

Builder **VS.** *Breaker*

AppSec 2012 Edition



**Brett
Hardin**
MODERATOR

@miscsecurity



**Brett
Hardin**
MODERATOR

@miscsecurity

I REPRESENT you

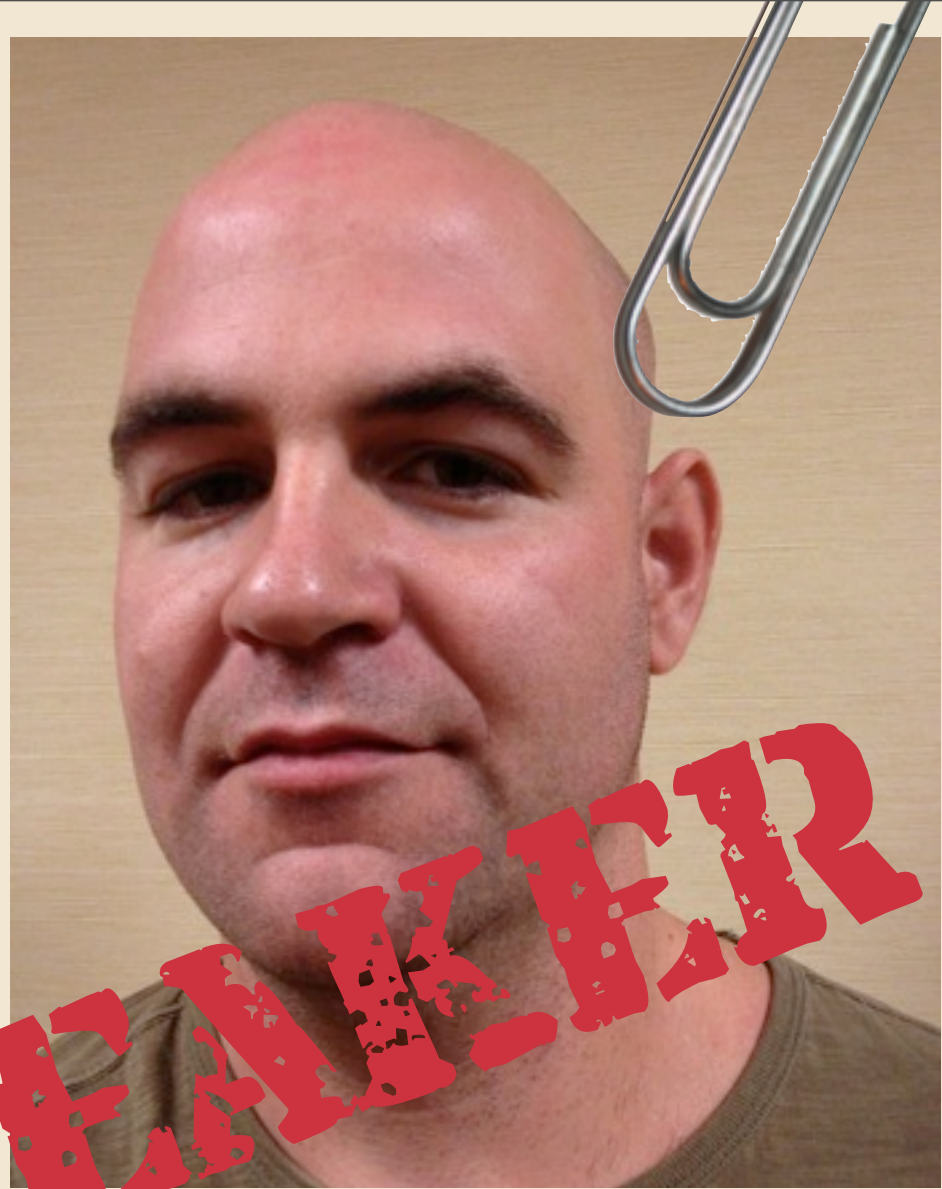


JON

Rose

Builder

Matt Konda



PREFAB

QUICK POLL

Builder

~ OR ~

Breaker

1 Question & Debate
Audience Member

Vote & Drink!

BUILDER'S CONCERNS



Features



**Functional
Quality**



Dates

BREAKER'S CONCERNS



VULNS!



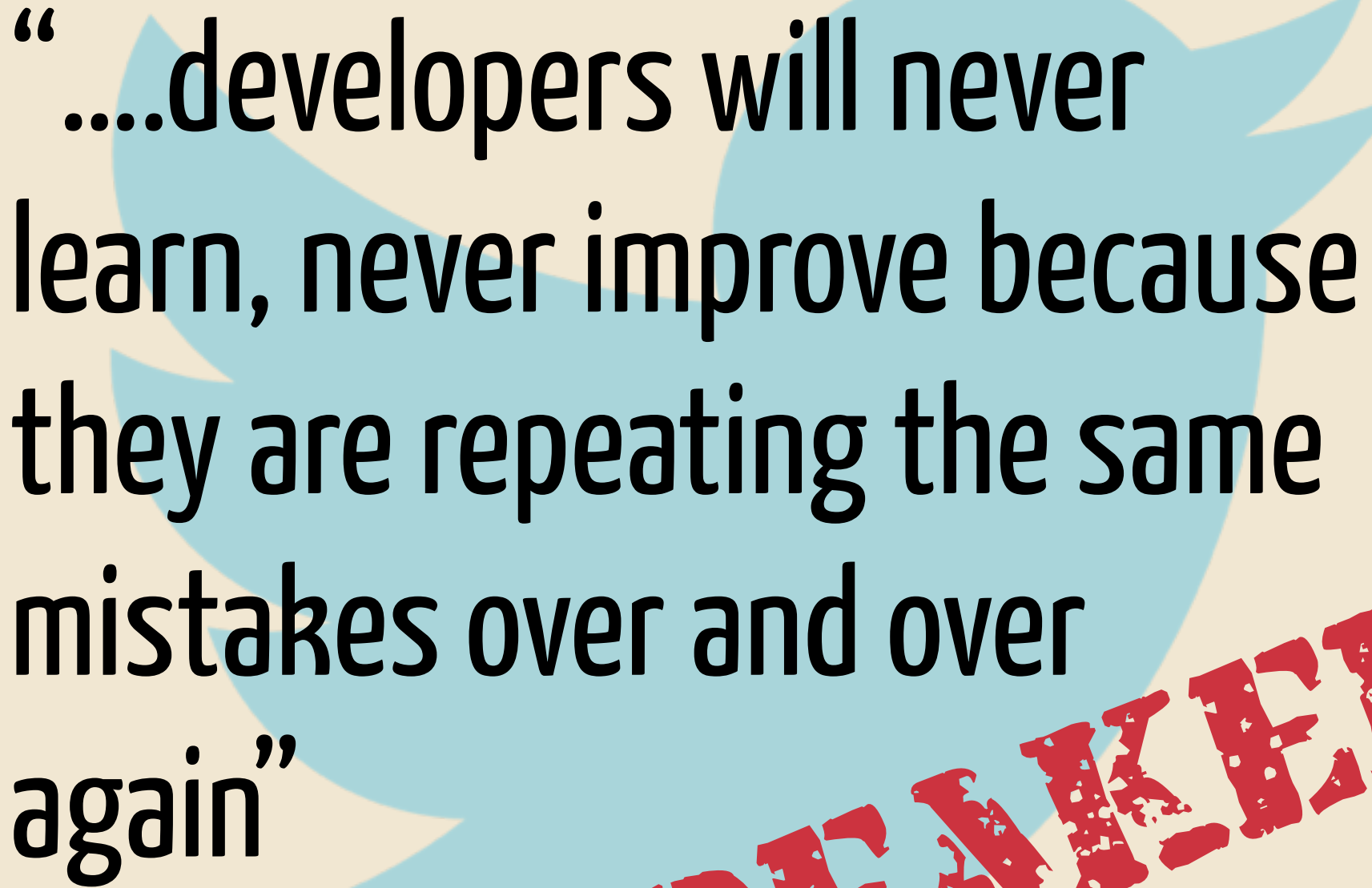
Compromise!



LOL's!

*Let's
get
in
the
mood*





“....developers will never learn, never improve because they are repeating the same mistakes over and over again”

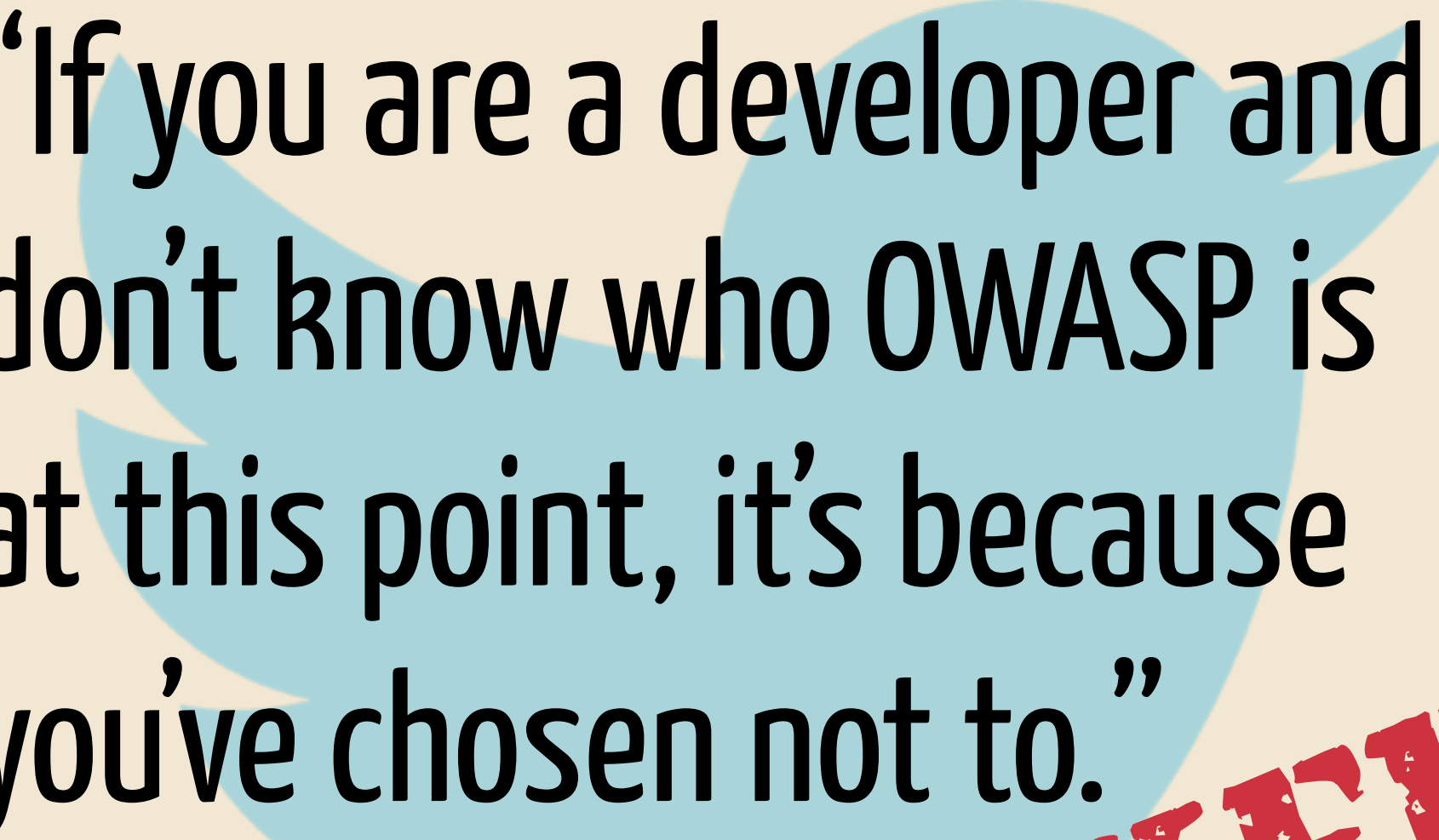
PREFAKER



“...only good at ranting. Zero
contriBs, and almost zero
constructive feedbacks but
bashing”

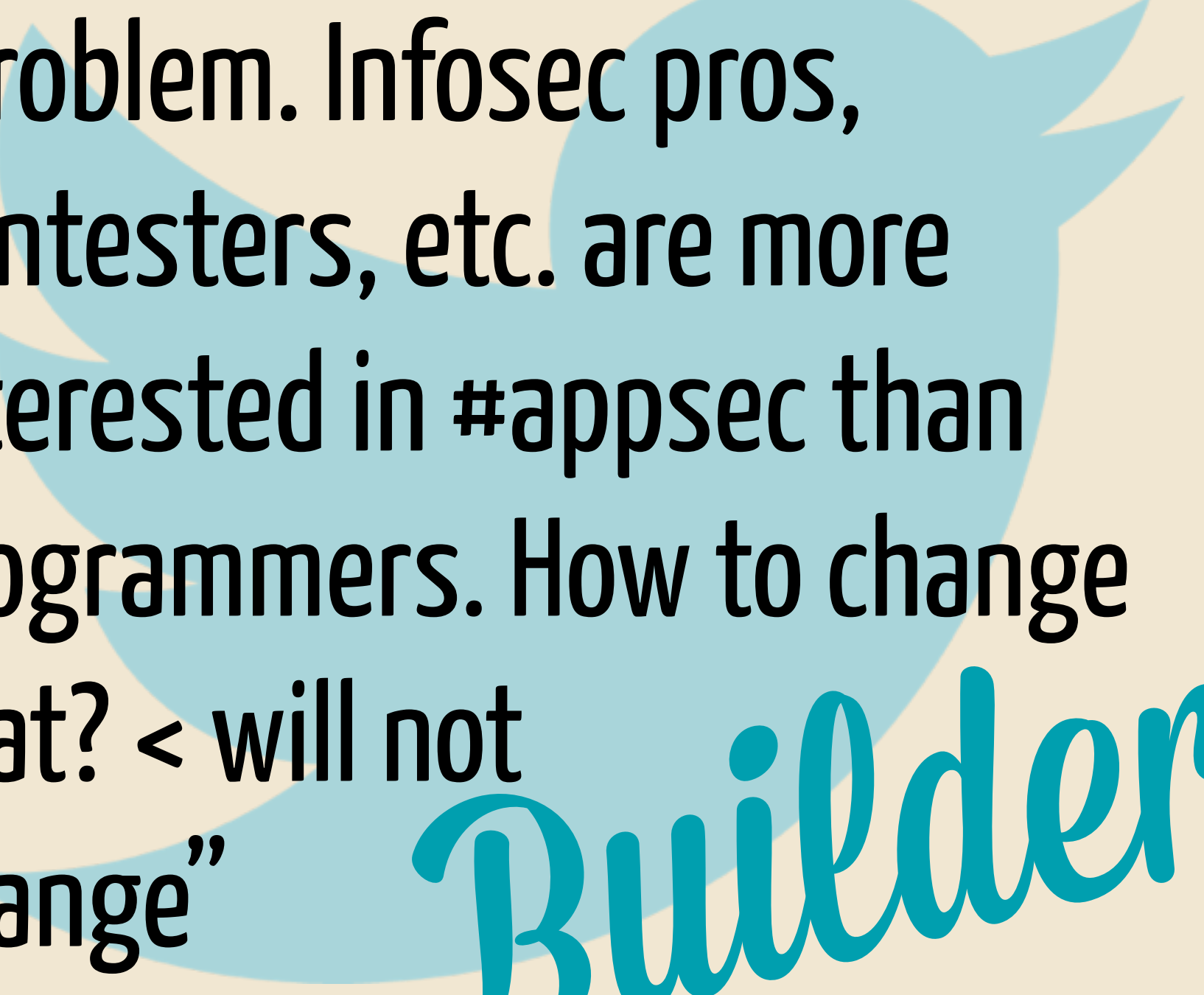
Builder

Response




“If you are a developer and don’t know who OWASP is at this point, it’s because you’ve chosen not to.”

REFALKER



“Problem. Infosec pros,
pentesters, etc. are more
interested in #appsec than
programmers. How to change
that? < will not
change”

Builder



“... the developer
who did this
should be taken
out into the street
and beaten ...”

BREAKER



“Agile: Most
security guys are
useless”
Builder



BUILDER



BREAKER

A large, billowing mushroom cloud from a nuclear explosion, with a thick column of smoke and debris rising from the ground and spreading out at high altitude. The cloud is composed of various shades of grey and white, with some darker, more turbulent sections near the base.

THE

CLOUD


**MAKES
ME**

SECURE


Customers Don't Ask For Security



Friday, October 26, 2012



BREACHES
are
CHEAPER
than
SECURE
CODING



Agile



Hurts

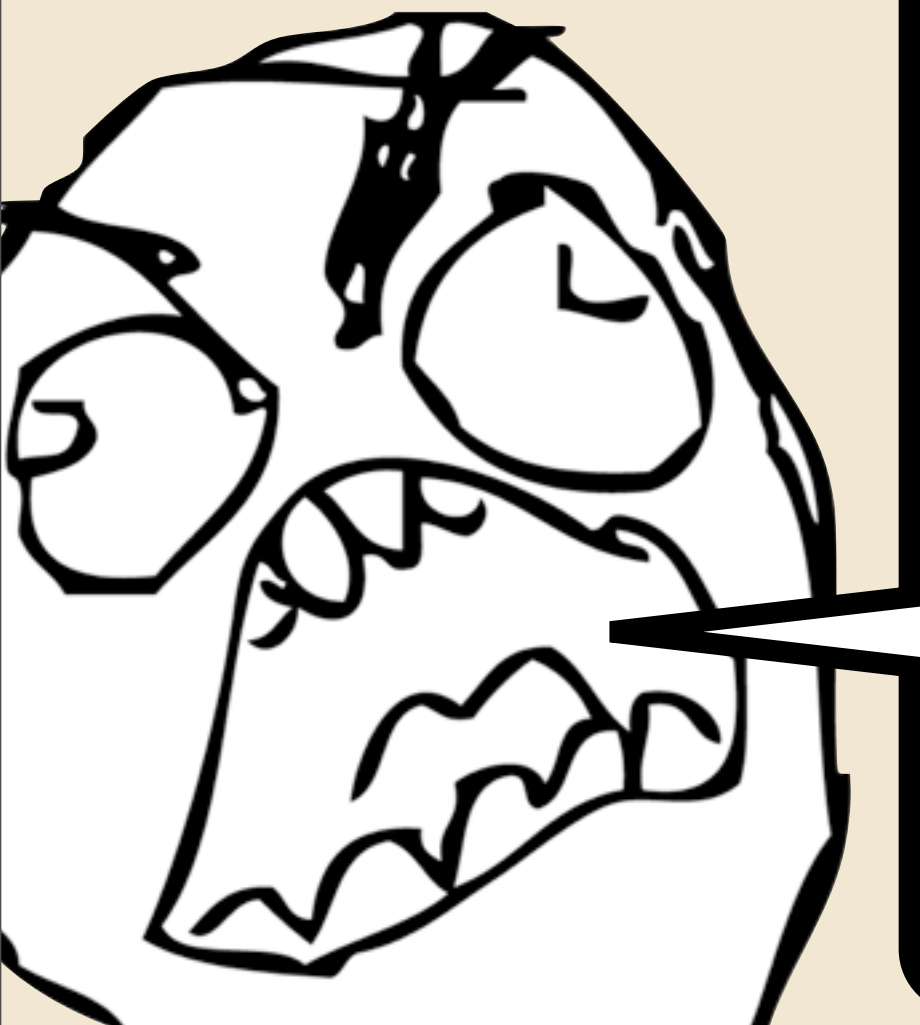
Security

Breakers

DON'T

understand
DEVELOPMENT

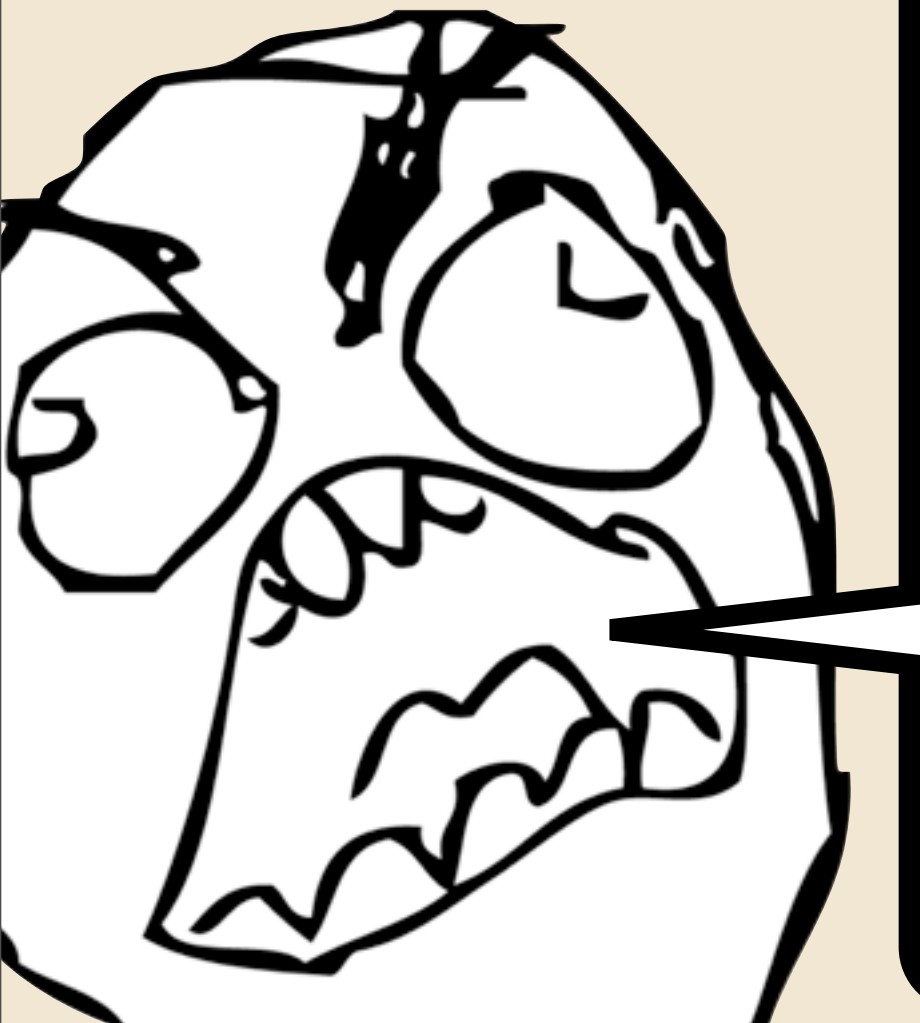




FFFFFFF

UUUUUUU

UUUUUUU



Builders

NEED TO

understand

VULNERABILITIES

WAF!

WAF!

WAF!

WAF!

WAF!

WAF!

WAF!

WAF!

WAF!


WAF!

WAF!

WAF + Rails
SOLVES

THE

PROBLEM



**FALSE
POSITIVES
ARE A
NECESSARY
EVIL**

We don't really feel this way...

HARD STANCE

OPPOSITE THINKING

SAME CONCLUSION?

TAKE AWAYS



TAKE AWAYS

ENGAGE DEVS!



TAKE AWAYS



ENGAGE DEVS!
BE RESPECTFUL

TAKE AWAYS



ENGAGE DEVS!

BE RESPECTFUL

GET DIRTY

Thanks



The background is a solid light beige color. It is decorated with numerous question marks of varying sizes and shades of orange and red. Some question marks are large and prominent, while others are smaller and more subtle. They are scattered across the entire frame, creating a sense of mystery or inquiry.

The Fixer

Friday, October 26, 2012

DISCUSSION

IS

OWASP

WORKING?