



# Testing Application Code

Security Architecture & Tool Sets

# Testing Application Code

1. Scanning using a tool
  2. Automated vulnerability scanning tools
  3. Manual penetration testing
  4. Code review
- OWASP considers code reviews the best and most thorough of these options
  - “360 Reviews” combined code review with penetration testing, then review’s code again



# Code Reviews

- Shares knowledge of the code with others
- More experience is learned across the team
- Detects problems and enforces good coding
- Agile and formal models:
  - Pair Programming
  - Over-the-Shoulder
  - Pass-Around
  - Tool-Assisted
  - Fagan



# Pair Programming

- Agile development technique
- Two developers use one workstation
- Provides real-time code review but is costly



# Over-the-Shoulder

- Agile development technique
- Developer who coded software explains it to another developer
- Lower cost than pair programming since it occurs at intervals instead of having a constant review



# Pass-Around

- Form of review with one or more reviewers
- Code is emailed or shared for review
- Code documentation is much more important

```
43 <body <?php body_class()></div>
44 <div id="fb-root"></div>
45 <script>(function(d,s,id){
46   var js, fjs = d.getElementsByTagName(s)[0];
47   if (d.getElementById(id)) return;
48   js = d.createElement(s); js.id = id;
49   js.src = "//connect.facebook.net/en_US/sdk.js#xfbml=1&version=v2.6&appId=28864863618217";
50   fjs.parentNode.insertBefore(js, fjs);
51 })(document, 'script', 'facebook-jssdk');</script>
52 <div id="page" class="site">
53   <a class="skip-link screen-reader-text" href="#content"><?php esc_html_e( 'Skip to content', 'urduite' ); ?></a>
54   <header id="masthead" class="site-header" role="banner">
55     <div class="site-branding">
56       <div class="navBtn pull-left">
57         <?php if(is_home() && $xpanel['homepage-style'] == 1) { ?>
58           <a href="#" id="openMenu"><i class="fa fa-bars fa-3x"></i></a>
59         <?php } else { ?>
60           <a href="#" id="openMenu2"><i class="fa fa-bars fa-3x"></i></a>
61         <?php } ?>
62       </div>
63       <div class="logo pull-left">
64         <a href="<?php echo esc_url( home_url() ) ?>">
65           
66         </a>
67       </div>
68       <div class="search-box hidden-xs hidden-sm pull-left ml-10">
69         <?php get_search_form(); ?>
70       </div>
71       <div class="submit-btn hidden-xs hidden-sm pull-left ml-10">
72         <a href="<?php echo get_page_link($xpanel['submit-link']) ?>" class="header-submit-btn"><i class="fa fa-search fa-3x"></i></a>
73       </div>
74       <div class="user-info pull-right mr-10">
75         <?php
76         if ( is_user_logged_in() ) {
```

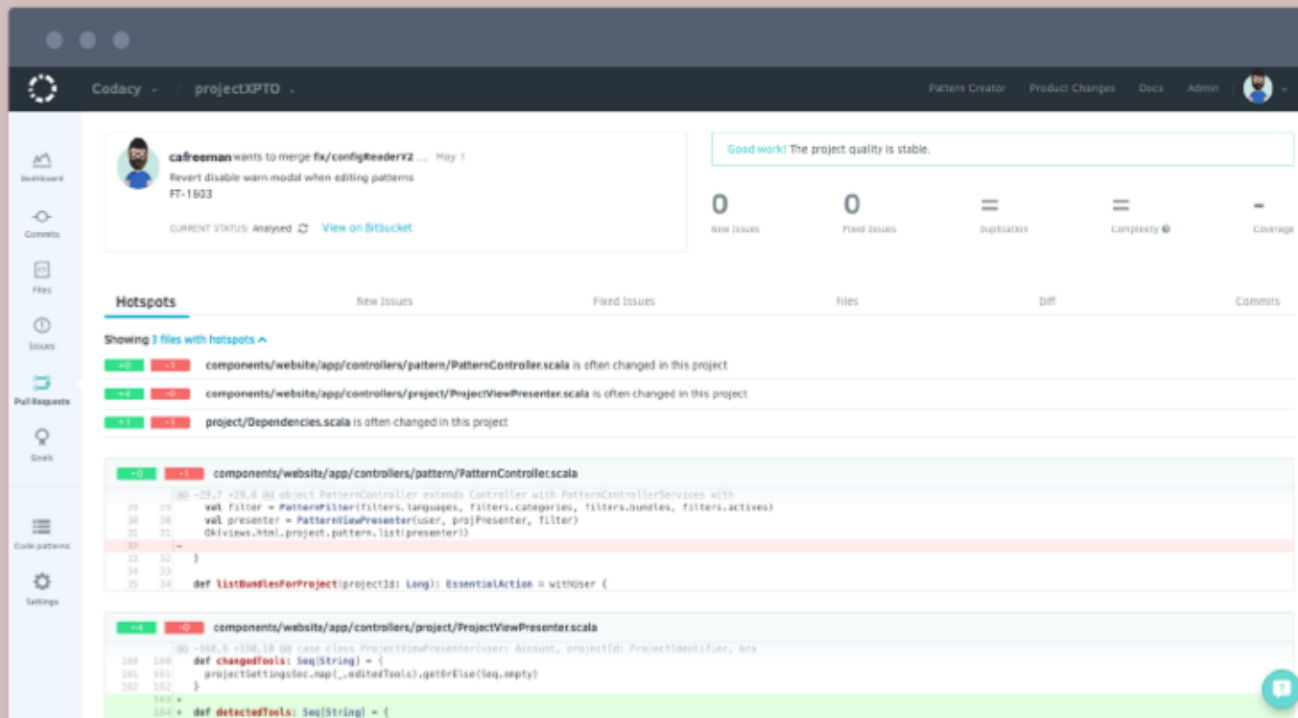


JASON DION  
TRAINING THE CYBER SECURITY WORKFORCE



# Tool-Assisted

- Formal or informal software-based tools conduct code reviews
- Specialized software allows the reviewers to mark up the code, provide feedback, and more



# Fagan

- Structured formal code review by a team of reviewers
- Specifies entry/exit criteria for each process
- More costly and harder to implement than other types of code reviews

