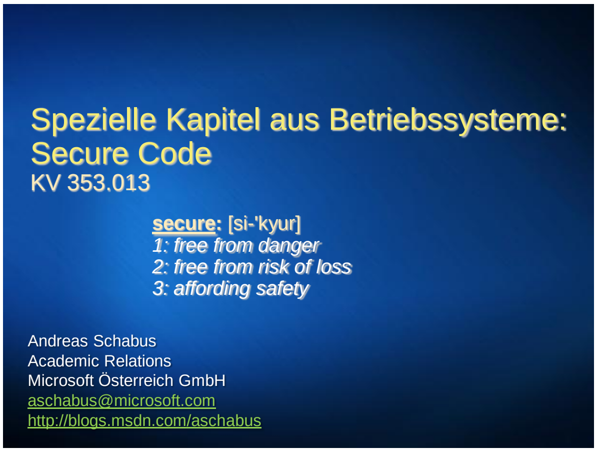
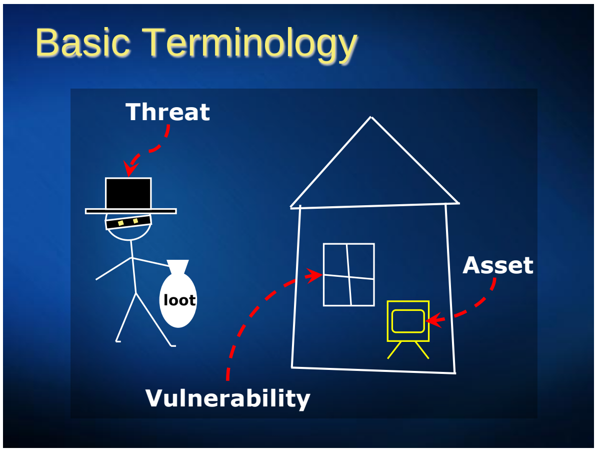


Spezielle Kapitel aus Betriebssysteme: Secure Code

KV 353.013

secure: [si-'kyur]
1: free from danger
2: free from risk of loss
3: affording safety

Andreas Schabus
Academic Relations
Microsoft Österreich GmbH
aschabus@microsoft.com
http://blogs.msdn.com/aschabus

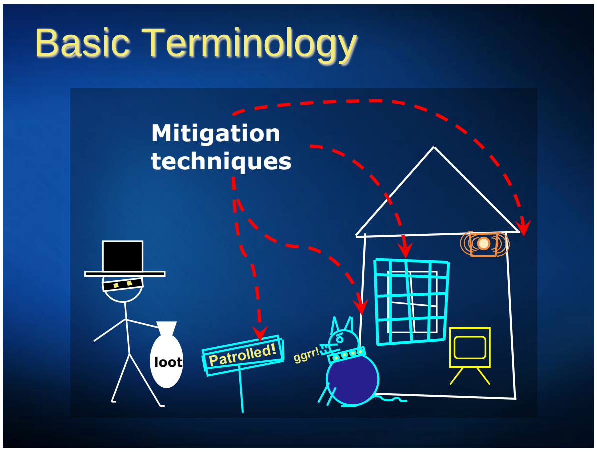


Basic Terminology

Threat

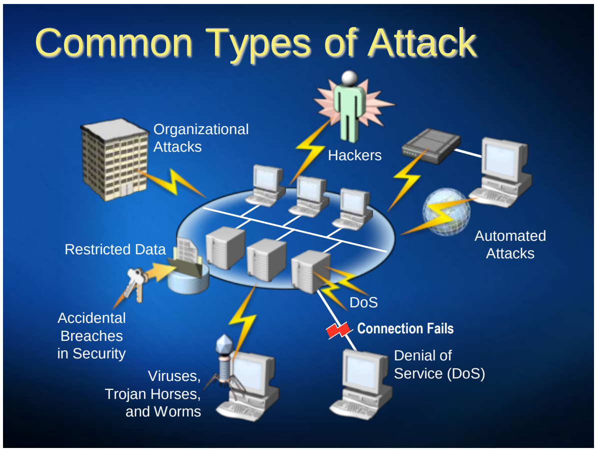
Asset

Vulnerability



Basic Terminology

Mitigation techniques



Common Types of Attack

Organizational Attacks

Hackers

Restricted Data

Automated Attacks

DoS

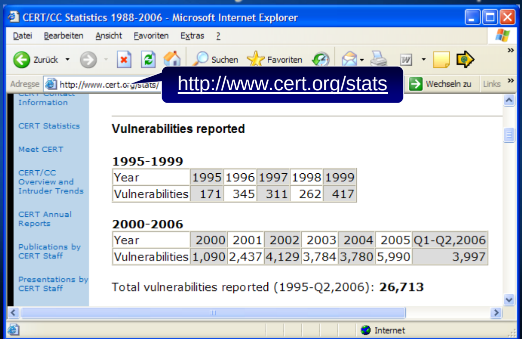
Connection Fails

Accidental Breaches in Security

Viruses, Trojan Horses, and Worms

Denial of Service (DoS)

Security is one of the top issues in today’s IT landscape


CERT/CC Statistics 1988-2006 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
http://www.cert.org/stats/
Wechseln zu
Links
CERT Contact Information
CERT Statistics
Meet CERT
CERT/CC Overview and Intruder Trends
CERT Annual Reports
Publications by CERT Staff
Presentations by CERT Staff
Internet

http://www.cert.org/stats

Vulnerabilities reported

1995-1999

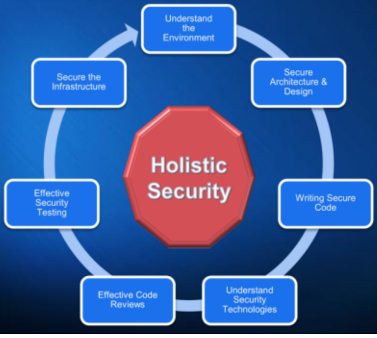
Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2006

Year	2000	2001	2002	2003	2004	2005	Q1-Q2,2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	3,997

Total vulnerabilities reported (1995-Q2,2006): **26,713**

We need a holistic security approach including development


Understand the Environment
Secure Architecture & Design
Writing Secure Code
Understand Security Technologies
Effective Code Reviews
Effective Security Testing
Secure the Infrastructure
Holistic Security

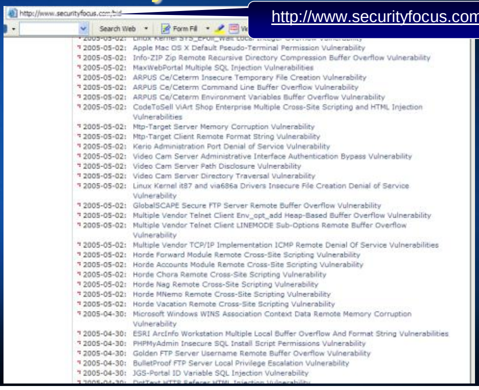
The Attacker‘s Advantage and the Defender‘s Dilemma

- The defender must defend all points; the attacker can choose the weakest point
- The defender can defend only against known attacks; the attacker can probe for unknown vulnerabilities
- The defender must be constantly vigilant; the attacker can strike at will
- The defender must play by the rules; the attacker can play dirty

Too often security is seen as an administration issue only

Our network is secure, right?
Oh sure, Don’t worry. We have several firewalls

An Industry Problem



http://www.securityfocus.com/bid

```
2005-05-02:  Apple Mac OS X Default Pseudo-Terminal Permission Vulnerability
2005-05-02:  Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow Vulnerability
2005-05-02:  MaxWebPortal Multiple SQL Injection Vulnerabilities
2005-05-02:  ARPUS Ce/Ceterm Insecure Temporary File Creation Vulnerability
2005-05-02:  ARPUS Ce/Ceterm Command Line Buffer Overflow Vulnerability
2005-05-02:  ARPUS Ce/Ceterm Environment Variables Buffer Overflow Vulnerability
2005-05-02:  CodeToSell ViArt Shop Enterprise Multiple Cross-Site Scripting and HTML Injection
             Vulnerabilities
2005-05-02:  Mtp-Target Server Memory Corruption Vulnerability
2005-05-02:  Mtp-Target Client Remote Format String Vulnerability
2005-05-02:  Kerio Administration Port Denial of Service Vulnerability
2005-05-02:  Video Cam Server Administrative Interface Authentication Bypass Vulnerability
2005-05-02:  Video Cam Server Path Disclosure Vulnerability
2005-05-02:  Video Cam Server Directory Traversal Vulnerability
2005-05-02:  Linux Kernel it87 and via686a Drivers Insecure File Creation Denial of Service
             Vulnerability
2005-05-02:  GlobalSCAPE Secure FTP Server Remote Buffer Overflow Vulnerability
2005-05-02:  Multiple Vendor Telnet Client Env_opt_add Heap-Based Buffer Overflow Vulnerability
2005-05-02:  Multiple Vendor Telnet Client LINEMODE Sub-Options Remote Buffer Overflow
             Vulnerability
2005-05-02:  Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities
2005-05-02:  Horde Forward Module Remote Cross-Site Scripting Vulnerability
2005-05-02:  Horde Accounts Module Remote Cross-Site Scripting Vulnerability
2005-05-02:  Horde Chora Remote Cross-Site Scripting Vulnerability
2005-05-02:  Horde Nag Remote Cross-Site Scripting Vulnerability
2005-05-02:  Horde MNemo Remote Cross-Site Scripting Vulnerability
2005-05-02:  Horde Vacation Remote Cross-Site Scripting Vulnerability
2005-04-30:  Microsoft Windows WINS Association Context Data Remote Memory Corruption
             Vulnerability
2005-04-30:  ESRI ArcInfo Workstation Multiple Local Buffer Overflow And Format String Vulnerabilities
2005-04-30:  PHPMyAdmin Insecure SQL Install Script Permissions Vulnerability
2005-04-30:  Golden FTP Server Username Remote Buffer Overflow Vulnerability
2005-04-30:  BulletProof FTP Server Local Privilege Escalation Vulnerability
2005-04-30:  JGS-Portal ID Variable SQL Injection Vulnerability
```

Security Today

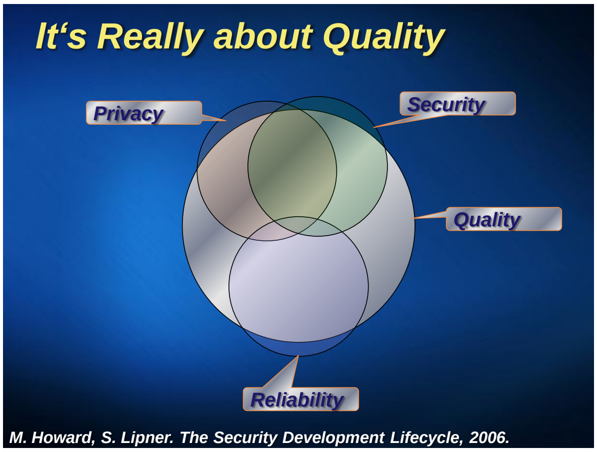
- Technology alone will not solve your problem
- Nobody believes anything bad can happen to them, until it does
- Security works only if the secure way also happens to be the easiest way
- In you do not keep up with security fixes, your network will not be yours for long
- There really is someone out there trying compromise your systems
- Your data and systems are of value to someone
- Security is not about risk elimination; it is about risk management

Note…

Security is only as good
as its weakest link

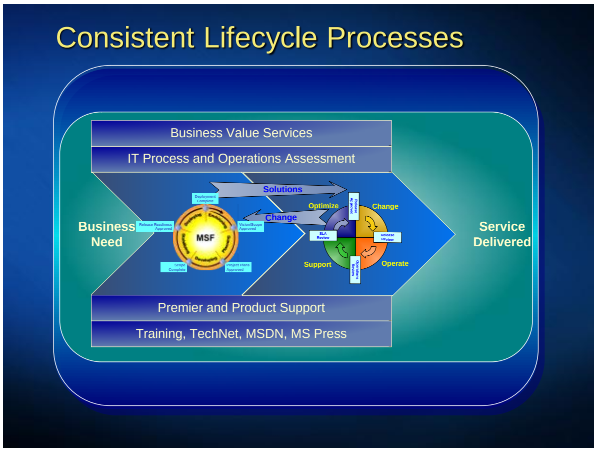
!!! Reminder !!!

Mind you, hacking is illegal and you are solely responsible for how you use what you learn ...



It‘s Really about Quality

M. Howard, S. Lipner. The Security Development Lifecycle, 2006.



Consistent Lifecycle Processes

Business Value Services

IT Process and Operations Assessment

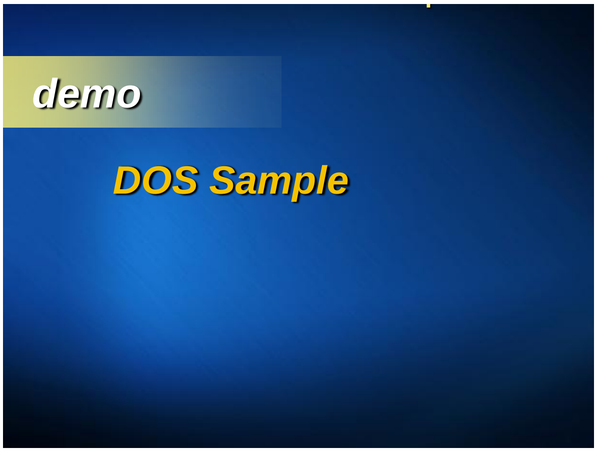
Business Need

Service Delivered

Premier and Product Support

Training, TechNet, MSDN, MS Press

Why should Developers care?



demo

DOS Sample

demo

Buffer-Overflow Sample

Security is (also) a challenge for Developers!

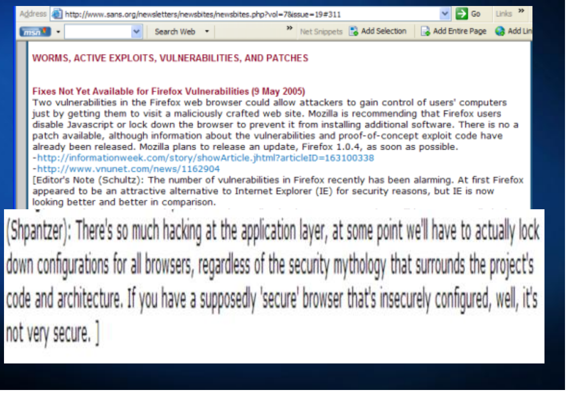
“Over 70 percent of security vulnerabilities exist at the application layer, not the network layer” – *Gartner*

“75 percent of hacks happen at the application” - *Gartner “Security at the Application Level”*

“The battle between hackers and security professionals has moved from the network layer to the Web applications themselves" *- Network World*

---

www.sans.org – 9.5.2005


Address
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=7&issue=19#311
Go
Links
msn
Search Web
Net Snippets
Add Selection
Add Entire Page
Add Lin

WORMS, ACTIVE EXPLOITS, VULNERABILITIES, AND PATCHES

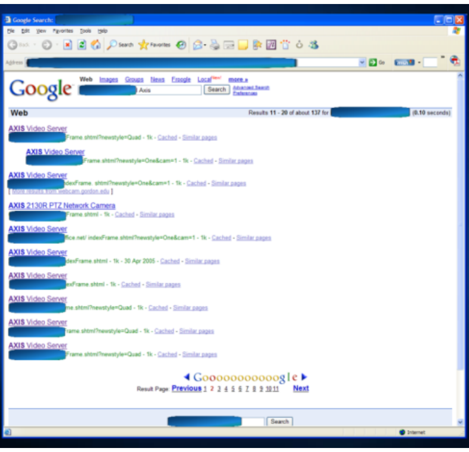
Fixes Not Yet Available for Firefox Vulnerabilities (9 May 2005)
Two vulnerabilities in the Firefox web browser could allow attackers to gain control of users' computers just by getting them to visit a maliciously crafted web site. Mozilla is recommending that Firefox users disable Javascript or lock down the browser to prevent it from installing additional software. There is no a patch available, although information about the vulnerabilities and proof-of-concept exploit code have already been released. Mozilla plans to release an update, Firefox 1.0.4, as soon as possible.
-http://informationweek.com/story/showArticle.jhtml?articleID=163100338
-http://www.vnunet.com/news/1162904
[Editor's Note (Schultz): The number of vulnerabilities in Firefox recently has been alarming. At first Firefox appeared to be an attractive alternative to Internet Explorer (IE) for security reasons, but IE is now looking better and better in comparison.

(Shpantzer): There's so much hacking at the application layer, at some point we'll have to actually lock down configurations for all browsers, regardless of the security mythology that surrounds the project's code and architecture. If you have a supposedly 'secure' browser that's insecurely configured, well, it's not very secure.]

Ridiculous Excuses We‘ve Heard

Excuse:
No one will do that!

Excuse:
Why would anyone do that?


Google Search: [redacted]
File Edit View Favorites Tools Help
Back Search Favorites
Address [redacted]
Go
Web Images Groups News Froogle Local New! more »
Search
Advanced Search
Preferences
Internet

[redacted] Axis

Web Results **11** - **20** of about **137** for [redacted] (**0.10** seconds)

AXIS Video Server
[redacted] Frame.shtml?newstyle=Quad - 1k - Cached - Similar pages

AXIS Video Server
[redacted] Frame.shtml?newstyle=One&cam=1 - 1k - Cached - Similar pages

AXIS Video Server
[redacted] dexFrame. shtml?newstyle=One&cam=1 - 1k - Cached - Similar pages
[More results from webcam.gordon.edu]

AXIS 2130R PTZ Network Camera
[redacted] Frame.shtml - 1k - Cached - Similar pages

AXIS Video Server
[redacted] ffice.net/ indexFrame.shtml?newstyle=One&cam=1 - 1k - Cached - Similar pages

AXIS Video Server
[redacted] dexFrame.shtml - 1k - 30 Apr 2005 - Cached - Similar pages

AXIS Video Server
[redacted] exFrame.shtml - 1k - Cached - Similar pages

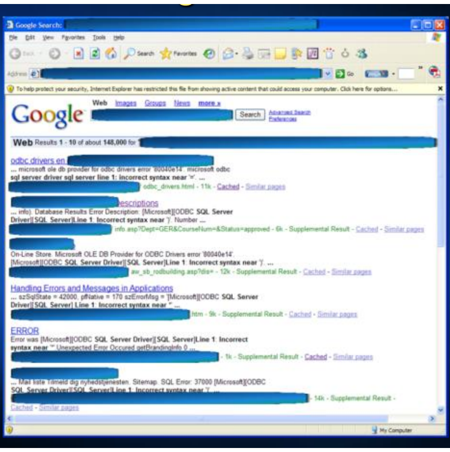
AXIS Video Server
[redacted] me.shtml?newstyle=Quad - 1k - Cached - Similar pages

AXIS Video Server
[redacted] rame.shtml?newstyle=Quad - 1k - Cached - Similar pages

AXIS Video Server
[redacted] Frame.shtml?newstyle=Quad - 1k - Cached - Similar pages

Goooooooooooogle
Result Page: **Previous** 1 2 3 4 5 6 7 8 9 10 11 **Next**

[redacted] Search


Google Search: [redacted]
File Edit View Favorites Tools Help
Back Search Favorites
Address [redacted]
Go
Web Images Groups News more »
Search
Advanced Search
Preferences
My Computer

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...

[redacted]

Web Results **1** - **10** of about **148,000** for [redacted]

odbc drivers en [redacted]
... microsoft ole db provider for odbc drivers error '80040e14'. microsoft odbc **sql server driver sql server line 1: incorrect syntax near** '='. ...
[redacted] odbc_drivers.html - 11k - Cached - Similar pages

[redacted] escriptions
... info). Database Results Error Description: [Microsoft][ODBC **SQL Server Driver][SQL Server]Line 1**: **Incorrect syntax near** ')'. Number ...
[redacted] info.asp?Dept=GER&CourseNum=&Status=approved - 6k - Supplemental Result - Cached - Similar pages

[redacted]
On-Line Store. Microsoft OLE DB Provider for ODBC Drivers error '80040e14'. [Microsoft][ODBC **SQL Server Driver][SQL Server]Line 1**: **Incorrect syntax near** ')'. ...
[redacted] aw_sb_rodbuilding.asp?dis= - 12k - Supplemental Result - Cached - Similar pages

Handling Errors and Messages in Applications
... szSqlState = 42000, pfNative = 170 szErrorMsg = '[Microsoft][ODBC **SQL Server Driver][SQL Server] Line 1**: **Incorrect syntax near** ''. ...
[redacted] .htm - 9k - Supplemental Result - Cached - Similar pages

ERROR
Error was [Microsoft][ODBC **SQL Server Driver][SQL Server]Line 1**: **Incorrect syntax near** ''' Unexpected Error Occured getBrandingInfo 0 ...
[redacted] - 1k - Supplemental Result - Cached - Similar pages

[redacted]
... Mail liste Tilmeld dig nyhedstjenesten. Sitemap. SQL Error: 37000 [Microsoft][ODBC **SQL Server Driver][SQL Server]Line 1**: **Incorrect syntax near** ')'. ...
[redacted] - 14k - Supplemental Result - Cached - Similar pages

Excuse:
We‘ve never been attacked

Excuse:
We‘re secure – we use cryptography

---

demo

Random Numbers

---

demo

Encryption

Hide & Seek Stored Keys

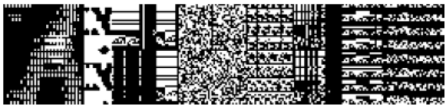


Figure 1 Key information (in the middle of the figure) looks more noisy than the rest of the data

---

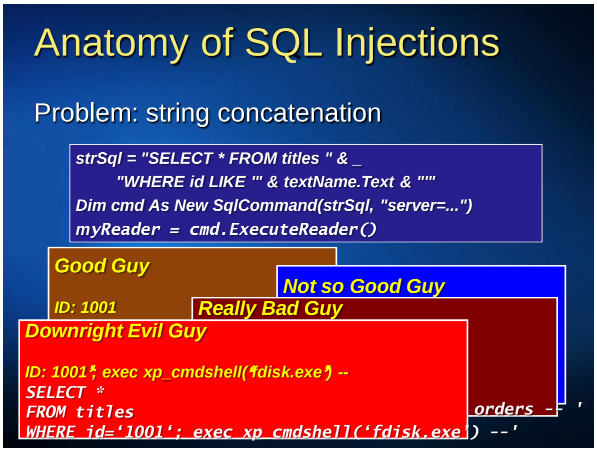
Excuse:
We‘re secure – we use ACLs

Excuse:
We‘re secure – we use a firewall

---

demo

SQL Injection



Anatomy of SQL Injections

Problem: string concatenation

```
strSql = "SELECT * FROM titles " & _
      "WHERE id LIKE '" & textName.Text & "'"
Dim cmd As New SqlCommand(strSql, "server=...")
myReader = cmd.ExecuteReader()
```

Good Guy

ID: 1001

Not so Good Guy

Really Bad Guy

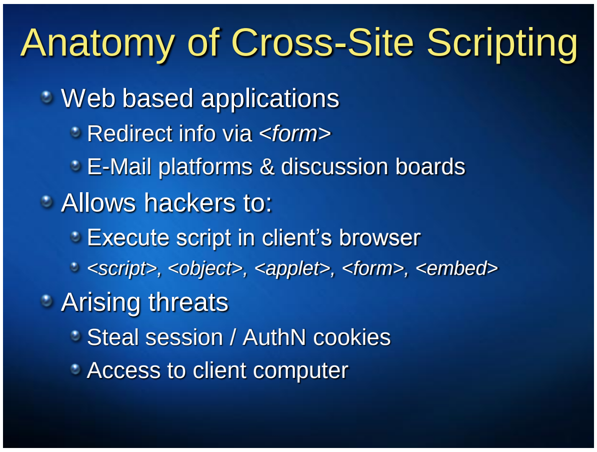
```
orders -- '
```

Downright Evil Guy

```
ID: 1001'; exec xp_cmdshell('fdisk.exe') --
SELECT *
FROM titles
WHERE id='1001'; exec xp_cmdshell('fdisk.exe') --'
```

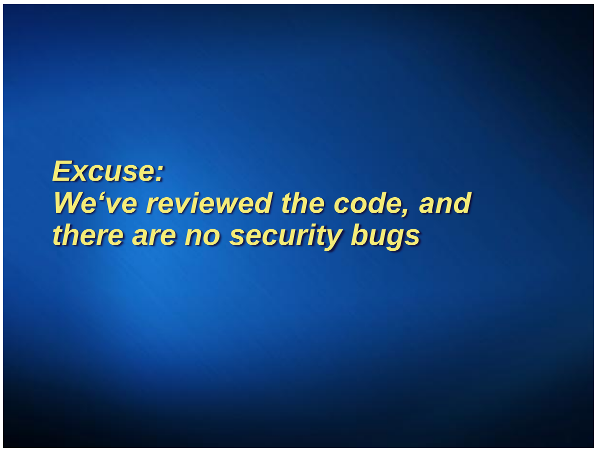
demo

Cross-Site Scripting



Anatomy of Cross-Site Scripting

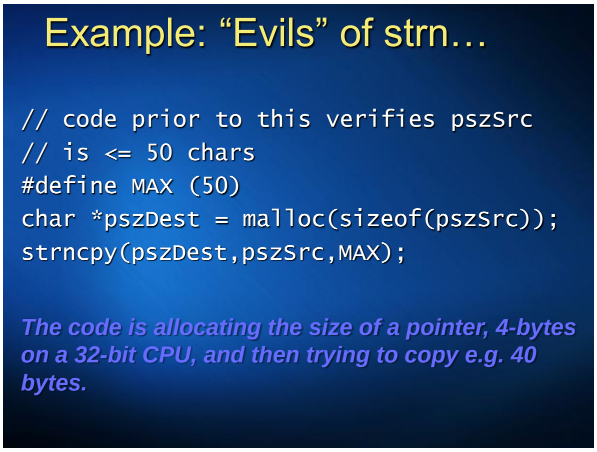
- Web based applications
  - Redirect info via <*form*>
  - E-Mail platforms & discussion boards
- Allows hackers to:
  - Execute script in client's browser
  - *<script>, <object>, <applet>, <form>, <embed>*
- Arising threats
  - Steal session / AuthN cookies
  - Access to client computer



Excuse:
We've reviewed the code, and there are no security bugs

demo

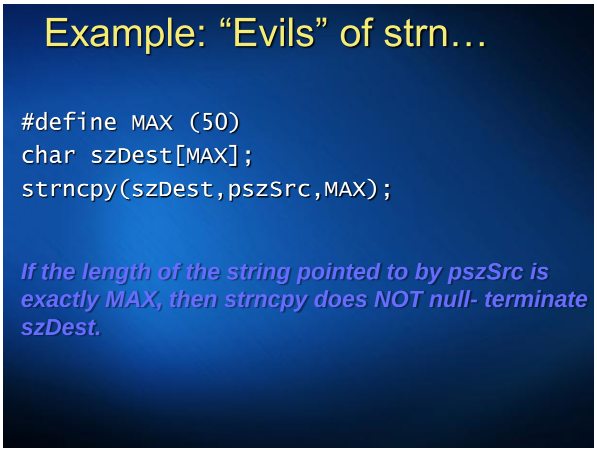
EBay



Example: “Evils” of strn…

```
// code prior to this verifies pszSrc
// is <= 50 chars
#define MAX (50)
char *pszDest = malloc(sizeof(pszSrc));
strncpy(pszDest,pszSrc,MAX);
```

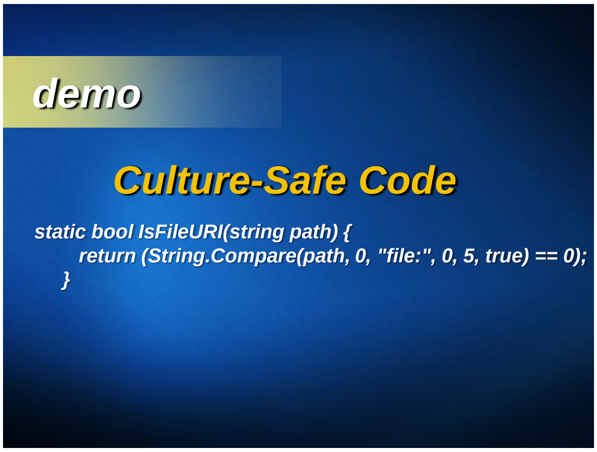
The code is allocating the size of a pointer, 4-bytes on a 32-bit CPU, and then trying to copy e.g. 40 bytes.



Example: “Evils” of strn…

```
#define MAX (50)
char szDest[MAX];
strncpy(szDest,pszSrc,MAX);
```

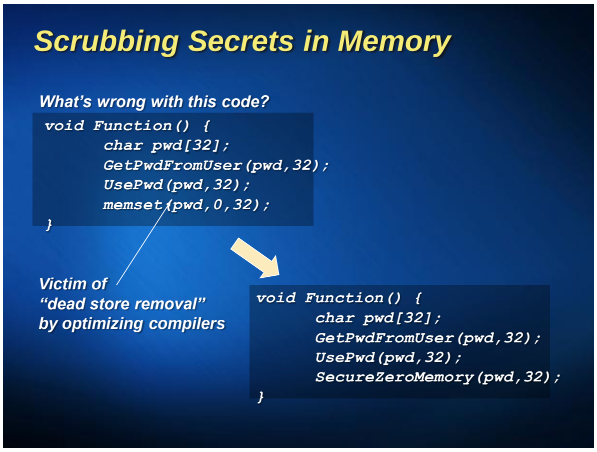
If the length of the string pointed to by pszSrc is exactly MAX, then strncpy does NOT null- terminate szDest.



demo

Culture-Safe Code

```
static bool IsFileURI(string path) {
      return (String.Compare(path, 0, "file:", 0, 5, true) == 0);
   }
```



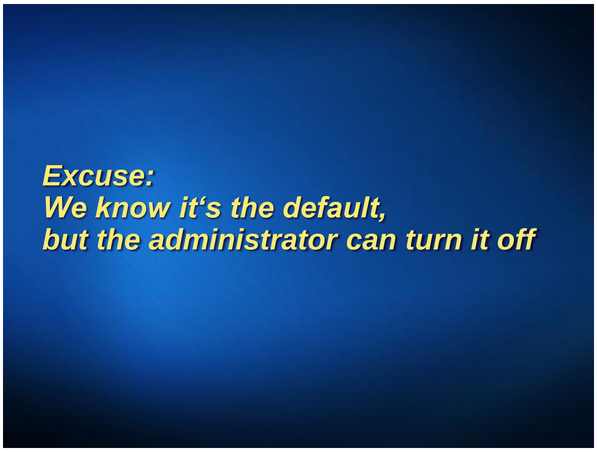
Scrubbing Secrets in Memory

What's wrong with this code?

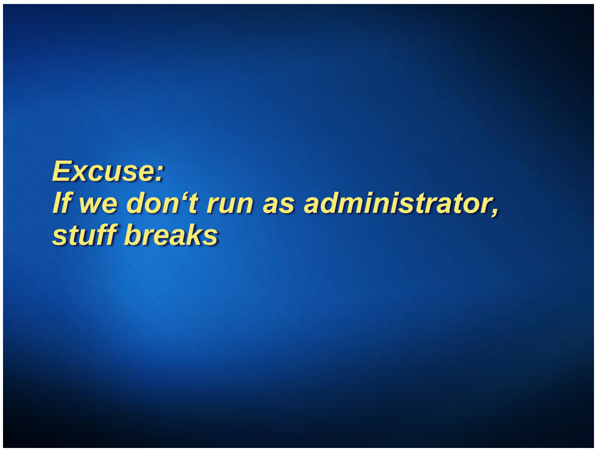
```
void Function() {
        char pwd[32];
        GetPwdFromUser(pwd,32);
        UsePwd(pwd,32);
        memset(pwd,0,32);
}
```

Victim of
"dead store removal"
by optimizing compilers

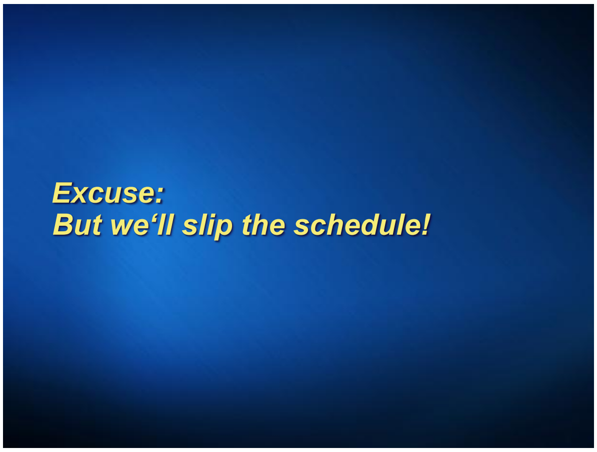
```
void Function() {
        char pwd[32];
        GetPwdFromUser(pwd,32);
        UsePwd(pwd,32);
        SecureZeroMemory(pwd,32);
}
```



Excuse:
We know it's the default,
but the administrator can turn it off



Excuse:
If we don't run as administrator,
stuff breaks

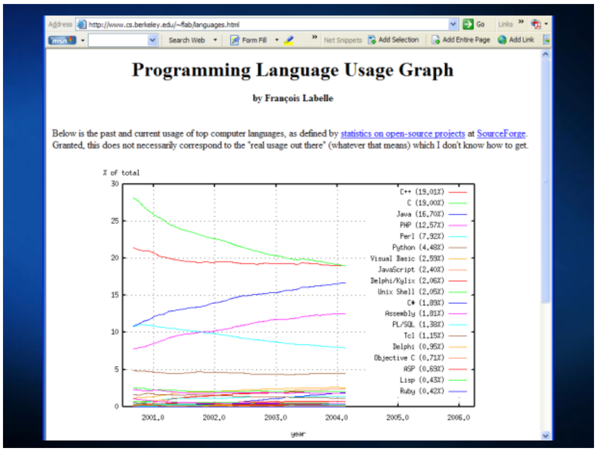


Excuse:
But we'll slip the schedule!

Excuse:
It‘s not exploitable!

Excuse:
But that‘s the way we‘ve always done it

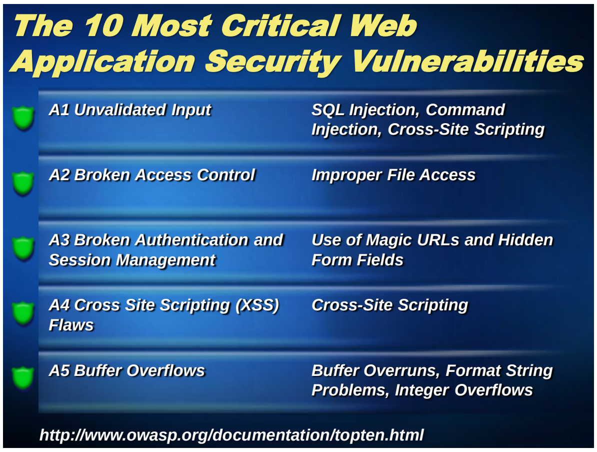
Excuse:
If only we had better tools …



Programming Language Usage Graph

by François Labelle

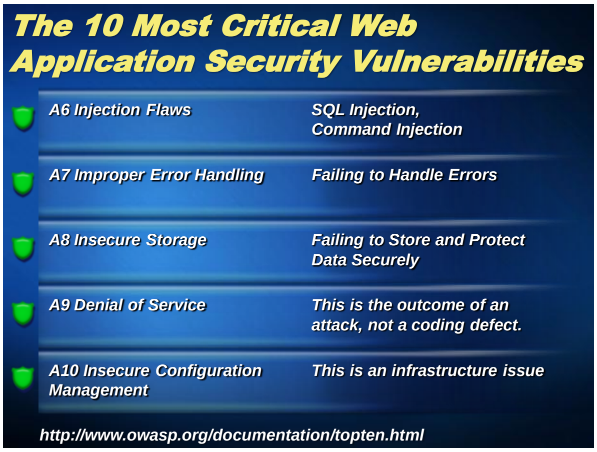
Below is the past and current usage of top computer languages, as defined by statistics on open-source projects at SourceForge. Granted, this does not necessarily correspond to the "real usage out there" (whatever that means) which I don't know how to get.



The 10 Most Critical Web Application Security Vulnerabilities

A1 Unvalidated Input	SQL Injection, Command Injection, Cross-Site Scripting
A2 Broken Access Control	Improper File Access
A3 Broken Authentication and Session Management	Use of Magic URLs and Hidden Form Fields
A4 Cross Site Scripting (XSS) Flaws	Cross-Site Scripting
A5 Buffer Overflows	Buffer Overruns, Format String Problems, Integer Overflows

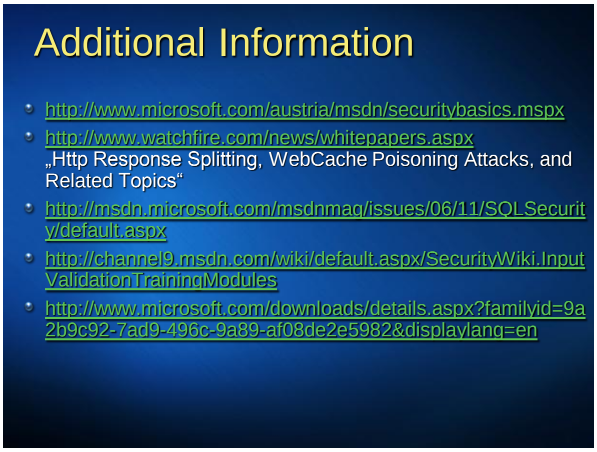
http://www.owasp.org/documentation/topten.html



The 10 Most Critical Web Application Security Vulnerabilities

A6 Injection Flaws	SQL Injection, Command Injection
A7 Improper Error Handling	Failing to Handle Errors
A8 Insecure Storage	Failing to Store and Protect Data Securely
A9 Denial of Service	This is the outcome of an attack, not a coding defect.
A10 Insecure Configuration Management	This is an infrastructure issue

http://www.owasp.org/documentation/topten.html

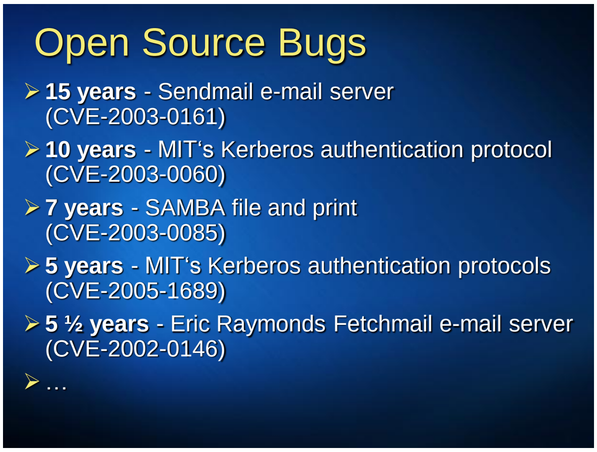


Additional Information

- http://www.microsoft.com/austria/msdn/securitybasics.mspx
- http://www.watchfire.com/news/whitepapers.aspx
  „Http Response Splitting, WebCache Poisoning Attacks, and Related Topics“
- http://msdn.microsoft.com/msdnmag/issues/06/11/SQLSecurity/default.aspx
- http://channel9.msdn.com/wiki/default.aspx/SecurityWiki.InputValidationTrainingModules
- http://www.microsoft.com/downloads/details.aspx?familyid=9a2b9c92-7ad9-496c-9a89-af08de2e5982&displaylang=en

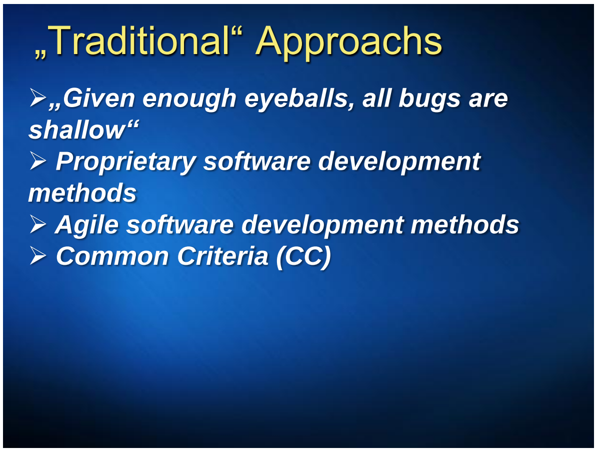
„Traditional“ Approaches

- ***„Given enough eyeballs, all bugs are shallow“***



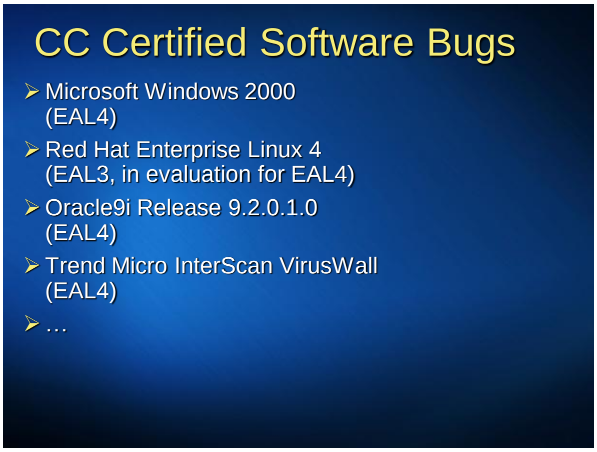
Open Source Bugs

- **15 years** - Sendmail e-mail server (CVE-2003-0161)
- **10 years** - MIT's Kerberos authentication protocol (CVE-2003-0060)
- **7 years** - SAMBA file and print (CVE-2003-0085)
- **5 years** - MIT's Kerberos authentication protocols (CVE-2005-1689)
- **5 ½ years** - Eric Raymonds Fetchmail e-mail server (CVE-2002-0146)
- …



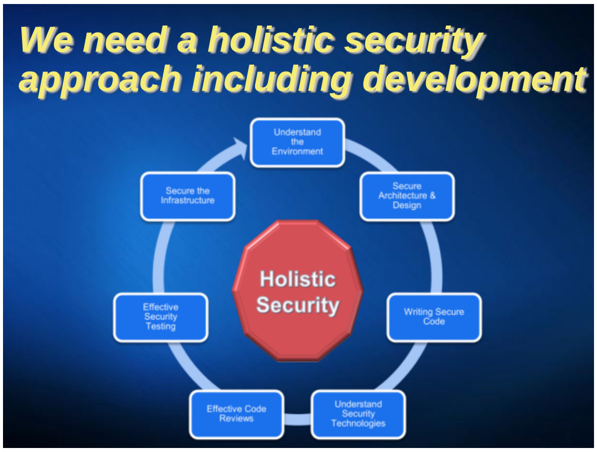
„Traditional" Approachs

- ***„Given enough eyeballs, all bugs are shallow"***
- ***Proprietary software development methods***
- ***Agile software development methods***
- ***Common Criteria (CC)***



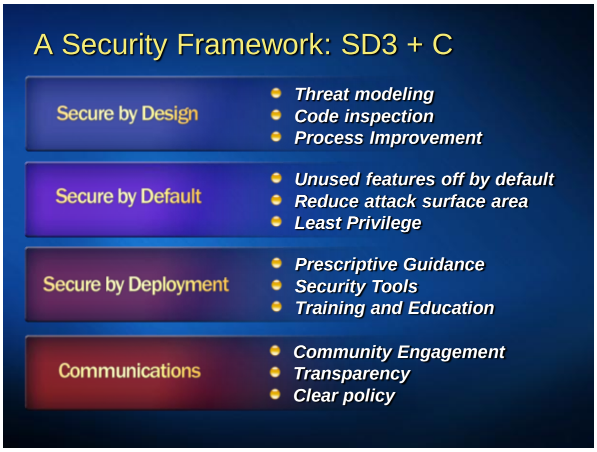
CC Certified Software Bugs

- Microsoft Windows 2000 (EAL4)
- Red Hat Enterprise Linux 4 (EAL3, in evaluation for EAL4)
- Oracle9i Release 9.2.0.1.0 (EAL4)
- Trend Micro InterScan VirusWall (EAL4)
- …



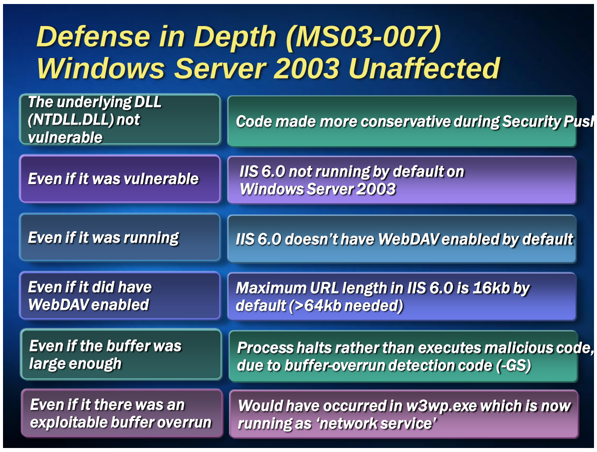
We need a holistic security approach including development

Understand the Environment
Secure Architecture & Design
Writing Secure Code
Understand Security Technologies
Effective Code Reviews
Effective Security Testing
Secure the Infrastructure
Holistic Security



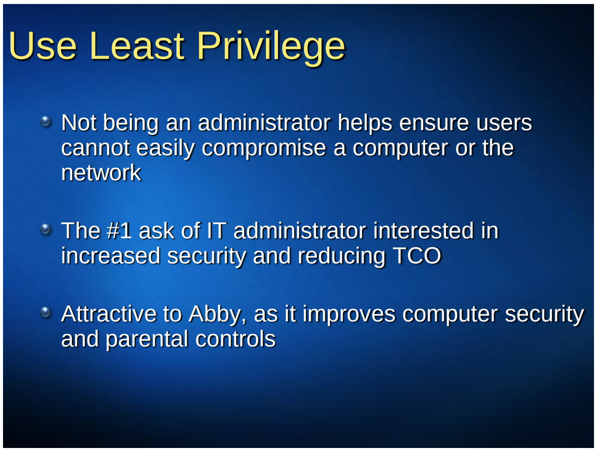
A Security Framework: SD3 + C

Secure by Design	*Threat modeling* *Code inspection* *Process Improvement*
Secure by Default	*Unused features off by default* *Reduce attack surface area* *Least Privilege*
Secure by Deployment	*Prescriptive Guidance* *Security Tools* *Training and Education*
Communications	*Community Engagement* *Transparency* *Clear policy*



Defense in Depth (MS03-007) Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable	*Code made more conservative during Security Push*
Even if it was vulnerable	*IIS 6.0 not running by default on Windows Server 2003*
Even if it was running	*IIS 6.0 doesn't have WebDAV enabled by default*
Even if it did have WebDAV enabled	*Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)*
Even if the buffer was large enough	*Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)*
Even if it there was an exploitable buffer overrun	*Would have occurred in w3wp.exe which is now running as 'network service'*



Use Least Privilege

- Not being an administrator helps ensure users cannot easily compromise a computer or the network
- The #1 ask of IT administrator interested in increased security and reducing TCO
- Attractive to Abby, as it improves computer security and parental controls

Minimize Your Attack Surface!

Secure Defaults

- Less code running by default = less stuff to attack by default
- Slammer & CodeRed would not have happened if the features were not enabled by default
- Reduces the urgency to deploy security fixes
  - A ‘critical’ may be rated ‘important’
- Defense in depth removes single points of failure
- Reduces the need for customers to ‘harden’ the product
- Reduces <u>your</u> testing workload
- Reduce your attack surface <u>early</u>!

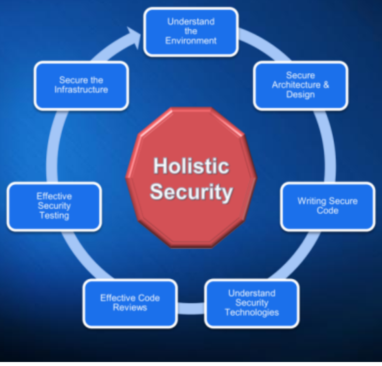
Assignment – Sample 1

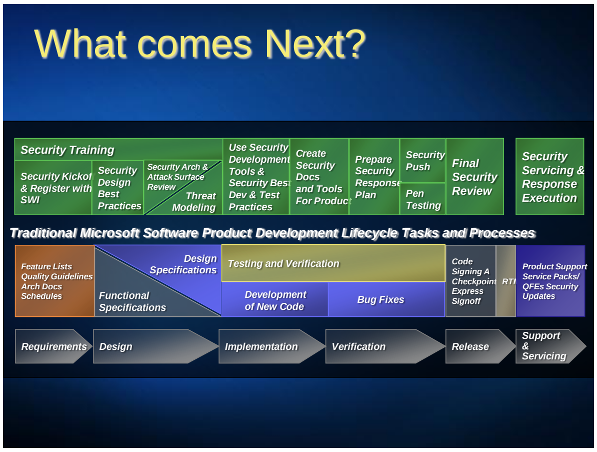
```
#include <iostream>
void SomeFunction(){
		int someLocalVar = 17;
		int someOtherLocalVar = 33;
}

void SomeOtherFunction(){
		int someLocalVar;
		int someOtherLocalVar;

		std::cout << "someLocalVar: " << someLocalVar << 
std::endl;
		std::cout << "someOtherLocalVar: " << 
someOtherLocalVar << std::endl;
}

void main(void){
		SomeFunction();
		SomeOtherFunction();
```

Assignment – Sample 2

```
#include <iostream>

void foo(){
    …
}

void main(void){
    int i = 0;

    foo();
    i++;
    std::cout << "i = " << i << std::endl;
}
```

Summary of Today


Understand the Environment
Secure Architecture & Design
Writing Secure Code
Understand Security Technologies
Effective Code Reviews
Effective Security Testing
Secure the Infrastructure
Holistic Security



What comes Next?

Security Training

Security Kickoff & Register with SWI

Security Design Best Practices

Security Arch & Attack Surface Review

Threat Modeling

Use Security Development Tools & Security Best Dev & Test Practices

Create Security Docs and Tools For Product

Prepare Security Response Plan

Security Push

Pen Testing

Final Security Review

Security Servicing & Response Execution

Traditional Microsoft Software Product Development Lifecycle Tasks and Processes

Feature Lists
Quality Guidelines
Arch Docs
Schedules

Design Specifications

Functional Specifications

Testing and Verification

Development of New Code

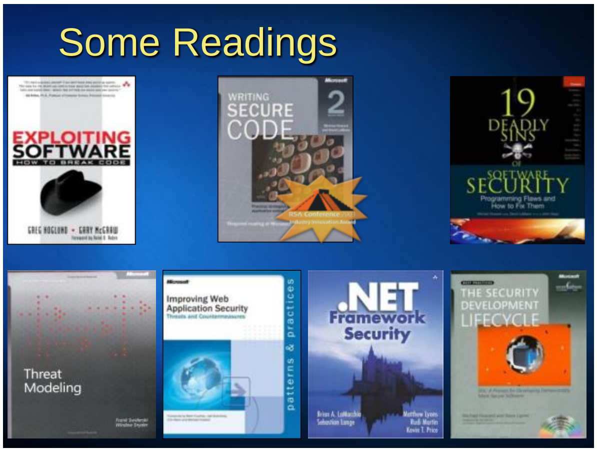
Bug Fixes

Code Signing A Checkpoint Express Signoff

RTM

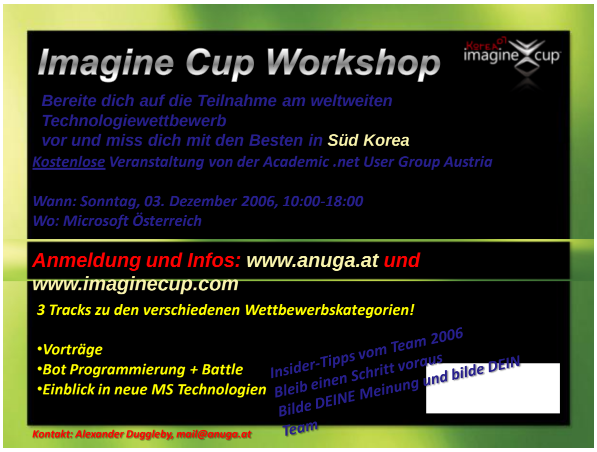
Product Support
Service Packs/
QFEs Security
Updates

Requirements → Design → Implementation → Verification → Release → Support & Servicing



Some Readings

EXPLOITING SOFTWARE
HOW TO BREAK CODE
GREG HOGLUND • GARY McGRAW
WRITING SECURE CODE 2
19 DEADLY SINS OF SOFTWARE SECURITY
Programming Flaws and How to Fix Them
Threat Modeling
Improving Web Application Security
Threats and Countermeasures
patterns & practices
.NET Framework Security
THE SECURITY DEVELOPMENT LIFECYCLE



Imagine Cup Workshop

Korea 07 imagine cup

Bereite dich auf die Teilnahme am weltweiten Technologiewettbewerb
vor und miss dich mit den Besten in Süd Korea

Kostenlose Veranstaltung von der Academic .net User Group Austria

Wann: Sonntag, 03. Dezember 2006, 10:00-18:00
Wo: Microsoft Österreich

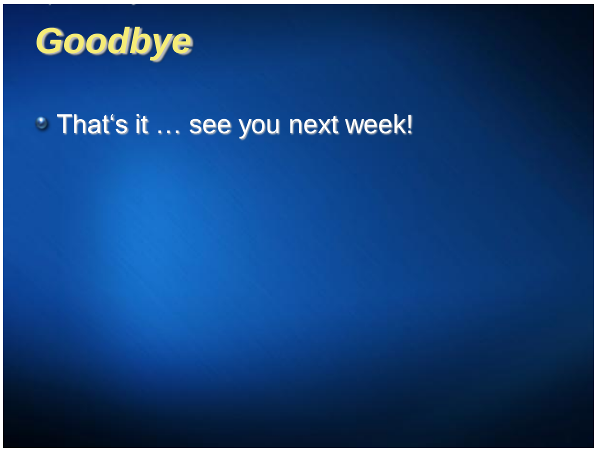
Anmeldung und Infos: www.anuga.at und www.imaginecup.com

3 Tracks zu den verschiedenen Wettbewerbskategorien!

- Vorträge
- Bot Programmierung + Battle
- Einblick in neue MS Technologien

Insider-Tipps vom Team 2006
Bleib einen Schritt voraus
Bilde DEINE Meinung und bilde DEIN Team

Kontakt: Alexander Duggleby, mail@anuga.at



Goodbye

- That‘s it … see you next week!