

# Security Innovation's TeamMentor™

Just-in-time Guidance System for Secure  
Software Development

## Reviewers Guide



**SecurityInnovation®**

BOSTON | SEATTLE

[www.securityinnovation.com](http://www.securityinnovation.com)

Security Innovation, Inc. 187 Ballardvale Street Suite A195 Wilmington, MA 01887 • Ph: 1.978.694.1008

## 1.0 TeamMentor Overview

The screenshot displays the TeamMentor Enterprise Edition web application. The browser window shows the URL <http://teammentor.securityinnovation.com/>. The interface includes a search bar, a navigation menu on the left with categories like 'Security Engineering Techniques' and 'Fundamentals of Security', and a main content area with filter tabs for Technology, Phase, Type, and Category. Below the filters is a table of security findings.

Title	Technology	Phase	Type	Category
Parent paths setting is disabled.	Web Application	Deployment	Checklist Item	Server Hardening
authentication element is not completely configured	ASP.NET 1.1	Implementation	Checklist Item	Configuration
customError element is used to configure custom error messages.	ASP.NET 1.1	Implementation	Checklist Item	Configuration
crossScripting element is configured properly	ASP.NET 1.1	Implementation	Checklist Item	Configuration
processModel element attributes are configured for specific purposes.	ASP.NET 1.1	Implementation	Checklist Item	Configuration
sessionState element is configured correctly	ASP.NET 1.1	Implementation	Checklist Item	Configuration
A certificate is installed on the database server to support SSL communication	SQL Server 2000	Deployment	Checklist Item	Deployment Considerations
A custom ASP.NET policy is used to deny non-SQL Server databases from accessing ASP.NET applications.	ADO.NET 2.0	Implementation	Checklist Item	Code Access Security
A system least-privileged anonymous account is created for anonymous access.	Web Application	Deployment	Checklist Item	Server Hardening
A Global Exception Handler is Used for Unhandled Exceptions	Java Web 1.4.2	Implementation	Checklist Item	Error and Exception Management

## GUIDANCE SYSTEMS

Secure software requires secure requirements, design, coding practices and testing. There are myriad “right” ways to do things and a challenge faced by development teams is determining which “right” way to do things. For example, defining robust feature requirements carries with it various security requirements for design, code and test. Different requirements will carry differing security components and/or implementation requirements, each of which may drive another path through the code and may open unexpected vulnerabilities through model conflicts or interactions. Another example is that there are many ways to implement specific secure functionality. The web and various IDE help systems provide help to developers when it comes to figuring out how to implement things, but the time involved can be extreme, which often leads to dropping secure functionality due to time constraints.

The best way to manage the problem is to provide the answers the designers, developers and testers need up front, in a manner they can internalize quickly and apply immediately. For decades, EXPERT SYSTEMS have provided guidance to many industries and streamlined the process of getting the job done by assisting those in need of the appropriate knowledge, be it manufacturing a widget, supporting a

customer or processing a record of some sort. This type of system is what's needed in the secure software application development arena. A good system would provide SECURITY GUIDANCE to every practitioner on the development team—from requirements to development to deployment, and would provide it in a way that each practitioner could leverage immediately. In addition to just providing the information, the mechanism for isolating the needed guidance would need to be simple, fast and provide unambiguous results.

TeamMentor™ by Security Innovation is such a system.

## 2.0 Product Details

---

Application security is an **ABSOLUTE** requirement in modern software—and developing secure application is difficult. The need for security has changed the way that software development teams need to work, the tooling they need to use, and it causes general disruption in the development process. Disruption in any process leads to change and the challenges that come with change. In the secure application development process these challenges are generally:

- Inadequate internal technical and process knowledge
- Difficulty locating and employing appropriate staff
- Understanding and implementing necessary systemic and process change

Security Innovation has guided software development teams through the process of developing secure applications for years—providing analysis, training and mentoring to ensure the construction of the best applications possible. This experience allows our engineers to recognize the problems that software development teams typically encounter and drive the behaviors they need to adopt to succeed. This rich experience has been captured in Security Innovation TeamMentor™.

TeamMentor™ is a sophisticated **APPLICATION SECURITY GUIDANCE SYSTEM** that delivers the collected experience of Security Innovation engineering to development teams of all sizes. It provides on-demand, task based collections of secure development knowledge, guidance and tooling to the specific practitioners at the appropriate lifecycle phase, and helps the entire teams quickly develop the most secure and stable applications they can.

The product supports key development technology silos including C#/ASP.NET, Java/Web and AMP<sup>1</sup>. For each environment, TeamMentor delivers its assets to developers through a rich AJAX based browser interface that guides them through the secure development process including:

---

<sup>1</sup> WAMP (Windows, Apache, MySQL, PHP), LAMP (Linux, Apache, MySQL, PHP), MAMP (Macintosh OS/X, Apache, MySQL, PHP)

- Guidelines, Checklists
- How To Guides
- Requirements
- Techniques
- Design Patterns/Antipatterns
- Principles
- Code Snippets and Examples
- Test Cases
- eLearning modules
- Attack/Vulnerability Descriptions

TeamMentor™ is a “learning” system that is capable of incorporating experience gained by the development team during the development process, and leveraging it in subsequent projects. Web 2.0 components such as collaboration, editorial comment and voting allow team members and larger user groups to discuss how specific guidance applies to their specific applications, how to focus and extend it, and finally how valuable the asset is to their environment. Team managers can use this feedback to grow and adapt TeamMentor to their specific environments, making it the most valuable single asset the team can own for security guidance.

To stay ahead of the curve, Security Innovation constantly updates TeamMentor™ via various subscription mechanisms. Updates include new assets that match new and emerging threats in the global threat landscape, new development and test principals, new tool interfaces and guidance, and anything else that effect the development of secure applications in the TeamMentor™ guided environments.

In summary, Security Innovation TeamMentor™ is a software development team’s in-house security expert. It guides them through all of the steps of defining, designing, coding, testing and deploying secure software applications in a time when the expertise is needed most, and hardest to find.

### 3.0 Guided Tour

TeamMentor™ provides a wealth of security guidance encapsulated in a specific collection of assets, each relating to a specific technology or problem. The size of the problem space is dramatic, but the TeamMentor™ UI metaphor makes it simple to locate and drill into whatever asset is needed.

#### MAIN SCREEN

The **Filter** system allows users to quickly isolate all or selected assets for a specific technology, category or type.

Rich search capabilities for global content or content limited by what's selected in the **filter system**.

**Infoline** provides instant understanding of what the asset applies to

Click the [+ ] to see a text summary that gives the user a hint to what the content is.

Clicking the title opens the full document in a manner similar to popular search engines.

**Guidance Views** allow users to quickly locate and isolate all items of a specific type

Selecting an item from the tree limits the result set to that type of item. Subsequent filtering will further limit the result set to that of the selected filter elements, thereby giving the user specific assets.

Searching allows full boolean searching of the entire knowledge base or the search may be limited to specific collection or item type selected in the tree, for example "SSL" in "Code Examples"

The screenshot shows the TeamMentor main screen. On the left is a 'Guidance Views' tree with categories like 'Security Engineering Techniques' and 'Fundamentals of Security'. The main area has a search bar and four filter panels: 'Technology' (with options like .NET 1.1, .NET 2.0, ASP.NET 1.1, ASP.NET 2.0, Java Web 1 & 2), 'Phase' (Design, Implementation, Test), 'Type' (Attack, Checklist Item, Code Example, Guideline, How To, Inspection Question, Principle, Question and Answer), and 'Category' (Assembly Level Checks, Auditing and Logging, Authentication, Authorization, Bindings). Below the filters is a table of results with columns for Title, Technology, Phase, Type, and Category. The table lists various security issues like 'Parent paths' setting is disabled, authentication element is incorrectly configured, etc. Callout boxes point to the filter system, search capabilities, infoline, and the table.

Title	Technology	Phase	Type	Category
"Parent paths" setting is disabled.	Web Application	Deployment	Checklist Item	Server Hardening
+ authentication element is incorrectly configured	ASP.NET 1.1	Implementation	Checklist Item	Configuration
+ customErrors element is used to configure custom error messages.	ASP.NET 1.1	Implementation	Checklist Item	Configuration
+ machineKey element is configured properly	ASP.NET 1.1	Implementation	Checklist Item	Configuration
+ processModel element attributes are configured for specific purposes.	ASP.NET 1.1	Implementation	Checklist Item	Configuration
+ sessionState element is configured correctly	ASP.NET 1.1	Implementation	Checklist Item	Configuration
+ A certificate is installed on the database server to enable SSL connections.	Web Application	Deployment	Checklist Item	Server Hardening
+ A custom ASP.NET policy is used to access non-SQL Server databases from partial trust ASP.NET applications.	Web Application	Deployment	Checklist Item	Server Hardening
+ A custom least-privileged anonymous account is created for anonymous access.	Web Application	Deployment	Checklist Item	Server Hardening
+ An unhandled exception handler is used for Unhandled Exceptions	Java Web 1.4.2	Implementation	Checklist Item	Error and Exception Management

## CONTENT SCREEN

Single screen content is presented when the user selects a title from the list. The content is used in any way the user to guide them through the process of defining, designing, coding or testing secure functionality in their application.

The screenshot displays the TeamMentor interface with the following content:

**Guidance Item attributes** (Table):

Category	Phase	Technology	Type	Date
Deployment Considerations	Deployment	SQL Server 2000	Checklist Item	2/20/2009 1:28:59 AM

**Focused content that describes the problem and the solution:**

**How to Fix**  
 If you use Windows authentication (NTLM or Kerberos), login credentials are not passed over the network to SQL Server. If you use SQL authentication, it is a good idea to secure the credentials because they are passed to SQL Server in unencrypted format. Do this by installing a certificate on the database server. This automatically results in the encryption of SQL credentials over the wire. It is also a good idea to make sure that your application securely stores database connection strings.

**User comment area for feedback and additional context-specific information:**

**Comments**  
 Add a comment...  
 No one has commented on this guidance item.

The content screen is used to display all the various asset types and provides a rich environment for collaboration.

## GETTING GUIDANCE

Finding what's needed to implement secure functionality is a simple, straight forward activity in TeamMentor™. The two primary mechanisms available to users are navigation and searching, both of which may be followed by a filtering activity to auger in on the key information. In the following walkthrough we assume that we're a developer working with Java for Web applications and we've been given the task of implementing an authentication system.

### STEP 1 – CLASS SELECTION

After logging in, select “Guidelines” from the navigation tree. Guidelines are overviews of key areas to consider in the development process. This operation limits the list to only guideline elements, which may be browsed and selected. Notice that the “Search under selected node” button becomes available after the guidelines element is selected. This feature allows users to limit searches to the single class of items rather than the global content, further helping users to locate the desired content.

### STEP 2 – FILTERING

Next we mouse over the “Sort/Filter by” options, stopping over category. From the drop down we select “Authentication”. The result of this operation is a set of guidelines that describe Authentication issues.

Notice that the **category** reference in each items info line says “Authentication” and the type reference says “Guideline”. Try selecting other nodes from the tree and notice that the result set changes to reference only those types of guidance.





### STEP 3 – FILTER AGAIN

Our goal is to get guidance on authentication in the Java Web environment. To finish drilling down to this set it is necessary to filter a second time by mousing over “Technology” and selecting **Java Web Application** from the list.

The resulting list of guidelines is specifically what the user needs to understand authentication implementation in a Java Web App. All other selections made from the Asset Navigator will also be limited to the set filters and will remain so until they are released by the user.

```

md.update(result);
rawKey = md.digest();
md.reset();
SecretKeySpec skeySpec = new SecretKeySpec(rawKey, "AES");
// Set up cipher
Cipher cipher = Cipher.getInstance("AES");
cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
// Convert char[] to byte[]
tempPass = new byte[pass.length];
for (int i = 0; i < pass.length; i++)
{
    tempPass[i] = (byte)pass[i];
}
// Encrypt password
byte[] encrypted = cipher.doFinal(tempPass);
//Clean tempPass
for (int i = 0; i < tempPass.length; i++)
{
    tempPass[i] = 0;
}
return encrypted;

```

### STEP 4 – READ, RATE AND REVIEW

The individual documents/assets are opened by selecting the blue **title** of desired item in the list. This opens the item in its own window and is ready for consumption.

Scrolling to the bottom of the document brings you to the “Rate Content” section. This is a simple voting system that allows users to let others know how valuable the content potentially is. Ratings, being what they are, have limited value as the need of the user and the focus of the

content may or may not be in alignment, hence users are also given the opportunity to enter a freeform review of the item. The text from the review may be used by the system administrator to enhance the content directly using the provided content authoring tool or it can remain in the review section—either way users play a major role in how the content is used and grows.

## SEARCHING FOR SPECIFIC ASSETS

Using the TeamMentor Asset Navigator is a simple way to locate appropriate items to guide you through the development of secure functionality in applications, but sometimes you're not sure what you need—so you need to conduct a search. For this example we assume that a developer is responsible for implementing a secure communications pipe using SSL but doesn't have a clear idea where to start.

### STEP 1 – BASIC SEARCHING

After logging in using “user” for the username and “user” for the password, enter SSL into the “Search for:” text box and click **Search**. The result is not only a list of various different assets, but a **NEW TREE** titled “Search Results”. This tree contains only items that match the search criteria and may be used in the same way as the main tree - to limit the result list to a specific type of asset.

### STEP 2 – FILTERING

Mouse over **Topic** and notice that the filter has two entries, **security** and **performance**. Select **security** as that's the primary interest of the developer coding a secure communications pipe. Next, mouse over **Category** and select **Communications Security**. Note that several assets of different types are now available; each of which contains key information in setting up secure communications channels in various different environments—guiding the developer through the learning and development process. Further experimentation provides additional information too. For example, mousing over **Topic** and selecting **(all)**, and then **Performance** creates an information set that is focused on SSL performance issues.

## TEAMMENTOR ASSETS

There are several types of secure development asset in TeamMentor, each of which speaks to a specific problem and provides unique guidance and/or knowledge.

### ACTIVITY PATTERNS

Activity patterns are concise methods for common security engineering activities, such as code review, threat modeling, attacks etc. TeamMentor presents Activity Patterns by defining the context to which the pattern applies, the problem that the pattern relates to, the forces or motivation driving the activity and the actual solution/method for executing on the pattern. Activity patterns show users how to perform the key activities needed to develop secure applications.

### ANTI-PATTERNS

Anti-patterns are classes of commonly-bad reinvented solutions in software development that lead to security vulnerabilities. TeamMentor presents anti-patterns by defining the context where the pattern occurs, one or more examples of a flawed solution with references, symptoms and consequences of the pattern, a proper solution with benefits, and finally a list of any known liabilities coincident with the proper solution. Anti-patterns provide users with the knowledge they need to do things right by showing them, in unambiguous terms, how to do it wrong.

## CHECKLISTS

Checklists are detailed collections of steps used to verify design, implementation or deployment of a feature or function in an application. TeamMentor presents checklists by defining the context in terms of the type of functionality or environment the checklist applies to, what to look for and why the process is important. Next the checklist tells the user how to check the item and how to fix common problems that may be encountered along with appropriate problem and solution code examples. Checklists provide development teams with the tools they need to ensure that appropriate measures were taken to develop securely and that nothing was missed in the process.

## CODE EXAMPLES

TeamMentor provides standalone code examples of key common functionality that users can cut and paste into their own applications. Code samples may be complete, secure systems or snippets that outline the key concepts needed for secure implementation.

## DESIGN PATTERNS

Design Patterns are proven solutions for common problems in software design. TeamMentor presents design patterns by defining the context of the pattern, the problem it solves, the forces and motivations driving its use, and the complete solution. Design patterns show developers what good design looks like and provides an appropriate context for developing their own secure applications.

## GUIDELINES

Guidelines are outlines for developing secure code in a specific development environment, why it's important and how to do it. TeamMentor presents guidelines by defining the what, why and when followed by detailed instructions on how to implement with appropriate problem and solution examples. Guidelines allow developers to recognize problem areas and understand the best way(s) to address them.

## HOW TO'S

How To's are step by step guides that lead to successful completion of a security related development task. TeamMentor presents How To's in the manner most appropriate to the technology area and provides complete guidance for implementation and/or use of specific functionality or resource usage. How To's reduce the amount of time users need to spend figuring out how to do something by providing the answers up front and just in time.

## PRINCIPLES

Principles are the fundamental laws that underlie the guidelines and other guidance types presented by TeamMentor. TeamMentor presents principles as granular items that describe the issue, its impact, potential vulnerabilities and countermeasures. Principles provide global context to users and ground security issues in reality for them.

## TEST CASES

Test Cases are specialized How To documents that walk users through the steps necessary to test for common vulnerabilities. TeamMentor presents Test Cases as collections of manual tests and techniques to uncover common problems. They include the environment the test applies to, a summary of the test

case and finally the test itself with appropriate variables, values, inputs, expected results and other key instruction. Test Cases enable users to perform focused security testing that they would normally not be equipped to execute; and uncover vulnerabilities before applications go into general use. TeamMentor's assets are updated regularly, with new items being added and existing ones revised to account for changes in the threat landscape or development technology. As needs arise, new asset classes may be added to the knowledge base and provide solutions to other problems that show up down the road.

## 4.0 Key Features and Benefits

---

### FOCUSED SECURITY GUIDANCE

Guidance for developing secure code is provided for major languages and deployment technologies in the forms best absorbed by all members of the development team including checklists, how-to guides, design patterns, design anti-patterns, principles, FAQs, etc.

### ASSET NAVIGATOR

Users can navigate into specific asset classes that span multiple technologies to locate the key items they need (i.e. "All Check Lists" or "All Principles"). Navigation into an asset class also enables focused searching within that class, so finding the specific guidance item a user needs is greatly simplified.

### ASSET FILTERING

Users can focus the items in lists resulting from navigation or searching by "filtering" the list and limiting it to only items of a specific technology, category, type, topic or priority. For example, if one searches for "SSL" a large list is returned. The user can then filter on "Java" and the new result list is reduced to only those items in the search that relate to Java.

### FOCUSED SEARCHING

Users can search the knowledge base globally, considering all available items, or limit the search to a single library or a single asset class within that library. This type of searching allows users to zero in on the assets they need quickly and effectively.

### REVIEWING AND RANKING

Users can rate guidance items and add comments to enhance them. Enhancements may be integrated with the main content using the administrator's authoring tool or left on the "Reviews" tab alongside the content.

### CONTENT AUTHORING

Users and administrators may create new views, items and complete libraries as needed using the administrators authoring tool.