The Vulnerability ?

Let’s Warmup

These Flaws can be Categorized To

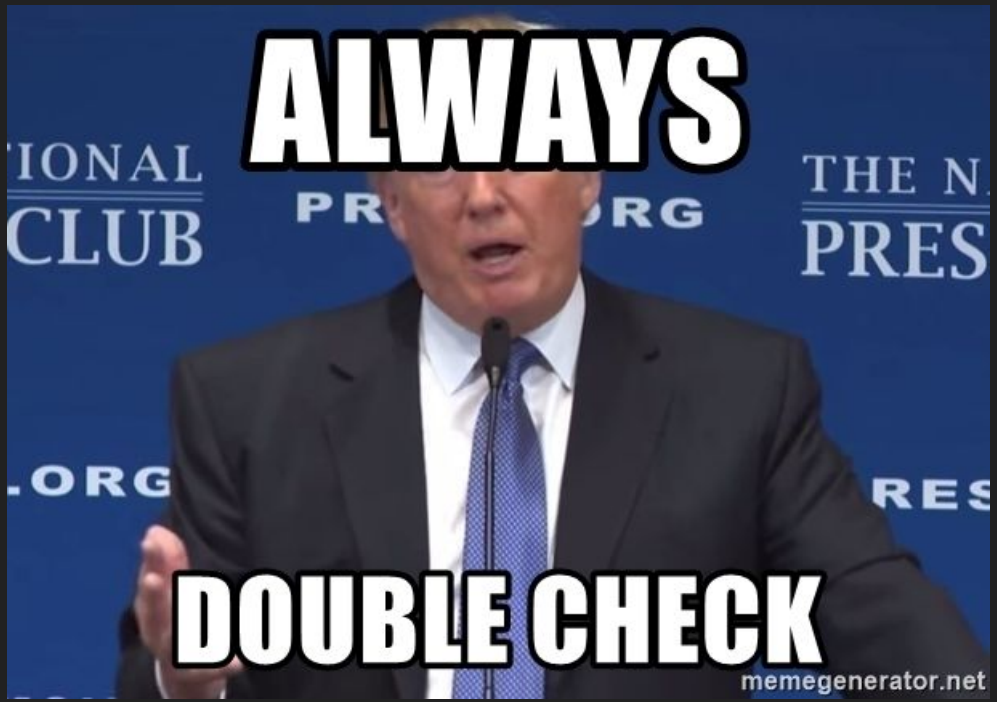
Type Confusion Related Bugs

Solution ?

Always Sanitize User input

Solution ?

Make sure to strictly check variable types



Solution ?

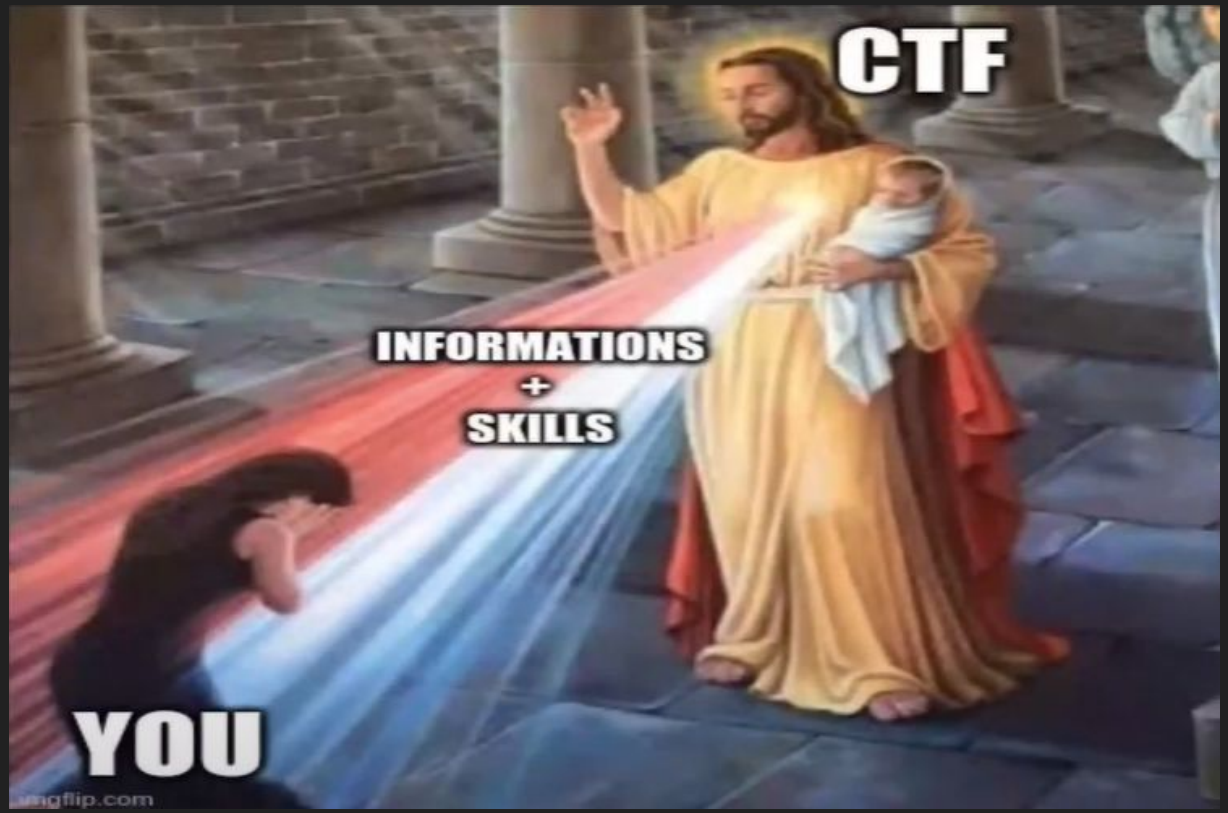
Code Review :D

Resources

Loose comparisons with ==

	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
-1	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
"1"	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
"0"	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
"-1"	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
NULL	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE
array()	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
"php"	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
""	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE

CTF : Capture The Flag



Q & A