David Rook
Agnitio
Security code review swiss army knife
OWASP, Holland
if (slide == introduction)
System.out.println("I’m David Rook");

SECURITY

• Application Security Lead, Realex Payments, Ireland
  CISSP, CISA, GCIH and many other acronyms

• Security Ninja (@securityninja)

• Speaker at developer and security conferences

• Microsoft Developer Security MVP

• Developed and released Agnitio
if (slide == introduction && replacement)
System.out.println("I’m Steven van der Baan");

• Senior Security consultant, Sogeti Nederland BV, Nederland
CISSP, OSCP, ASS and some other acronyms

• Not a blogger(@vdbaan)

• Project Leader OWASP CTF

• Dedicated dad

• Commented and contributed on Agnitio
• What is static analysis?

• Security code reviews: the good, the bad and the ugly

• Agnitio: security code review Swiss army knife
Static analysis

• What do I mean by static analysis?
  • A review of source code without executing the application
  • Can be either manual or automated through one or more tools
  • Human and/or tools analysing application source code
Static analysis

• Wetware or software?

  • Humans are needed with or without static analysis tools
  • The best thing about humans is that they aren’t software
  • The worst thing about humans is that they are humans
Static analysis

SECURITY

• Wetware or software?

Static analysis

• Wetware or software?

Static analysis

SECURITY

- Wetware or software?
  - Tools can cover more code in less time than a human
  - The best thing about software is that it isn’t human
  - The worst thing about software is that it’s software
The ugly security code reviews

“Ugly reviews” implies you do actually review code

- An unplanned magical mystery tour at the end of the SDLC
- Unstructured, not repeatable and heavily reliant on $\text{C}_{\text{s}}\text{H}_{\text{10}}\text{N}_{\text{4}}\text{O}_{\text{2}}$
- Too late in the SDLC making findings very expensive to fix
- Completely manual process, no tools used during reviews
- No audit trails, no metrics........no security?
- Better than nothing?
The bad security code reviews

• “Bad reviews” might be fine for some companies

  • A single planned code review in your SDLC
  • Some structure, normally based on finding the OWASP top 10
  • Still too late in the SDLC making findings very expensive to fix
  • Some automation, usually basic code analysis tools
  • Basic audit trails still no metrics so hard to measure “anything”
  • Better than ugly reviews, might be fine for some companies
The good security code reviews

• “Good reviews” don’t happen by accident

  • Multiple reviews defined as deliverables in your SDLC
  • Structured, repeatable process with management support
  • Reviews are exit criteria for the development and test phases
  • Automation used where useful freeing up the reviewer
  • Ability to produce reports, metrics and measure improvements
  • External validation of the review process and SDLC
Agnitio

• What is Agnitio?

  • Tool to help with manual static analysis
  • Checklist based with reviewer & developer guidance
  • Produces audit trails & enforces integrity checks
  • Single tool for security code review reports & metrics
Agnitio

SECURITY

What is Agnitio?

- C# open source application, GPLv3 license
- Five different versions in 12 months
- 10,000+ downloads from users in over 100 countries
- Used by SMEs, consulting firms and companies of the NYSE
Checklists?

- An application for doing checklist reviews? *yawn* how boring!
- Checklists are for n00bs! I don't need a checklist to review code!
- I beg to differ, would you say Doctors and Pilots are n00bs?
# A Checklist for Checklists

<table>
<thead>
<tr>
<th>Development</th>
<th>Drafting</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Do you have clear, concise objectives for your checklist?</td>
<td>✓ Does the Checklist:</td>
<td>✓ Have you:</td>
</tr>
<tr>
<td>Is each item:</td>
<td>✓ Utilize natural breaks in workflow (pause points)?</td>
<td>✓ Trialed the checklist with front line users (either in a real or simulated situation)?</td>
</tr>
<tr>
<td>- A critical safety step and in great danger of being missed?</td>
<td>✓ Use simple sentence structure and basic language?</td>
<td>✓ Modified the checklist in response to repeated trials?</td>
</tr>
<tr>
<td>- Not adequately checked by other mechanisms?</td>
<td>✓ Have a title that reflects its objectives?</td>
<td></td>
</tr>
<tr>
<td>- Actionable, with a specific response required for each item?</td>
<td>✓ Have a simple, uncluttered, and logical format?</td>
<td>Does the checklist:</td>
</tr>
<tr>
<td>- Designed to be read aloud as a verbal check?</td>
<td>✓ Fit on one page?</td>
<td>✓ Fit the flow of work?</td>
</tr>
<tr>
<td>- One that can be affected by the use of a checklist?</td>
<td>✓ Minimize the use of color?</td>
<td>✓ Detect errors at a time when they can still be corrected?</td>
</tr>
<tr>
<td>Have you considered:</td>
<td>Is the font:</td>
<td>✓ Can the checklist be completed in a reasonably brief period of time?</td>
</tr>
<tr>
<td>- Adding items that will improve communication among team members?</td>
<td>- Sans serif?</td>
<td>✓ Have you made plans for future review and revision of the checklist?</td>
</tr>
<tr>
<td>- Involving all members of the team in the checklist creation process?</td>
<td>- Upper and lower case text?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Large enough to be read easily?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Dark on a light background?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Are there fewer than 10 items per pause point?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Is the date of creation (or revision) clearly marked?</td>
<td></td>
</tr>
</tbody>
</table>

Please note: A checklist is NOT a teaching tool or an algorithm

Last updated 1/14/10
<table>
<thead>
<tr>
<th>Before Induction</th>
<th>Before Skin Incision</th>
<th>Before Patient Leaves Room</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIGN IN</strong></td>
<td><strong>TIME OUT</strong></td>
<td><strong>SIGN OUT</strong></td>
</tr>
<tr>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SURGEON, ANESTHESIA, PERFUSIONIST AND NURSE VERBALLY CONFIRM</strong></td>
<td><strong>NURSE VERBALLY CONFIRMS WITH THE TEAM:</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>PATIENT</strong></td>
<td><strong>NAME OF THE PROCEDURE</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SITE</strong></td>
<td><strong>THAT INSTRUMENT, SPONGE AND NEEDLE COUNTS ARE CORRECT</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>PROCEDURE</strong></td>
<td><strong>HOW THE SPECIMEN IS LABELLED</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>CONSENT</strong></td>
<td><strong>INCLUDING PATIENT NAME</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>DOES PATIENT HAVE A KNOWN ALLERGY?</strong></td>
<td><strong>SENT FOR APPROPRIATE TESTS</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>NO</strong></td>
<td><strong>WHETHER THERE ARE ANY EQUIPMENT PROBLEMS TO BE ADDRESSED</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>YES</strong></td>
<td><strong>SURGEON, ANESTHESIA PROFESSIONAL AND NURSE</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>DRUGS</strong></td>
<td><strong>REVIEW THE KEY CONCERNS FOR POST-OP RECOVERY AND MANAGEMENT OF THIS PATIENT</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>LATEX</strong></td>
<td><strong>BLOOD PRODUCTS USED</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td><strong>BLOOD PRODUCTS STILL AVAILABLE</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>H&amp;P CURRENT (&lt; 30d)</strong></td>
<td><strong>BREAKS IN TECHNIQUE</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>WEIGHT RE-CHECKED</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>ANESTHESIA SAFETY CHECK COMPLETED (Machine and Meds)</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>PULSE OXIMETER ON PATIENT AND FUNCTIONING</strong></td>
<td><strong>PERFUSION STRATEGY:</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>DIFFICULT AIRWAY/ASPIRATION RISK?</strong></td>
<td><strong>CANNULATION SITES</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>NO</strong></td>
<td><strong>CANNULAE SIZES</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>YES</strong></td>
<td><strong>BYPASS PRIME (blood vs prime)</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>H &amp; E, EQUIPMENT/ASSISTANCE AVAILABLE</strong></td>
<td><strong>TARGETED CORE TEMP</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>INTRAVENOUS ACCESS AND FLUIDS PLANNED</strong></td>
<td><strong>USE OR NON-USE OF DHCA, SELECTIVE CEREBRAL PERFUSION</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>WARMER (blankets and fluids) IN PLACE</strong></td>
<td><strong>ICE ON THE HEAD</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>BLOOD BANK NOTIFIED AND BLOOD PRODUCTS AVAILABLE WHEN NEEDED</strong></td>
<td><strong>OTHER BYPASS CONSIDERATIONS (shunts, collaterals, AR, LV venting, CARDIOPLEGIA, etc)</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SIGN (NURSING):</strong></td>
<td><strong>ANESTHESIA TEAM REVIEWS:</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SIGN (ANESTH):</strong></td>
<td><strong>ANY FURTHER PATIENT-SPECIFIC CONCERNS?</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SIGN (SURG):</strong></td>
<td><strong>NURSING TEAM REVIEWS:</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SIGN (SURG):</strong></td>
<td><strong>EQUIPMENT STERILITY CONFIRMED?</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
<tr>
<td><strong>SIGN (SURG):</strong></td>
<td><strong>ARE THERE EQUIPMENT/PROSTHESES ISSUES OR ANY CONCERNS?</strong></td>
<td><strong>CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME</strong></td>
</tr>
</tbody>
</table>
**FUEL INJECTED CESSNA 172 CHECKLIST**

### CABIN CHECK
- **Fuel**
  - CHECK (122.85)

### EXTERIOR INSPECTION
- **Fuel Sumps**
  - CHECK
- **Fuselage Left Side**
  - CHECK
- **Elevator/Rudder**
  - REMOVE
- **Tail Tie-down**
  - CHECK
- **Fuselage Right Side**
  - CHECK
- **Right Flap & Aileron**
  - CHECK
- **Wing Tie-down**
  - CHECK
- **Fuel Sumps**
  - SAMPLE (5)
- **Main Wheel Tire/Brakes**
  - CHECK
- **Chocks**
  - REMOVE
- **Static Source**
  - CHECK
- **Fuel Quantity (Right Tank)**
  - CHECK VISUALLY
- **Engine Oil Level**
  - CHECK MIN, 5 QTS
- **Fuel Strainer/Selector Drains**
  - CHECK
- **Propeller & Spinner**
  - CHECK
- **Alternator Belt**
  - CHECK
- **Landing Light**
  - CHECK
- **Engine Air-intake Filter**
  - CHECK
- **Nose Wheel Strut & Tire**
  - CHECK
- **Nose Chocks**
  - REMOVE
- **Static Source**
  - CHECK
- **Fuel Quantity (Left Tank)**
  - CHECK VISUALLY
- **Wing Tie-down**
  - CHECK
- **Pilot Tube Cover**
  - REMOVE
- **Fuel Tank Vent**
  - CLEAR
- **Stall Warning Horn Opening**
  - CHECK
- **Left Flap & Aileron**
  - CHECK
- **Main Wheel Tire/Brakes**
  - CHECK
- **Chocks**
  - REMOVE
- **Move Airplane**
  - CHECK TIRES
- **Overall Condition**
  - REVIEW

**BEFORE ENGINE START**
- **Seatbelts/Shoulder Harness**
  - FASTENED
- **Fuel Selector**
  - BOTH
- **Fuel Shutoff Valve**
  - ON IN
- **Circuit Breakers**
  - CHECK
- **Beacon**
  - OFF
- **Avionics Switch**
  - ON
- **Master Switch**
  - ON
- **Throttle**
  - OPEN 1/4 INCH
- **Mixture**
  - IDLE CUTOFF
- **Aux. Pump**
  - ON
- **Mixture Rich 3-5 GPH**
  - ON
- **Aux. Pump**
  - OFF
- **Propeller Area**
  - CLEAR

**AFTER ENGINE START**
- **Ignition Switch**
  - START RICH
- **Mixture At Engine Start**
  - CHECK
- **Engine RPM**
  - 1000 RPM CHECK LEANED MAX
- **Oil Pressure**
  - CHECK
- **Flaps**
  - RETRACT

**BEFORE TAKEOFF**
- **Parking Brakes**
  - SET FREE & CORRECT
- **Flight Controls**
  - SET BOTH
- **Fuel Selector**
  - SET RICH FOR RUNUP
- **Elevator & Rudder Trim**
  - CHECK DISCONNECT 1800 RPM
- **Autopilot**
  - CHECK
- **Ammeter**
  - CHECK
- **Engine Instrumentation**
  - CHECK
- **Suction**
  - CHECK 125/50
- **Magnetos**
  - IDLE CHECK THROTTLE BYPASS & 600 RPM ± 25 THEN 1000 RPM
- **Radios**
  - SET BRAKES
- **Brakes**
  - RELEASE

**FINAL ITEMS**
- **Door/Windows**
  - CLOSED
- **Flaps**
  - AS REQUIRED
- **Mixture**
  - RICH (BELOW/3000 FT)

**ENGINE SHUTDOWN**
- **Throttle**
  - IDLE CHECK DISCONNECT
- **Mags**
  - 1000 RPM
- **Throttle**
  - CUTOFF
- **Avionics/Electrical Equip.**
  - CUTOFF
- **Mixture**
  - OFF
- **Master/Alternator Switch**
  - OFF
- **Ignition Switch**
  - OFF
- **Ignition Key**
  - GLARESHIELD

**SECURING AIRCRAFT**
- **Hobbs & Tach**
  - RECORD
- **Control Lock**
  - INSTALL
- **Tie downs/Chocks**
  - INSTALL
- **Propeller (For Fuel)**
  - VERTICAL
- **Fuel**
  - LEFT TANK

**BEFORE LANDING**
- **Seatbelts**
  - ADJUST
- **Fuel Selector**
  - BOTH
- **Engine Gauges**
  - CHECK
- **Heading Indicator**
  - ALIGNED
- **Attitude Setting**
  - SET
- **Radios**
  - OFF
- **Auto Pilot**
  - ON

**AFTER LANDING**
- **“LIGHTS” (Except Beacon)**
  - OFF
- **“CAMERA” (Transponder)**
  - OFF
- **“ACTION” (Mixture, Flaps)**
  - OFF

**TAKING OFF**
- **“LIGHTS” (ALL)**
  - ON
- **“CAMERA” (Transponder)**
  - ON
- **“ACTION” (RPM, Oil Press, Time)**
  - FULL POWER
- **Climb Speed**
  - 74 KTS (172R)
  - 79 KTS (172S)
• Checklists?
  
  • Do you use checklists for your source code reviews?
  • What's the worst that could happen if you don’t?
Ariane 5 flight 501
L_M_BV_32 := TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) * G_M_INFO_DERIVE(T_ALG.E_BV));

if L_M_BV_32 > 32767 then
  P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
elsif L_M_BV_32 < -32768 then
  P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
else
  P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32));
end if;

P_M_DERIVE(T_ALG.E_BH) := UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) * 
G_M_INFO_DERIVE(T_ALG.E_BH)));
Mars Climate Orbiter

To Earth

To Sun

Planned Trajectory

Actual Trajectory
• Checklists?

• Do you use checklist for your source code reviews?
• What's the worst that could happen if you don’t?
• Four people dead and over €700m of equipment destroyed
• Checklists can be useful to pilots, doctors and code reviewers!
Agnitio

SECURITY

• So, why did I develop Agnitio?

  • I love using checklists for security code reviews!
  • Even if your process is good it might not be smart
  • Is your review process really repeatable and easy to audit?
  • How about producing metrics, useful reports & integrity checks?
  • No? That’s why I developed Agnitio!
Why did I develop Agnitio?

- Demonstration: application profiles
Why did I develop Agnitio?

SECURITY

• Demonstration: security code reviews
Why did I develop Agnitio?

- Demonstration: security code review reports
Why did I develop Agnitio?

- Demonstration: application security metrics
Why did I develop Agnitio?

SECURITY

• Demonstration: customise your Agnitio installation
Agnitio hands on

SECURITY

- Create a PHP rule
Agnitio hands on

SECURITY

• Analyse the PHP application
Agnitio v2.2

**SECURITY**

- Verification records for the code you analyse
- Ability to use open source static analysis tools
- Full screen mode, syntax highlighting etc
- Suggested security test cases for failed items
- Save reviews without completing them
- Plus many more new features!
My “shoot for the moon” vision for Agnitio

SECURITY

“we pretty much need a Burp Pro equivalent for Static Analysis – awesome, powerful in the right hands, and completely affordable!”

http://www.securityninja.co.uk/application-security/can-you-implement-static-analysis-without-breaking-the-bank/comment-page-1
Using Agnitio

• How you can use Agnitio in your reviews
  • Download Agnitio from Source Forge
  • Focus security code reviews on root causes not vulnerabilities
  • Use your language/s in all code examples and checklist items
  • Use Agnitio to conduct principles based security code reviews