MS_logo_KMICROSOFT SDL - DEVELOPER STARTER KIT:

BANNED APIs (LEVEL 200)

Comprehension Questions

Version 1.0

The following questions accompany the materials for the Microsoft SDL - Developer Starter Kit Banned APIs (Level 200) presentation.

For the latest information, please see [www.microsoft.com/sdl](http://go.microsoft.com/?linkid=9672761).

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Visual C#, Visual C++, Visual Studio, Windows, Windows Server, SQL Server, and Windows Vista are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

CONTENTS

[1.0 Microsoft SDL - Developer Starter Kit Content Comprehension Questions 2](#_Toc233530736)

[1.1 INTRODUCTION 2](#_Toc233530737)

[2.0 Banned APIs (Level 200) Questions 2](#_Toc233530738)

# 1.0 Microsoft SDL - Developer Starter Kit Content Comprehension Questions

## 1.1 INTRODUCTION

“The Microsoft Security Development Lifecycle (SDL) is an industry-leading software security assurance process. A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture. Combining a holistic and practical approach, the SDL introduces security and privacy early and throughout all phases of the development process. It has led Microsoft to measurable and widely-recognized security improvements in flagship products, such as Windows Vista, Windows Server (2003 and 2008) and SQL Server. Microsoft is publishing the detailed SDL process guidance as part of its commitment to enable a more secure and trustworthy computing ecosystem.” -- [The Microsoft SDL 3.2 Whitepaper](http://go.microsoft.com/?linkid=9672762)

To help promote the adoption and awareness of the Microsoft SDL, Microsoft has developed content and demonstrations specifically for external developer audiences. The remainder of this document provides individuals who will present this content internally within their respective organizations with questions that may be used to ascertain comprehension of the subject matter addressed within the Microsoft SDL Training Module: Banned APIs (Level 200) presentation. These questions have been designed to enable the presenter to ascertain the extent at which the participating personnel with application development responsibilities have comprehended the subject matter addressed in the Banned APIs (Level 200) training module, as well as enabling the presenter to assess participants’ ability to apply the subject matter addressed to practical secure and trustworthy application development scenarios.

# 

# 2.0 Banned APIs (Level 200) Questions

**Question #1:** True or false: The functions and libraries listed in the Microsoft Banned API listing are only relevant for applications developed using Microsoft technologies and platforms.

1. True.
2. False.

**Answer:** The correct answer is “B”. The Microsoft Banned API listing is essentially a listing of C runtime functions and libraries that, in Microsoft’s experience, when used incorrectly can lead to serious vulnerabilities. Since C can be used to implement applications on almost every known operating system and platform, the Microsoft Banned API listing is also applicable to non-Microsoft technologies and platforms.

**Question #2:** True or false: The C runtime “n” functions are considered safe alternatives to the functions and libraries listed in the Microsoft SDL Banned APIs listing.

1. True.
2. False.

**Answer:** The correct answer is “B” (False). The C runtime “n” functions are also included as part of the Microsoft SDL Banned APIs listing. In Microsoft’s experience, the C runtime “n” functions are difficult for developers to call correctly without extensive knowledge of these functions. To err on the side of caution, Microsoft has decided to also ban the use of the C runtime “n” functions for applications developed to be aligned with the Microsoft SDL.

**Question #3:** Under what conditions will szDest not be null-terminated?

void Function(char \* pszSrc)

{

char szDest[32];

strncpy(szDest,pszSrc,32);

}

1. When the length of pszSrc is greater than or equal to 32 bytes.
2. When the length of pszSrc is 1 byte.
3. When the length of pszSrc is 8 bytes.
4. When the length of pszSrc is 16 bytes.

**Answer:** The correct answer is “**D**”. In the code above, strncpy will not null-terminate the destination buffer when the length of the source parameter is equal to or greater than 32 bytes. Small nuances like these regarding the C runtime “n” functions make them difficult to use and is one of the reasons why they are listed as part of the Microsoft SDL Banned API listing.

**Question #4:** Can the Safe CRT Secure Template Overloads feature be used in the C code below?

void Function(char \* s1, size\_t length)

{  
 char \* temp = (char \*)malloc(length)

strcpy(temp,s1);  
 }

1. Yes, because the function does not provide a return value to the caller.
2. Yes, because the length of the buffer is defined as a size\_t.
3. No, because the length of the buffer is not known at compile-time.
4. No, because Safe CRT Secure Template Overloads is applicable to C++ applications and not C applications.

**Answer:** The correct answer is “**C**”. In order to use the Safe CRT Secure Template Overloads feature, the length of the allocated buffer must be known at compile-time. The length of the temp buffer in the code shown above is known at run-time only.

**Question #5:** A developer has taken proactive steps to improve her code by replacing banned API instances with safer StrSafe alternatives. The developer is unsure as to whether she has used StrSafe appropriately and has asked you to help review the new code as shown below. What is wrong, if anything, with the code shown below?

#include <strsafe.h>

HRESULT Function(char \* s1)

{

char temp[256];

HRESULT hr = StringCchCopy(temp,strlen(s1),s1);

return(hr);

}

1. There is nothing wrong with the code shown above.
2. The call to StringCchCopy or any other StrSafe function does not return a return value.
3. The size parameter provided to StringCchCopy uses the length of the source buffer, and not the destination buffer.

**Answer:** The correct answer is “**C**”. The StringCchCopy size parameter should be the size of the destination buffer. This is an example why using safer alternatives to the Microsoft SDL Banned APIs listing still requires developers to take care to verify that destination buffer sizes are correct.