Building a shield of security - Vulnerability Management by the numbers and dumb robots!
Rahim Jina

- Director BCC Risk Advisory
- OWASP Contributor & OWASP Ireland ex-board member
- Co-Architect of edgescan.com
- Ex-Head of Security of Fonality (US VOIP Provider)
- Ex-Big 4 Consultant
RISK
Context
Context
Automation
Fraud - Technical Vulns
“40% of applications tested by BCC Risk Advisory in the last 12 months had a critical business logic vulnerability”
“(Cyber crime is the) second cause of economic crime experienced by the financial services sector” – PwC

Globally, every second, 18 adults become victims of cybercrime – Symantec

2012 Cyber Crime
• US $20.7 billion in direct losses
• Global $110 billion in direct losses
• Global $338 billion + downtime

“The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history” – Keith Alexander

Almost 1 trillion USD was spent in 2012 protecting against cybercrime

“One hundred BILLION dollars” – Dr Evil

“Jimmy, I didn’t click it” – My Grandma

“556 million adults across the world have first-hand experience of cybercrime -- more than the entire population of the European Union.”
Example 1 - Loan Calculator & Approval
Example 1 - Loan Calculator & Approval
Example 2 - Coupon Abuse

Stacking

Trust the Machine

DISC10
Example 2 - Coupon Abuse
Example 3 - Flight Booking
Example 3 - Flight Booking
Example 4 - ‘Smart’ Bank

1. Application Form
2. Document Photos
3. Bank Teller Verify
4. Bank Teller Authenticate

Submit

Final Submission

New Account!
Example 4 - ‘Smart’ Bank

1. Application Form
2. Document Photos
3. Bank Teller Verify
4. Bank Teller Authenticate

Submit

New Account!

Final Submission

YOU DON'T NEED TO SEE OUR CREDENTIALS

RISK ADVISORY
Example 4 - ‘Smart’ Bank

My Money went to NIGERIA and all I got was this lousy T-Shirt
Example 5 – e-Dating
Example 5 - e-Dating

```cpp
("d":null,"_metadata":null,"uri":"/Data/ODATA/1.0","type":"DataServiceProvider.User","ID":null,"amtbIvewcncjpc
9uIHEvfy2t2","U1RLBVEVMSwgUXEVTAQgVlDSyBNUVxMSU6BT1BDQF1E2STQgoVHEFIPNQFUQcSEVEBCwgyMvVcnlu2y3hIgJvd2wgb2ygb2FOeGvY1g9u1HdoaWNo2IGdCWH1/HehS9y1GHexeS
Bjcm9zc2VkJBoIBHIcL/BvulvldxyBcmvC31/2yuBnm3duCBjBpmcmrPS2/ZQcIHdchcy8zDvXWY1vZQg2VucGxL1/6eGlu2CBeaWQyTk/jdgHl1IGp6gQgbwW9
yblmu2YBhaXiUeI/HgIHgIHgQgdHg1GJvd2jwYxvZnQgW5K1j/6udG6u2ZQ6CN/0IeIEhHOvaWvFGk1GFOsdGFyZEBKuCoGKGsFsdGVKLcS3wZBwZV
YgQgS39G/bI0AUG2GQYayB3aV5aW5aJ/0Wlycy8hbmGQyT2SbGkYHVwVNYx2z5GcGoE6SgQ0C9t2ZSE1cSVgS21uY2qIENvbWY6XMs","ids":null,"axa attackers
code: true}
```
Example 5 - e-Dating
What's your point?

- Robots don’t have curiosity
- SIMPLE
- COMMON
- LEGALITIES
“We need an Onion”

SDL
- Design review
- Threat Modeling
- Code review/SAST/Continuous Integration/IAST
- Negative use/abuse cases/Fuzzing/DAST

Live/
- Continuous/Frequent monitoring/Testing

Ongoing
- Manual Validation
- Vulnerability management & Priority
- Dependency Management ....

“Robots are good at detecting known unknowns”
“Humans are good at detecting unknown unknowns”
Continuous Security

Traditional Security Assessment Approach:

Attacker Schedule

 Defender Schedule

Continuous Security Assessment Approach:

Attacker Schedule

 Defender Schedule
Continuous Integration with SAST

Code changes invoke SAST
Build Pass/Fails
SAST Rules control
Rule Tuning
False Positive Tuning
Framework awareness
Really, what’s your point?

- There is no big button
- Automation helps but is only part of the solution
- Pure blackbox tests are dumb
- Manual effort
- Onion Approach 🌳
- Think C-O-N-T-I-N-U-O-U-S
Thanks for Listening

Some websites were harmed during the making of this presentation

rahim@bccriskadvisory.com
rahim.jina@owasp.org

www.bccriskadvisory.com

© BCC Risk Advisory Ltd 2014.
All rights reserved.