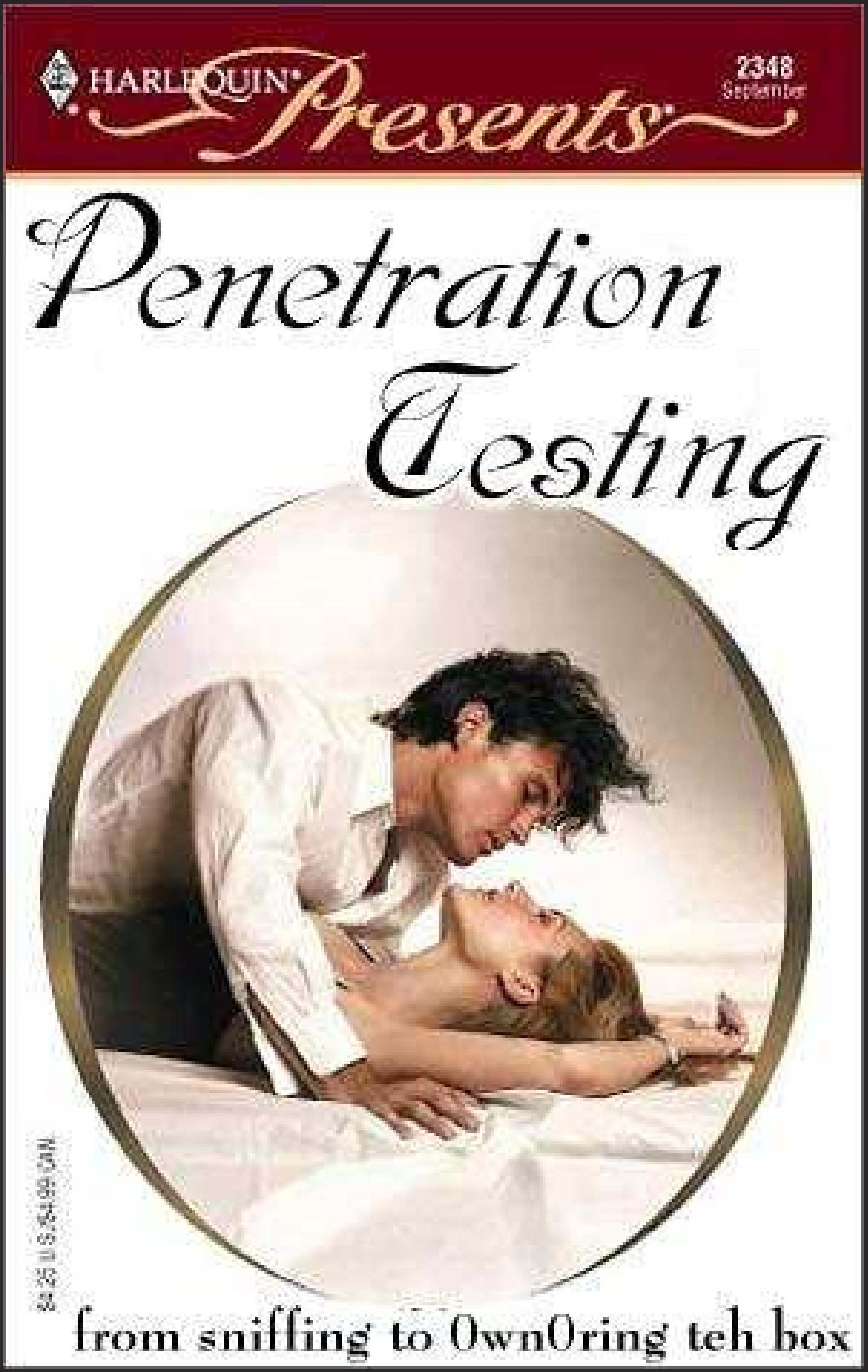
Penetration testing

- OWASP Göteborg 2012-11-22

Robin Blokker
ISA/N

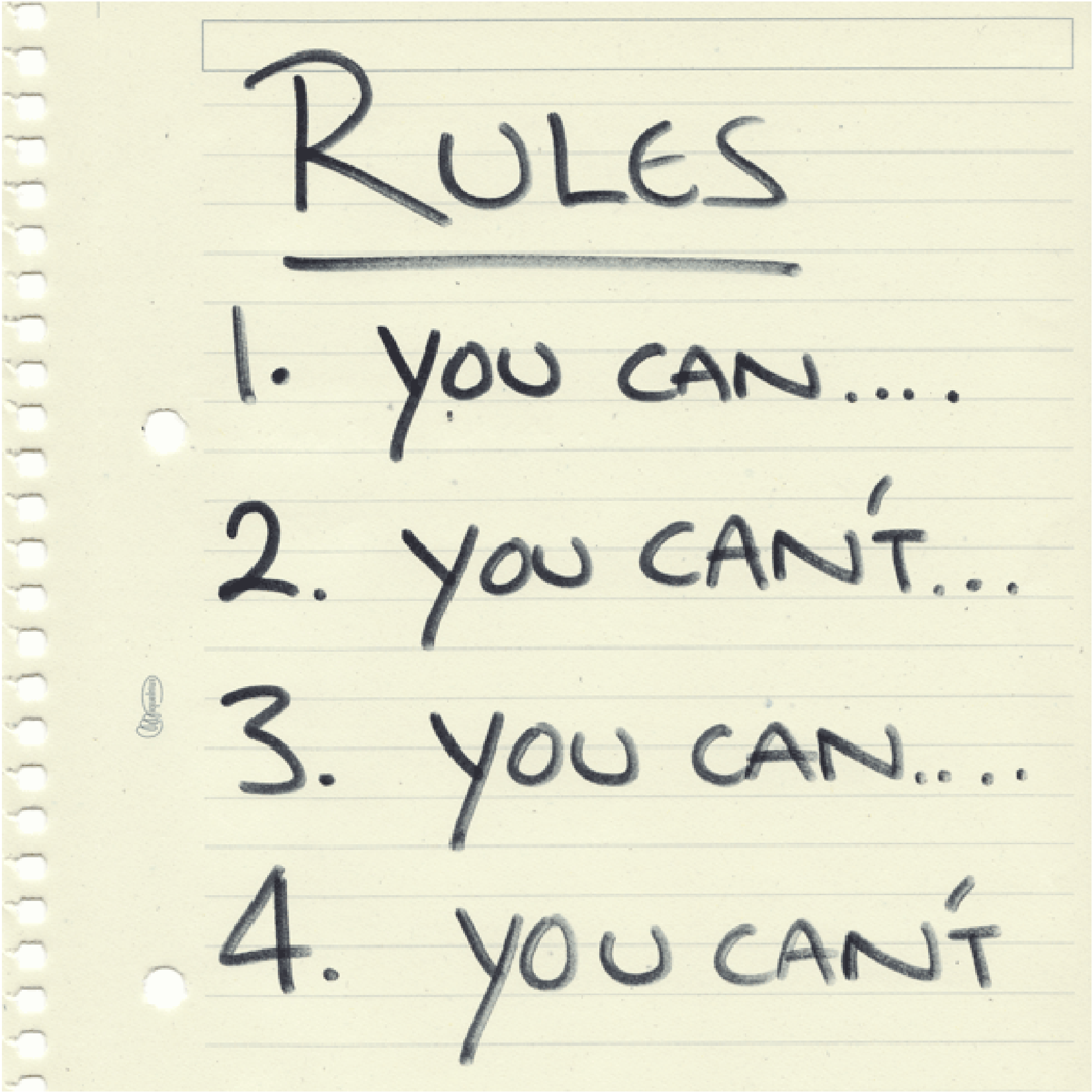
National Defence Radio Establishment


HARLEQUIN Presents
2348
September
Penetration Testing
$4.25 U.S./$4.99 CAN.
from sniffing to 0wn0ring teh box

Golden eggs

Scope

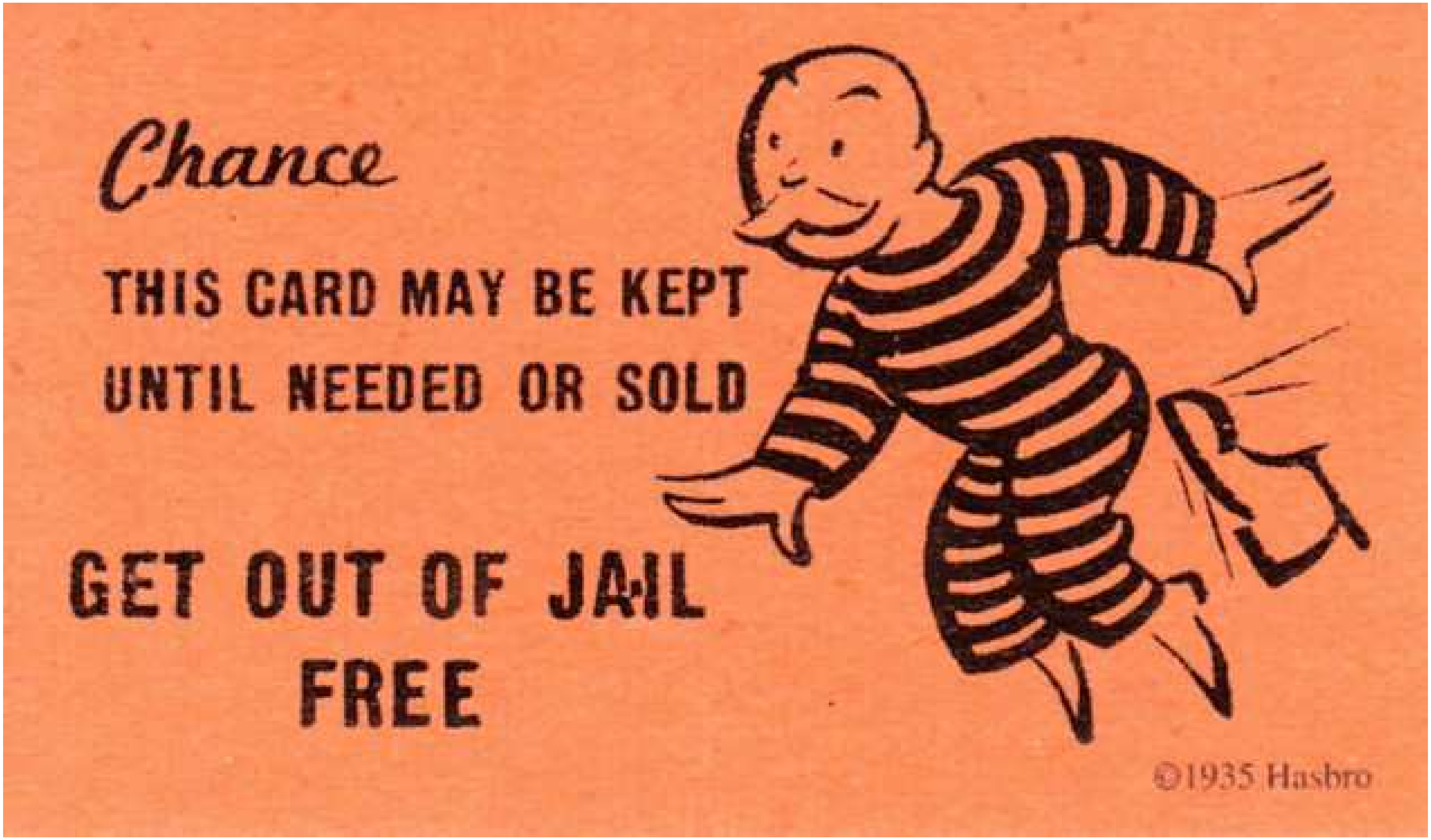
Rules of engagement



RULES

1. YOU CAN....
2. YOU CAN'T...
3. YOU CAN...
4. YOU CAN'T

Contract



Chance

THIS CARD MAY BE KEPT
UNTIL NEEDED OR SOLD

GET OUT OF JAIL
FREE

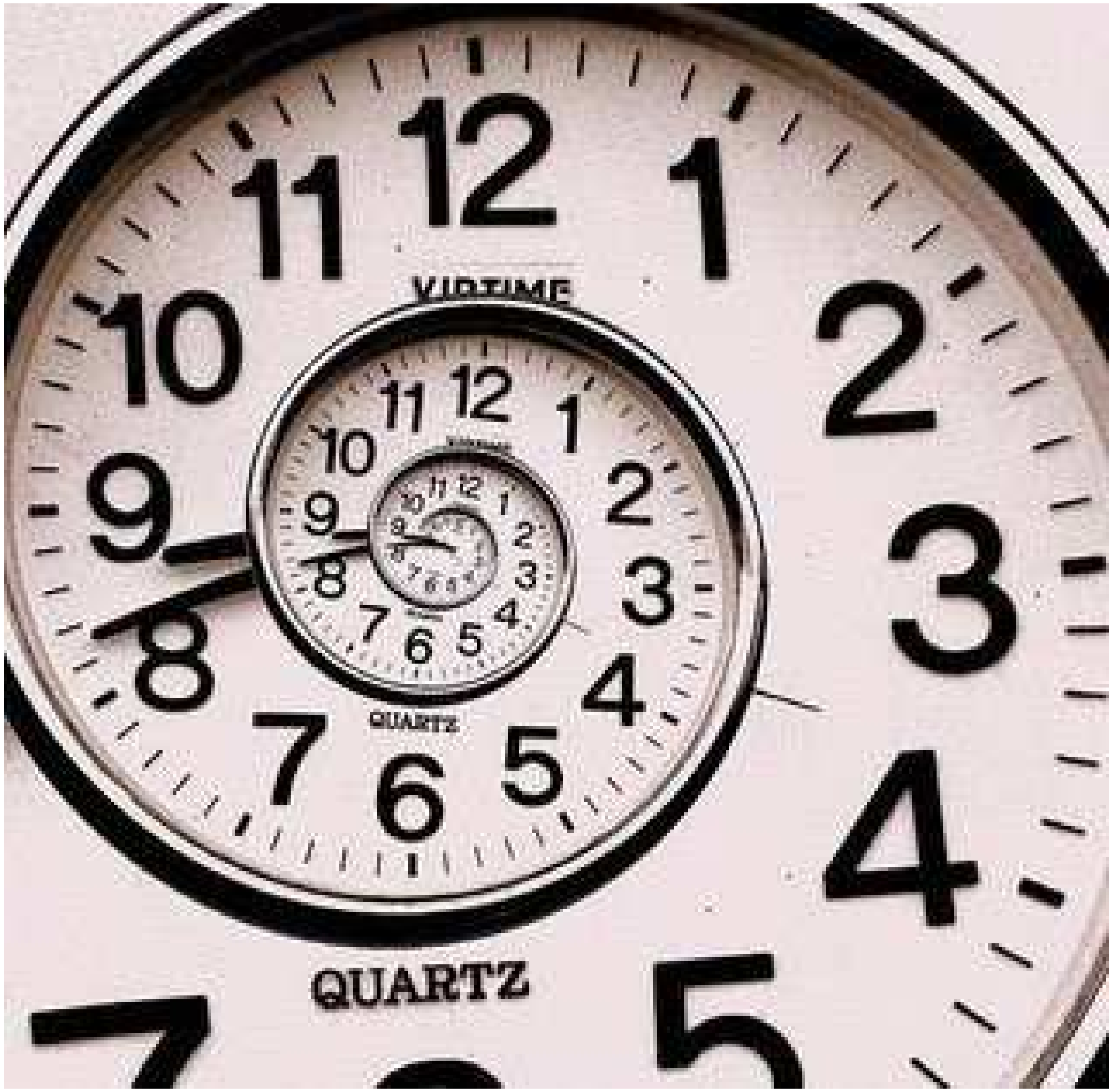
©1935 Hasbro

POC

Respect the natives

Blackbox vs. whitebox

Time



Record

AUTO STOP
commodore
RECORD
PLAY
REWIND
F.FWD
STOP
EJECT
SAVE

Encrypt

Screenshot

Canon
EOS
CANON ZOOM LENS EF-S 18-55mm 1:3.5-5.6 II
CANON INC.
φ58mm
350D
DIGITAL

Logs and monitoring

Find exceptions

Password and account management

THIS LIFE
CREATE NEW PASSWORD?
Tap Tap Tap
'PENIS'
Tap Tap Tap
SORRY– YOUR PASSWORD ISN'T LONG ENOUGH

Account lockout

use exploit/windows/smb/ms08_067_netapi

Patchlevel

Fileshare

Multi function devices

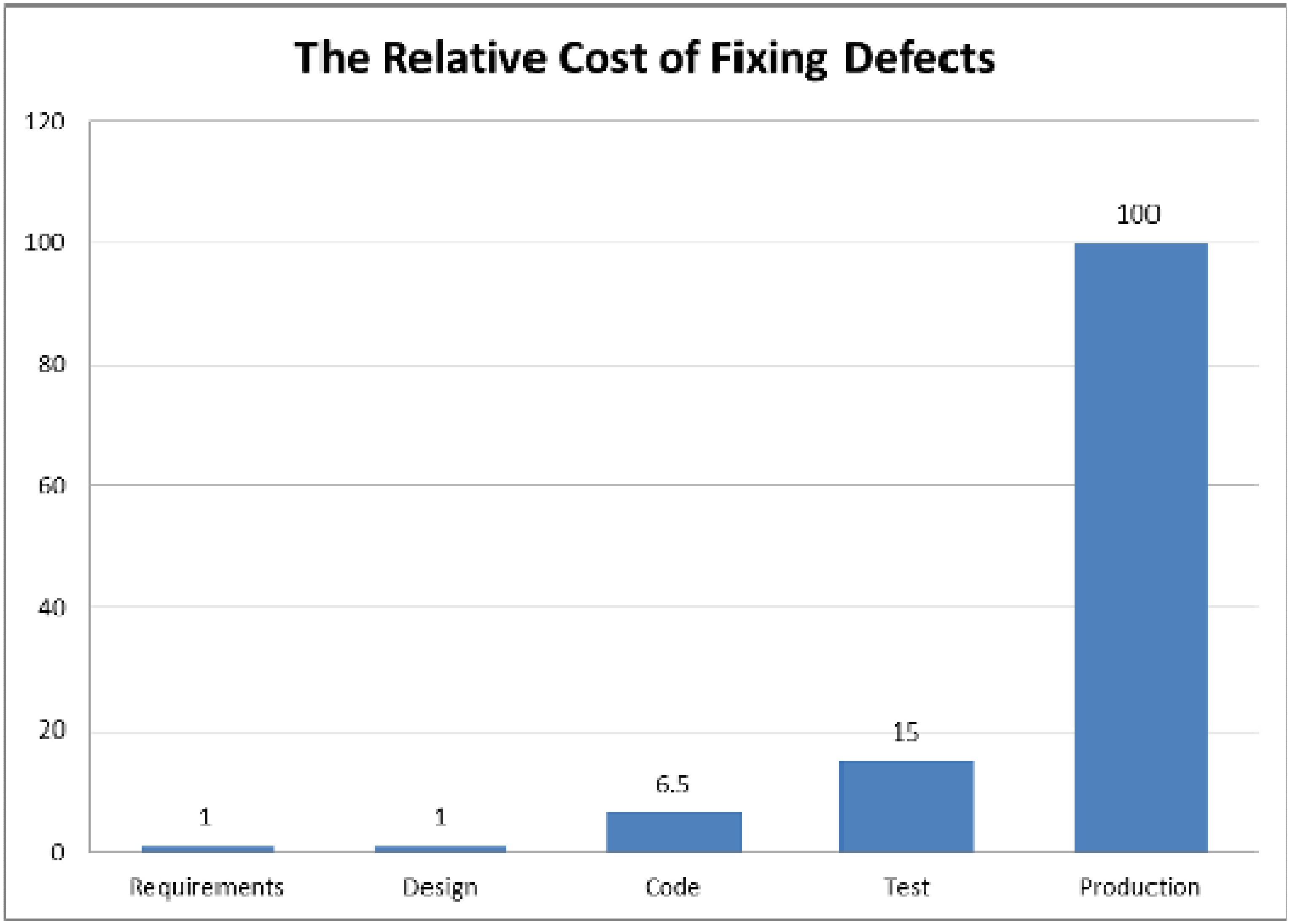
Beneath layer 7

Use the src

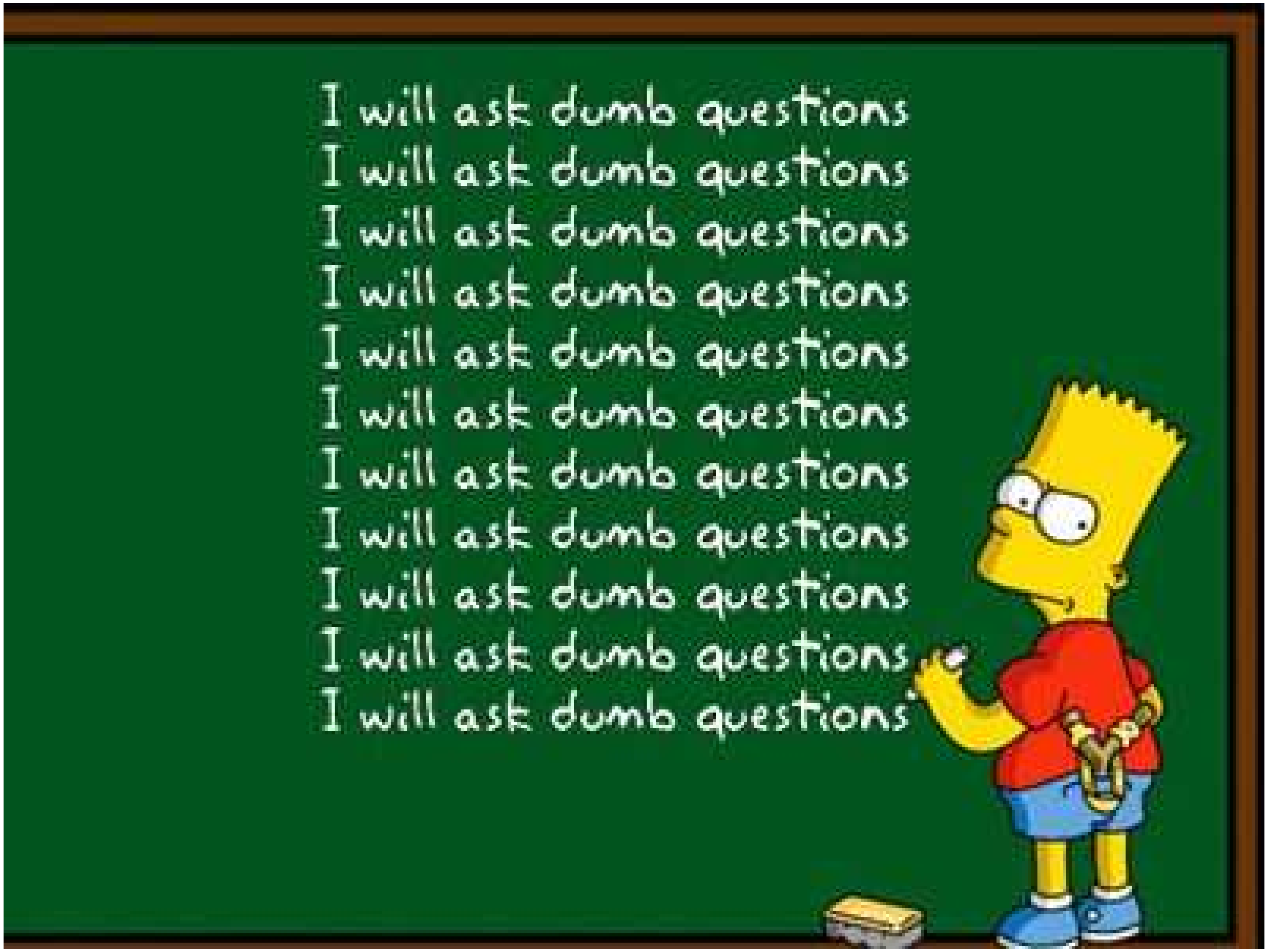
Tools

Reporting

Fix early


The Relative Cost of Fixing Defects
120
100
80
60
40
20
0
1
1
6.5
15
100
Requirements
Design
Code
Test
Production

Questions ?


I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions
I will ask dumb questions