Java Security Interview Questions

1. What are the different things to consider regarding security of a web application?
2. What are the important things to consider regarding user authentication and authorization?
3. What are the important factors to consider when exposing an application to Internet?
4. What are important security factors to consider in communicating with external interfaces?
5. What are the Best Practices regarding handling security for a web application?

What are the different things to consider regarding security of a web application?

Security related consideration can be split into these parts

- User Authentication and Authorization
- Web Related Issues
- External Interfaces
- Infrastructure Related Security

What are the important things to consider regarding user authentication and authorization?

Following are the important considerations:

- Proper separation of authenticated and unauthenticated resources. These can be split into separate deployable units if possible.
- Proper use of filters to ensure that the configuration for authenticated resources is centralized.

- Use a proper framework like Spring Security to implement authorization.

What are the important factors to consider when exposing an application to Internet?

OWASP (Open Web Application Security Project) is normally a great starting point. Important factors to consider are

- Validaton of user data : Ensure they are validated also in Business Layer.
- SQL Injection : Never build sql queries using string concatenation. Use a Prepared Statement. Even better, use Spring JDBCTemplate or frameworks like Hibernate, iBatis to handle communication with database.
- XSS - Cross Site Scripting : Ensure you check against a white list of input characters.
- Avoid using Old versions of software

What are important security factors to consider in communicating with external interfaces?

Security for web services (over JMS or HTTP) has to be handled at two levels : Transport level and Application level.

For HTTP based services, SSL is used to exchange certificates (HTTPS) to ensure transport level security. This ensures that the server (service producer) and client (service consumer) are mutually authenticated. It is possible to use one way SSL authentication as well.

For JMS based services, transport level security is implemented by controlling access to the Queues.

At the application level (for both JMS and HTTP based services), security is implemented by transferring encrypted information (digital signatures, for example) in the message header (SOAP Header). This helps the server to authenticate the client and be confident that the message has not been tampered with.

What are the Best Practices regarding handling security for a web application?

Best practices are:

- Threat Modelling : Do threat modelling and understand the various security threats posed to the application
- Static Security Analysis : Use a static security analysis tool like Fortify.
- Educate Developers and Testers : Most important part. Developers and Testers should be aware of the latest security threats.
- Dynamic Security Tests : Dynamic security tests done by a professional security testing team should be an important part of the release cycle. It is preferable to do this as early as possible.

questions.html), REST Web Services (http://www.javainterview.in/p/rest-web-services-interview-questions.html),Security (http://www.javainterview.in/p/security-interview-questions.html), Continuous Integration (http://www.javainterview.in/p/continuous-integration-interview.html)

Home (http://www.javainterview.in/)