Builder vs. Breaker

AppSec 2012 Edition

Brett

Hardin

MODERATOR

@miscsecurity

Brett Hardin

MODERATOR

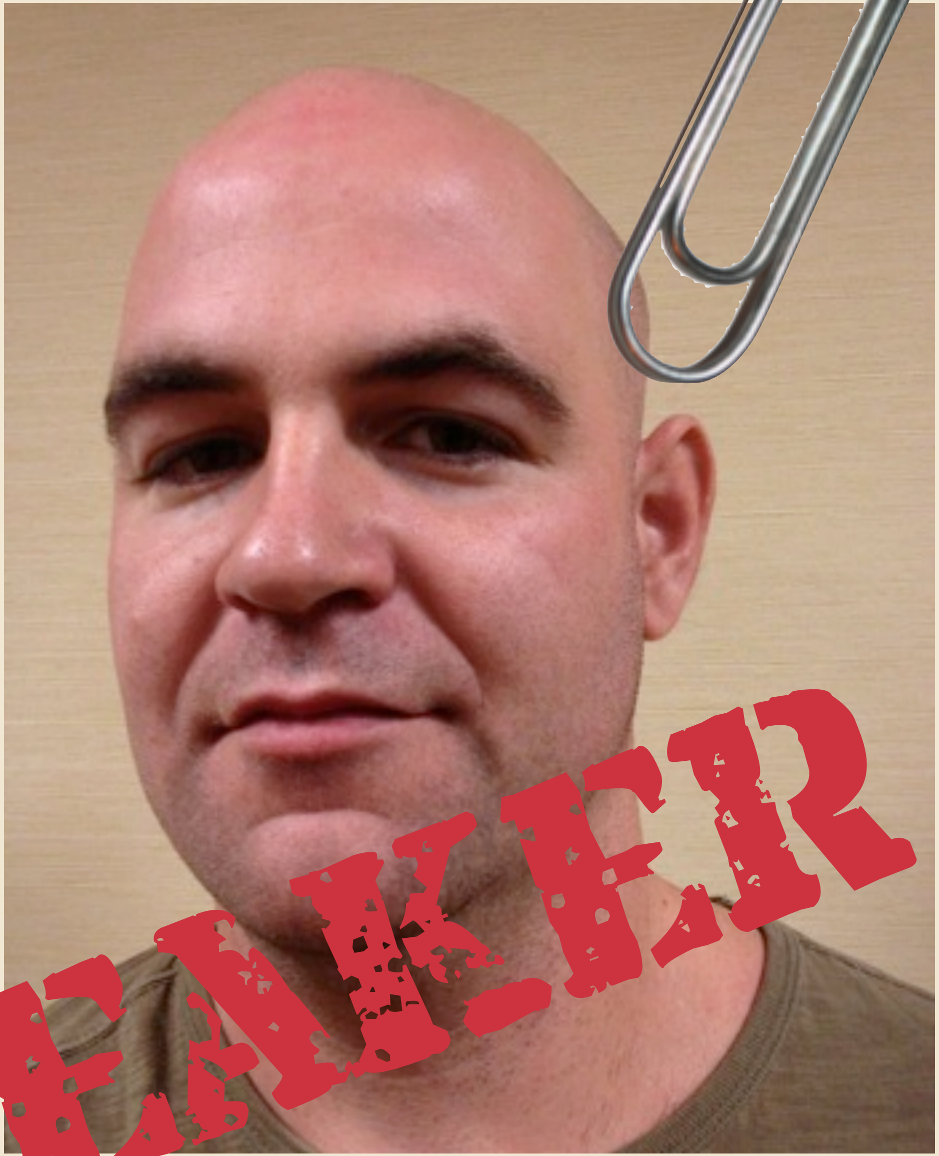
@miscsecurity

I REPRESENT YOU

JON Rose

Builder

Matt Konda



BREAKER

QUICK POLL

Builder

~ OR ~

Breaker

1 Question & Debate

1 Audience Member

Vote & Drink!

BUILDER'S CONCERNS

- NEW 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”

BREAKER

"...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.”

BREAKER

"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
VS
BREAKER

THE CLOUD MAKES ME SECURE

Customers Don't Ask For Security

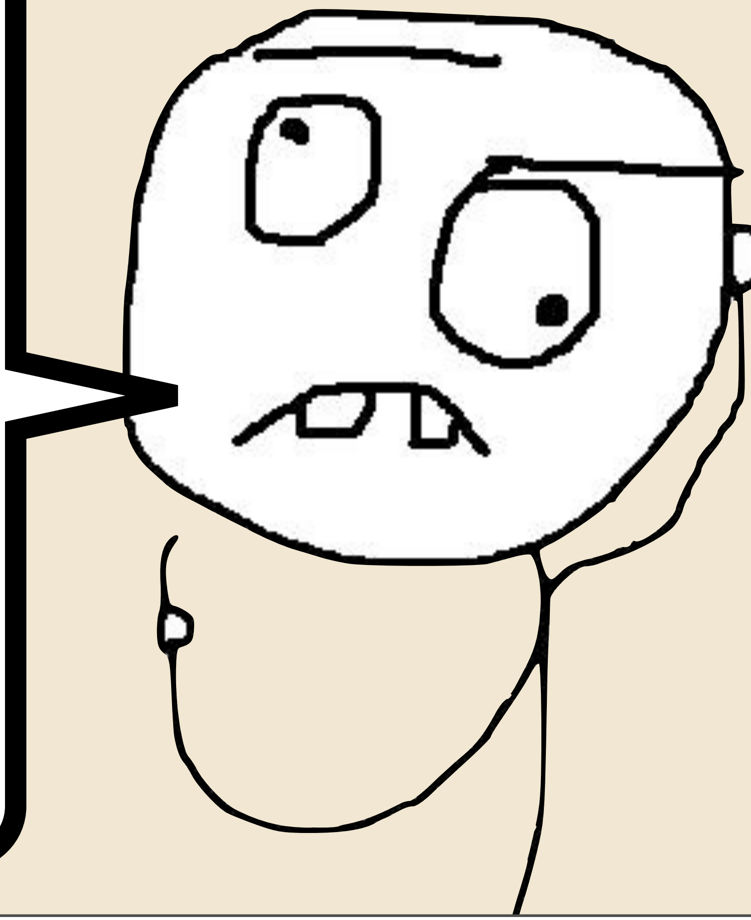
BREACHES are CHEAPER than SECURE CODING

Agile

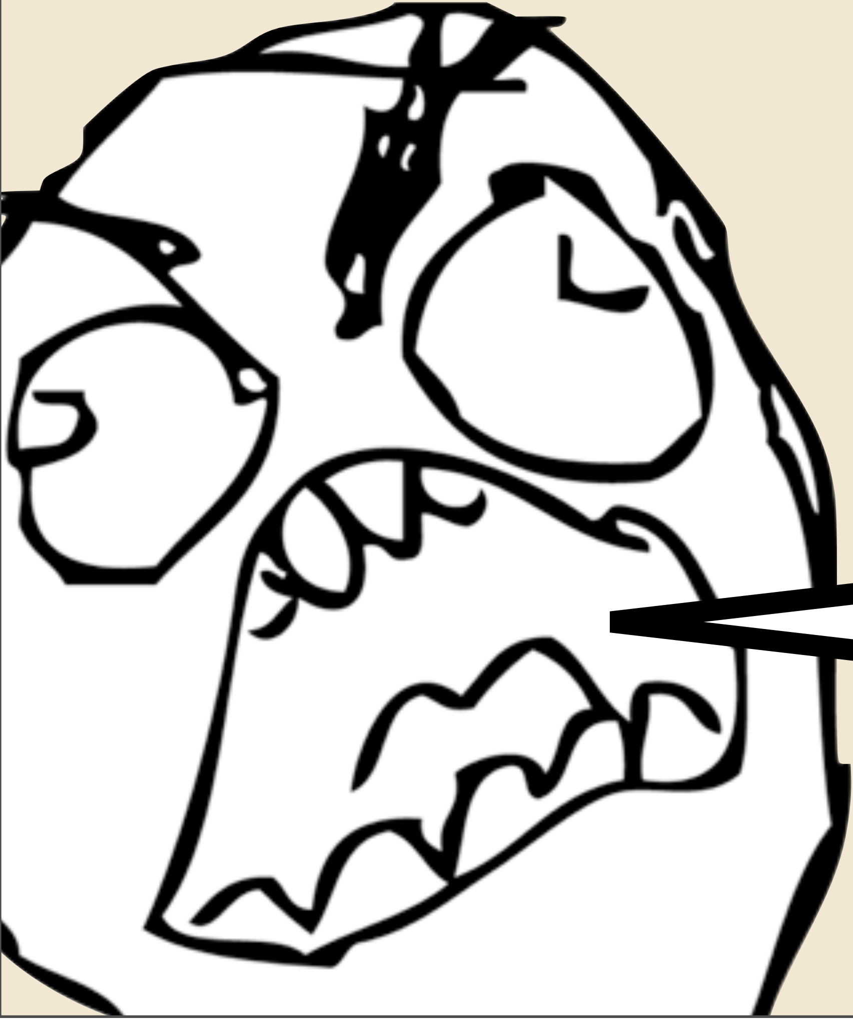
Hurts

Security

Breakers DON’T understand DEVELOPMENT



FFFFFFF
UUUUUU
UUUUUU



Builders NEED TO understand VULNERABILITIES

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 Fixer

DISCUSSION

IS OWASP WORKING?