



# Security Toolbox for .NET Development and Testing

Johan Lindfors & Dag König  
Microsoft

**OWASP**

Copyright 2007 © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**  
<http://www.owasp.org>

---

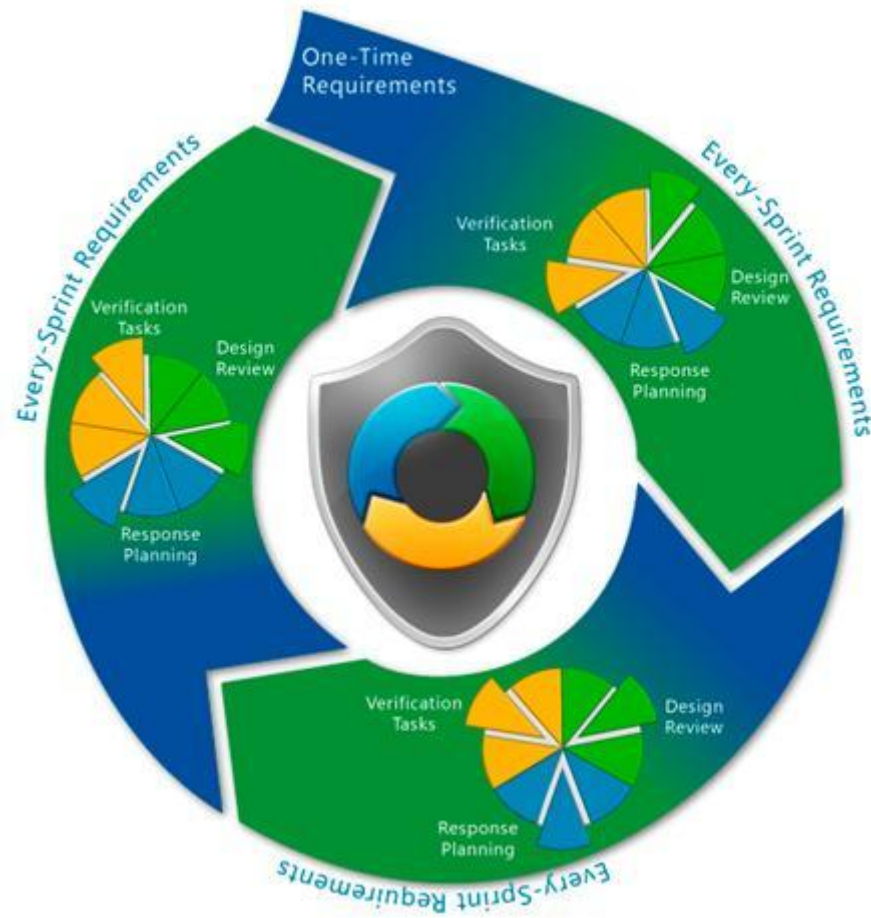
# Security: When and what?

- Design
- Development
- Testing
- Secure by design
- Secure by default

---

# **MSF Agile + SDL 5.0** **in** **Team Foundation Server**

+ SDL Threat Modeling Tool



---

# WPL

- Web Protection Library
- AntiXSS
  - ▶ White Lists
  - ▶ Secure Globalization
- Security Runtime Engine
  - ▶ Cross Site Scripting
  - ▶ SQL Injections

---

# Static Code Analysis

## ■ FxCop

- ▶ Analysis of performance, design and security issues
- ▶ Primarily focused on Code Access Security

"Have you used security features the right way?"

## ■ CAT.NET - Code Analysis Tool

- ▶ Previously only and internal tool

"Have you written your other features securely?"

# Pex and Moles



- Pex automatically generates test suites
  - ▶ High code coverage
  - ▶ Interesting input/output values
- Moles allows to replace .NET methods with delegates

Pex Exploration Results - stopped - 12 tests, 192 runs - 21/21 dynamic coverage

StringExtensions.Capitalize(String)

	value	result	Summary/Exception	Error Message
1	null		ArgumentNullException	Value cannot be null.Parameter name: value
2	""	""		
3	"\0"	""		
4	":"	""		
5	"a"	"A"		
6	"h\0"	"H"		
7	"ha"	"Ha"		
8	"haa"	"Haa"		
9	"\0"	""		
10	"::"	""		
11	"h\u8061\0"	"H_\u8061"		
12	"h::zh\0\0..."	"H_Z_H_..."		

# WACA

## ■ Web Application Configuration Analyzer

- ▶ CAT.NET 2.0
- ▶ IIS and .NET Framework
- ▶ SQL Server
- ▶ Windows Permissions

## ■ Export report

- ▶ Excel, HTML, TFS

## ■ Remote scans

Microsoft Web Application Configuration Analyzer v1.0 - [Scan Report 1]

Select a scan: JOHANL2\_22062010221344

### Scan Report for JOHANL2\_22062010221344

Summary of the scan			
Machine Name:	JOHANL2	Start Time:	06/22/2010 22:13:45
SQL Server:	JOHANL2\SQLEXPRESS	End Time:	06/22/2010 22:17:01
General Application Rules:	47.06% (8 of 17) Passed		52.94% (9 of 17) Failed
IIS Application Rules:	77.55% (38 of 49) Passed		22.45% (11 of 49) Failed
SQL Application Rules:	NaN% (0 of 0) Passed		NaN% (0 of 0) Failed
All Rules:	69.7% (46 of 66) Passed		30.3% (20 of 66) Failed

#### General Application Rules

1	Is Drive (C:) Partition a Non-NTFS File System?	No, Passed	
2	Is guest account enabled on the server?	No, Passed	
3	Does Windows Drive Root Folder (C:) NTFS ACL contain Everyone ACE? Does Windows Drive Root Folder (Q:) NTFS ACL contain Everyone ACE?	No, Passed Yes, Failed	Windows Drive Root Folder (Q:) NTFS ACL contains ACE for Everyone
4	Does Windows Drive Root Folder (C:) NTFS ACL contain Authenticated Users ACE? Does Windows Drive Root Folder (Q:) NTFS ACL contain Authenticated Users ACE?	Yes, Failed No, Passed	Windows Drive Root Folder (C:) NTFS ACL contains ACE for Authenticated Users
5	Does Windows Drive Root Folder (C:) NTFS ACL contain Guest ACE? Does Windows Drive Root Folder (Q:) NTFS ACL contain Guest ACE?	No, Passed No, Passed	
6	Are the password complexity rules disabled on server?	No, Passed	



# CodeContracts



- Express coding assumptions
  - ▶ Pre-conditions
  - ▶ Post-conditions
  - ▶ Object invariants
- Static and runtime checking
- Documentation Generation

---

## How to keep updated!

[blogs.msdn.com/securitytools](https://blogs.msdn.com/securitytools)

[msdn.microsoft.com/security](https://msdn.microsoft.com/security)

[msdn.microsoft.com/practices](https://msdn.microsoft.com/practices)

[www.codeplex.com](https://www.codeplex.com)

[msdn.se](https://msdn.se)

---

# ***Microsoft***<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. 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 provided after the date of this presentation.  
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

