OutSystems

Security-Specialist
Security Specialist (OutSystems 11)

Questions & Answers PDF

For More Information:

https://www.certswarrior.com/

Features:

- ➢ 90 Days Free Updates
- ➢ 30 Days Money Back Guarantee
- ➢ Instant Download Once Purchased
- ➢ 24/7 Online Chat Support
- ➢ Its Latest Version

Latest Version: 6.0

Question: 1

How does OutSystems address the requirement of audit controls under HIPAA Technical safeguards to track and monitor access to EPHI?

A. OutSystems relies on external audit tools, and it does not have built-in audit controls.
B. OutSystems only logs successful access attempts, neglecting failed attempts.
C. OutSystems includes a robust audit trail feature, capturing and logging all activities related to ePHI access.
D. Audit controls are not a concern for OutSystems, as it focuses solely on application development.

Answer: C

Question: 2

In OutSystems, when configuring a SAML identity provider for Okta integration, what is a crucial consideration to ensure secure communication?

A. Use a single, shared SAML certificate for all applications.
B. Ensure the SAML certificate is securely stored and regularly rotated.
C. Implement a separate SAML identity provider for each application.
D. Enable automatic user provisioning without additional security checks.

Answer: B

Question: 3

What is a potential security risk that developers should be aware of when storing Google API keys in OutSystems applications, and how can it be mitigated?

A. Embedding API keys in client-side variables increases the risk of exposure. Mitigation: Utilize serverside logic to fetch API keys securely.
B. Storing API keys in a shared configuration module poses a risk of cross-module access. Mitigation: Implement access controls to restrict module access.
C. Storing API keys in server-side configuration files exposes them to unauthorized access. Mitigation: Implement encryption for stored API keys.
D. Using environment variables for API key configurations may lead to deployment errors. Mitigation: Implement automated deployment scripts for consistency.

Answer: C

Question: 4

In a Reactive Web application, what is the primary purpose of the Content Security Policy (CSP), and how does it contribute to security?

A. CSP is used for styling purposes only.
B. CSP restricts the types of content that can be loaded, mitigating risks such as Cross-Site Scripting (XSS).
C. CSP focuses on server-side security only.
D. CSP is irrelevant in Reactive Web applications.

Answer: B

Question: 5

When designing an anonymous screen for a password recovery page in OutSystems, what is a recommended practice to tackle vulnerabilities related to sensitive user information?

A. Store recovered passwords in clear text for seamless troubleshooting.
B. Implement proper input validation and ensure secure handling of password recovery requests.
C. Avoid using encryption for password recovery to simplify the process.
D. Display the recovered password directly on the screen for user convenience.

Answer: B

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ