

GlobalTcert.com

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

Total Questions #64.

Missing answers will be provided in next update.

QUESTION 1

You are an application developer for GlobalitcerT .com. You develop library assemblies that are called by your main applications. These library assemblies access confidential data in the applications. To ensure that this data is not accessed in an unauthorized and unsafe manner, users must not be allowed to call the library assemblies from their own applications. You apply a strong name to all assemblies to support versioning.

You need to prevent users from writing managed applications that make calls to your library assemblies. You need to achieve this goal while minimizing the impact on response times for applications.

What should you do?

- A. Use the internal access modifier to declare all classes and structures in each library.
- B. Use the protected internal access modifier to declare all classes and structures in each library.
- C. Add the following attribute to each class and structure in each library assembly:
<StrongNameIdentityPermission(SecurityAction.Demand, PublicKey:="002400..bda4")>
- D. Add the following attribute to each class and structure in each library assembly:
<StrongNameIdentityPermission(SecurityAction.LinkDemand, PublicKey:="002400..bda4")>

Answer: C

QUESTION 2

You are an application developer for GlobalitcerT .com. You are developing an application that can be extended by using custom components. The application uses reflection to dynamically load and invoke these custom components. In some cases, custom components will originate from a source that is not fully trusted, such as the Internet.

You need to programmatically restrict the code access security policy under which custom components run so that custom components do not run with an elevated permission grant.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

- A. Create a new application domain and set the security policy level. Run custom components in this application domain.
- B. Use permission class operations to modify the security policy.
- C. Implement custom permission classes to protect custom component resources.
- D. Programmatically modify the machine-level security policy file after loading a custom component.

Answer: B, C

QUESTION 3

You are an application developer for your company, which is named GlobalitcerT .com. You are developing an ASP.NET Web application that users in the accounting department will use to process payroll reports and view payroll reports. The application will use Integrated Windows authentication to authenticate all users.

Because payroll data is confidential only users in the accounting department will be granted access to the application. All employees in the accounting department belong to a specific Active Directory group. However, users in the IT department can add themselves to various Active Directory groups in order to troubleshoot resource access problems. These IT department users must not be granted access to the ASP.NET Web application.

The following rules can be used to distinguish between users in the accounting department and users in the IT department:

- All users in the accounting department are members of a group named GlobalitcerT \Accounting.
- Some users in the IT department are members of the GlobalitcerT \Accounting group.
- All users in the IT department are members of a group named GlobalitcerT \Domain Admin.
- No users in the accounting department are members of the GlobalitcerT \Domain Admin group.

You need to configure URL authorization for the application by adding an <authorization> element to the Web.config file in the application root.

Which element should you use?

A. <authorization>

```
<deny roles=" GlobalitcerT \Domain Admin"/>
```

```
<allow roles=" GlobalitcerT \Accounting"/>
```

```
<deny users="*/>
```

```
</authorization> B.
```

```
<authorization>
```

```
<allow roles=" GlobalitcerT \Accounting"/>
```

```
<deny roles=" GlobalitcerT \Domain Admin"/>
```

```
<dent users="?"/>
```

```
<authorization>
```

C. <authorization>

```
<deny roles="Domain Admin"/>
```

```
<allow roles="Accounting"/>
```

```
<deny users="*/>
```

```
</authorization> D.
```

```
<authorization>
```

```
<allow roles="Accounting"/>
```

```
<deny roles="Domain Admin"/>
```

```
<deny users="?"/>
```

```
</authorization>
```

Answer: A

QUESTION 4

You are an application developer for GlobalitcerT .com. You develop an ASP.NET Web application for GlobalitcerT 's intranet. The application accesses data that is stored in a Microsoft SQL Server database. The

application authenticates users by using Windows authentication, and it has impersonation enabled. You configure database object permissions based on the identity of the user of the application. You need to provide the user's identity to the SQL Server database. What should you do?

- A. Connect to the database by using the following connection string
"Persist Security Info=False;Integrated Security=SSPI;
database=ApplicationDB;server=DataServer;"
- B. Connect to the database by using the following connection string
"User ID=ASPNET;Persist Security Info=False;Integrated
Security=False;
database=ApplicationDB;server=DataServer;"
- C. Develop a serviced component that wraps all database operations.
Use COM+ role-based security to restrict access to database operations based on user identity.
- D. Disable impersonation.

Answer: A

QUESTION 5

You are an application developer for GlobalitcerT .com. You create an ASP.NET Web application that all authenticated network users will access. The authentication mode in the Web.config file is currently set to None. Due to recent security threats, the network administrator requires that all connections to the application's Web server use the network credentials of the authenticated user.

You need to configure the application to use the network credentials of the authenticated user as HttpContext.Current.User.

Which action or actions should you perform? (Choose all that apply)

- A. Ask the network administrator to configure the IIS directory security to Anonymous authentication.
- B. Ask the network administrator to configure the IIS directory security to Integrated Windows authentication.
- C. Set the authentication mode in the Web.config file to Forms.
- D. Set the authentication mode in the Web.config file to Windows.
- E. Set the impersonation attribute of the identity element in the Web.config file to true.

Answer: B, D, E

QUESTION 6

You are an application developer for GlobalitcerT .com. You develop a Windows Forms application. You want your application to use a class library that was developed by another developer. You run the Permissions View tool on the class library and receive the following output.

Microsoft (R) .NET Framework Permission Request Viewer. Version
1.1.4322.573

Copyright (C) Microsoft Corporation 1998-2002. All rights reserved.
minimal permission set:

```
<PermissionSet class="System.Security.PermissionSet"  
version="1">
```