Peer Review of “Top 5 Secure Coding Practices” Presentation

1 Main Ideas

1. **Input Validation:** Ensures only properly formatted data is accepted using methods like regular expressions.
2. **Output Encoding:** Prevents XSS attacks by encoding special characters in outputs.
3. **Authentication and Password Management:** Focuses on strong password policies.
4. **Session Management:** Handles session IDs securely and renews them periodically.
5. **Access Control:** Uses least privilege principles to regulate access to resources.
6. **Error Handling and Logging:** Avoids revealing sensitive information in error messages and logs securely.
7. **Data Protection:** Maintains data confidentiality and integrity through encryption.
8. **Communication Security and Database Security:** Uses TLS for secure data transmission and safe database operations.
9. **File and Memory Management:** Implements safe file uploads and prevents memory vulnerabilities like buffer overflows.

2 Topics in the Discussion Forum

The discussion forum encouraged participants to explore various aspects of secure coding practices.

- The differences between client-side and server-side validation.
- The role of output encoding in preventing vulnerabilities.

- Techniques for secure password storage.
- Best practices for session management.

3 Critique of the Presentation Slide (30 Points)

3.1 Improvement Over the Original (2023 Version)

The current version is comprehensive.

Recommendation: Add a comparative chart or a “What’s New” section to highlight changes since 2023.

3.2 Flow

The information flows logically from basic to more specific topics.

Recommendation: Use transition slides or a case study to show how practices are connected.

3.3 Coverage

All topics are covered with examples but some areas could use more detailed real-world examples.

Recommendation: Add practical use cases to provide a more complete discussion.

4 Critique of the Discussion Forum Activity (10 Points)

4.1 Questions/Comments

The questions are relevant focusing on key aspects of secure coding.

Recommendation: Include scenario-based or open-ended questions.

4.2 Major Issues

The questions address core concerns like XSS prevention.

Recommendation: Add questions about new threats or trends such as AI-related vulnerabilities.

5 Critique of the Discussion Forum Interaction (10 Points)

5.1 Presenter Engagement

It's hard to assess engagement but the forum structure suggests active participation.

Recommendation: Highlight notable discussions or presenter contributions to show engagement.

5.2 Further Discussion

The questions encourage meaningful discussion but could use follow-up prompts.

6 Recommendations for Improvement

6.1 Presentation Content

Use more visuals like diagrams to explain complex concepts and include real-world case studies.

6.2 Forum Activity

Encourage participants to share personal experiences or industry-specific challenges.