

Bezpieczeństwo heterogenicznej platformy hostingowej

GERARD FRANKOWSKI, MARCIN JERZAK

Zespół Bezpieczeństwa PCSS / Centrum Innowacji Microsoft



Agenda



- Poznajmy się: PCSS i MIC
- Dlaczego heterogeniczny hosting?
- Zabezpieczenie systemu i serwera
- IIS i PHP w jednym stali domu...
- Bezpieczeństwo baz danych
- Interpreter języka stron

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

PCSS



- Operator Polskiego Internetu Optycznego (PIONIER)
- Operator sieci POZMAN
- Centrum przetwarzania danych (HPC/HTC) oraz zaawansowanego hostingu
- Bezpieczeństwo sieci i systemów
- Centrum badawcze dla sieci, portali, gridów nowej generacji
- Centrum Innowacji Microsoft (MIC)



Zespół Bezpieczeństwa PCSS



- Ukonstytuowany zespół działa od 1996 r.
 - Zabezpieczanie infrastruktury PCSS
 - Zadania bezpieczeństwa w projektach R&D
 - Szkolenia, transfer wiedzy
 - Badania własne
 - Usługi zewnętrzne
- Wybrane badania z ostatnich lat:
 - Bezpieczeństwo bankowości elektronicznej
 - Bezpieczeństwo serwerów WWW (Apache, MS IIS)
 - Bezpieczeństwo sklepów internetowych

Centrum Innowacji Microsoft



- Pierwsze w Polsce
 - Otwarcie: 1.06.2006
 - Microsoft Polska, PCSS, Politechnika Poznańska
- Główne zadania w 2009:
 - Wirtualizacja (zapraszamy na sesję MIC o 13:10!)
 - Zaawansowany hosting
 - HPC
 - Interoperacyjność rozwiązań i technologii
 - Bezpieczeństwo
 - Szkolenia

Więcej informacji

- PCSS
 - WWW: <http://www.pcss.pl>
- Zespół Bezpieczeństwa PCSS
 - WWW: <http://security.psnc.pl>
- Centrum Innowacji Microsoft w Poznaniu
 - WWW: <http://mic.psnc.pl>
 - Szkolenia: <http://mic.psnc.pl/szkolenia>

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

Dlaczego?



- Interoperacyjność rozwiązań i technologii
 - Zmniejszenie kosztów adaptacji rozwiązań
 - Ludzie chcą mieć wybór (i wygodę)
- Jedynie słuszny zestaw?
 - Często tak, ale może nie zawsze...
- Przyzwyczajenie jest drugą naturą
 - Skoro znam dobrze PHP, to czy nie mogę skorzystać z niego na wszystkich systemach?
- Eksperymenty źródłem wiedzy

Dla kogo?

- Dzisiejsza prezentacja ma na celu przedstawienie możliwości budowy mieszanego środowiska hostingowego ze zwróceniem uwagi na bezpieczeństwo IT
- Sesja jest przeznaczona głównie dla:
 - Administratorów serwerów WWW oraz twórców aplikacji webowych w PHP
 - Specjalistów bezpieczeństwa IT

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

Zabezpieczanie systemu i serwera

- **Zagrożenia**
- System operacyjny
- Serwer IIS
- IIS + PHP
- Wersje PHP
- URLScan

Zagrozenia



Źródło: <http://jkontherun.files.wordpress.com/2009/01/hacker.jpg>

Zagrozenia (2)

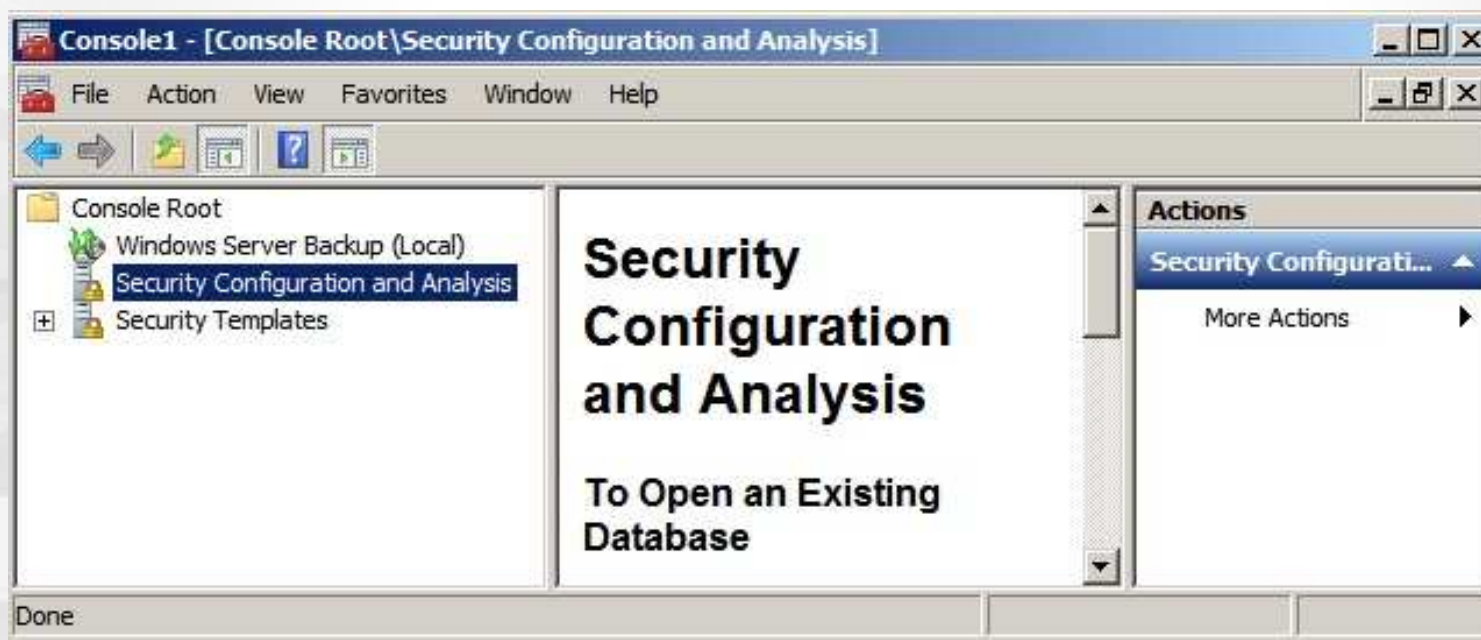
- **SMB, Remote Code Execution**
([CVE-2009-3103](#))
- **TCP/IP Packet State, Remote Code Execution**
([CVE-2009-1925](#))
- **ATL Components, Remote Code Execution**
([CVE-2009-0901](#))
- **IE JavaScript, Denial Of Service**
([CVE-2009-3019](#))
- **IIS FTP Service, Denial Of Service**
([CVE-2009-2521](#))

Zabezpieczanie systemu i serwera

- Zagrożenia
- **System operacyjny**
- Serwer IIS
- IIS + PHP
- Wersje PHP
- URLScan

System operacyjny

- Utwardzanie konfiguracji
 - Szablony zabezpieczeń
 - Security Compliance Management Toolkit



```
Secedit /configure /db baza.sdb /cfg "szablon.inf" /overwrite
```

System operacyjny (2)

- Minimalizacja powierzchni ataku
 - Kreator konfiguracji zabezpieczeń
 - Windows Server Core
- Firewall (!)
- Windows Server Backup
- Ochrona antywirusowa
- IDS/IPS

System operacyjny (3)

- Aktualizacja oprogramowania
 - Microsoft Baseline Security Analyzer
- Okresowe audyty bezpieczeństwa
- Strategia *Defense in depth*
- Świadomość zagrożenia
- Wykorzystanie wbudowanych w system mechanizmów zabezpieczających pamięć

System operacyjny (4)

2002 – opcja kompilatora GS

2003 – opcja kompilatora SafeSEH

2004 – DEP

2006 – ASLR

System operacyjny (5)

- **DisableExceptionChainValidation = 0**
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\
- **Movelimages**
 - 0 – nigdy
 - - 1 – zawsze
 - 1 – tylko dla niektórych obrazów
- HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management\
bcdedit.exe /set {current} **nx AlwaysOn**

System operacyjny (6)

- Start -> Uruchom -> **sysdm.cpl**
- Zaawansowane -> Wydajność -> Ustawienia -> Zapobieganie wykonywaniu danych

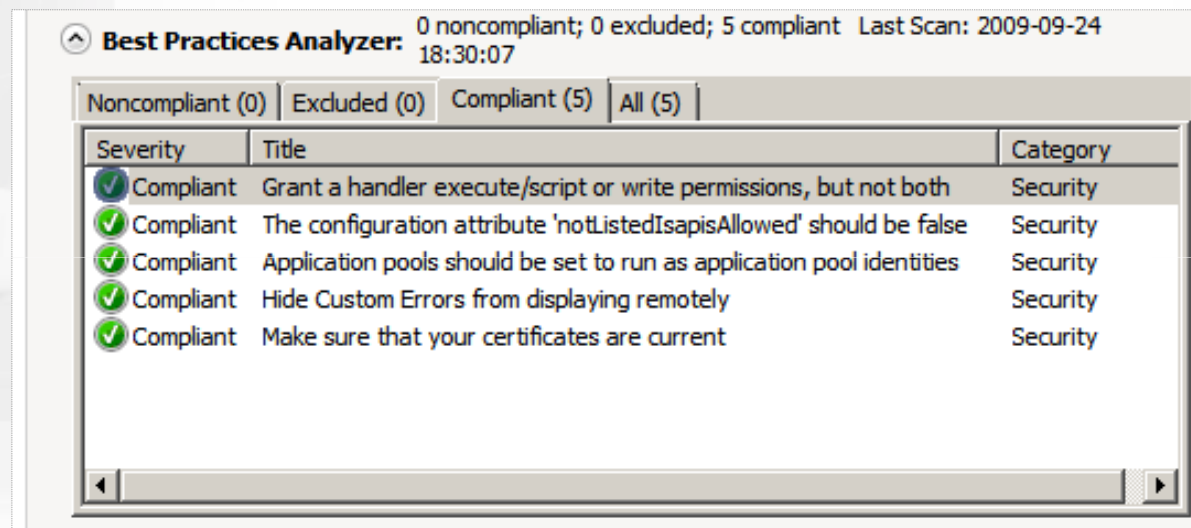


Zabezpieczanie systemu i serwera

- Zagrożenia
- System operacyjny
- **Serwer IIS**
- IIS + PHP
- Wersje PHP
- URLScan

Internet Information Services

- „Domyślnie bezpieczny”
- Dedykowany serwer
- Minimalna powierzchnia ataku
- Best Practices Analyzer (BPA) (v7.5)



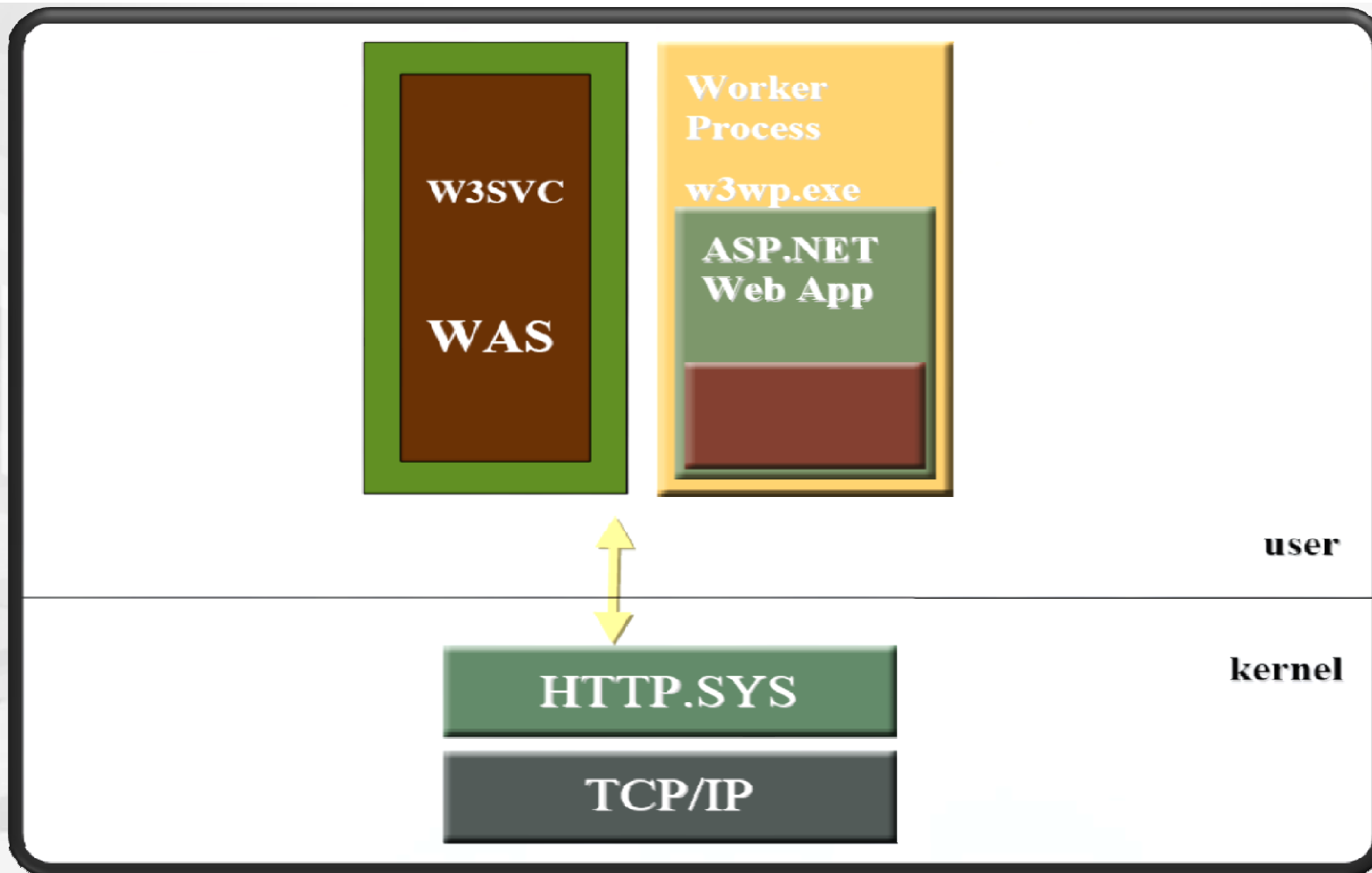
Severity	Title	Category
✓ Compliant	Grant a handler execute/script or write permissions, but not both	Security
✓ Compliant	The configuration attribute 'notListedIsapisAllowed' should be false	Security
✓ Compliant	Application pools should be set to run as application pool identities	Security
✓ Compliant	Hide Custom Errors from displaying remotely	Security
✓ Compliant	Make sure that your certificates are current	Security

- Typy MIME (Internet Media Type)

Internet Information Services (2)

- Windows Process Activation Service (WAS)
 - Pule aplikacji – izolacja
 - Limit CPU
 - Limit HD
- Kernel Mode Authentication
- Zabezpieczenia warstwy aplikacji
 - Wykorzystanie narzędzia SDL
 - Audyty kodów źródłowych
- Filtrowanie zapytań (URLScan)

Architektura serwera IIS



Zabezpieczanie systemu i serwera

- Zagrożenia
- System operacyjny
- Serwer IIS
- **IIS + PHP**
- Wersje PHP
- URLScan

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

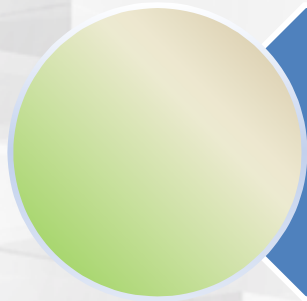
IIS + PHP



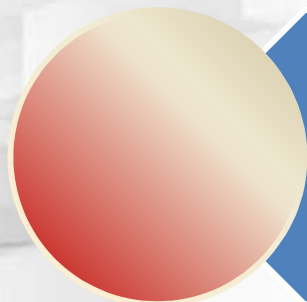
CGI



Sposób
domyślny



Zaleta:
Stabilność



Wada:
Wydajność

zapytanie o stronę
.php

uruchamiany jest
proces php-cgi.exe

proces php-cgi.exe
obsługuje zapytanie

proces php-cgi.exe
jest zamykany

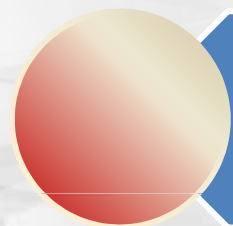
ISAPI



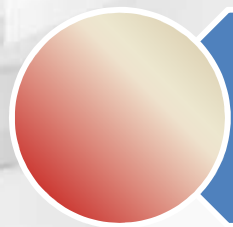
Moduł serwera IIS



Zaleta: Wydajność
(5x szybciej niż CGI)

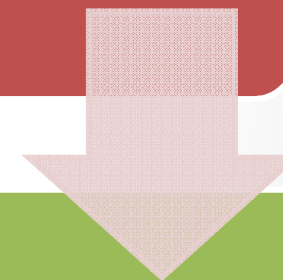


Wada: Stabilność



Wada:
Wielowątkowość*

zapytanie o
stronę .php

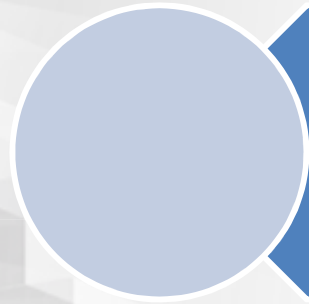


php5isapi.dll

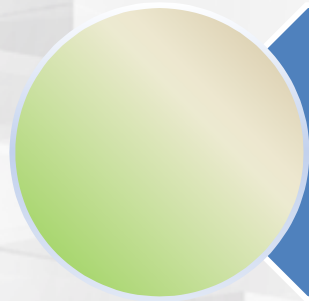
ISAPI - instalacja

- Instalacja PHP
- Konfiguracja w pliku php.ini
 - `cgi.force_redirect = 0`
 - `session.save_path`
 - `extension = php_mysql.dll*`
- Dodanie PHP do PATH
- Dodanie filtra ISAPI
 - Wtyczka `php5isapi.dll` – rozszerzenie `.php`

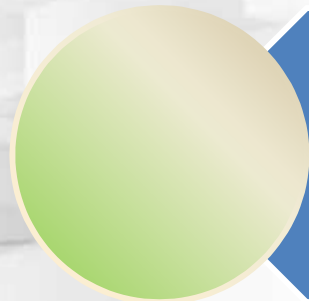
FastCGI



Bufor
wywołań
php-cgi



Zaleta:
Stabilność



Zaleta:
Wydajność

zapytanie o stronę
.php

IIS trzyma w
gotowości wiele
procesów
php-cgi.exe

Zapytanie kierowane
jest do wolnego
procesu php-cgi.exe

FastCGI (2)

- „Kompromis” pomiędzy CGI i ISAPI
- Implementacje Microsoft i Zend
- FastCGI komunikuje się przez TCP
 - Skalowalność
 - Load balancing
- Windows Cache Extension for PHP
 - `php.ini -> extension = php_wincache.dll`
 - PHP opcode cache
 - File cache
 - Relative file path cache

FastCGI - instalacja

- Wsparcie dla CGI
- Instalacja PHP
- Mapowanie modułu
 - FastCGIModule
- Ustawienia php.ini
 - Fastcgi.impersonate = 1
 - Cgi.fix_pathinfo = 1
 - Cgi.force_redirect = 0

Zabezpieczanie systemu i serwera

- Zagrożenia
- System operacyjny
- Serwer IIS
- IIS + PHP
- **Wersje PHP**
- URLScan

Różne wersje PHP

- PHP 5.3.0
 - Thread-safe
- PHP 5.2.11
 - Non-thread-safe
- PHP 6.0
 - Nie dla systemów produkcyjnych

Różne wersje PHP (2)

- Poszczególne pliki binarne PHP w różnych miejscach
- Osobna pula dla każdej z wersji
- Plik php.ini – parametr open_basedir

```
<fastCgi>
```

```
  <application fullPath="C:\PHP5\php-cgi.exe" arguments="-d  
  open_basedir=C:\WWW\Strona1" />
```

```
  <application fullPath="C:\PHP4\php-cgi.exe" arguments="-d  
  open_basedir=C:\WWW\Strona2" />
```

```
</fastCgi>
```

Zabezpieczanie systemu i serwera

- Zagrożenia
- System operacyjny
- Serwer IIS
- IIS + PHP
 - CGI
 - ISAPI
 - FastCGI
- Wersje PHP
- **URLScan**

URLScan

- URLScan jest filtrem ISAPI monitorującym i blokującym żądania HTTP
 - Ostatnia wersja: 3.1
 - Działa dla IIS 5.1, 6.0, 7.0
 - Integracja z IIS 7.5
- Zaawansowane możliwości filtrowania oraz logowania informacji
- Ochrona przed atakami typu:
 - SQL Injection
 - Cross Site Scripting

Czy potrzebujemy URLScan-a?

- Spora część funkcjonalności narzędzia może być osiągnięta w samym IIS, ale
 - URLScan jest bardziej elastyczny
 - Działa na wcześniejszym etapie przetwarzania żądania, szybciej odrzucając groźne pakiety
 - Dywersyfikuje ryzyko popełnienia błędu
 - Jego zastosowanie lepiej realizuje strategię *Defense in depth*
 - Po przejściu na IIS 7.5 dylemat zniknie ;)

Wybrane opcje

- UseAllowVerbs
 - „Biała” lub „czarna lista”
dozwolonych/zabronionych metod HTTP
 - Wartość domyślna = 1 (dopuszczanie żądań wymienionych w sekcji [AllowVerbs], 0 powoduje odrzucanie żądań z sekcji [Deny Verbs])
- UseAllowExtensions
 - Działa na identycznej zasadzie, jak powyżej, ale odnosi się do rozszerzeń żądanych plików

Wybrane opcje (2)

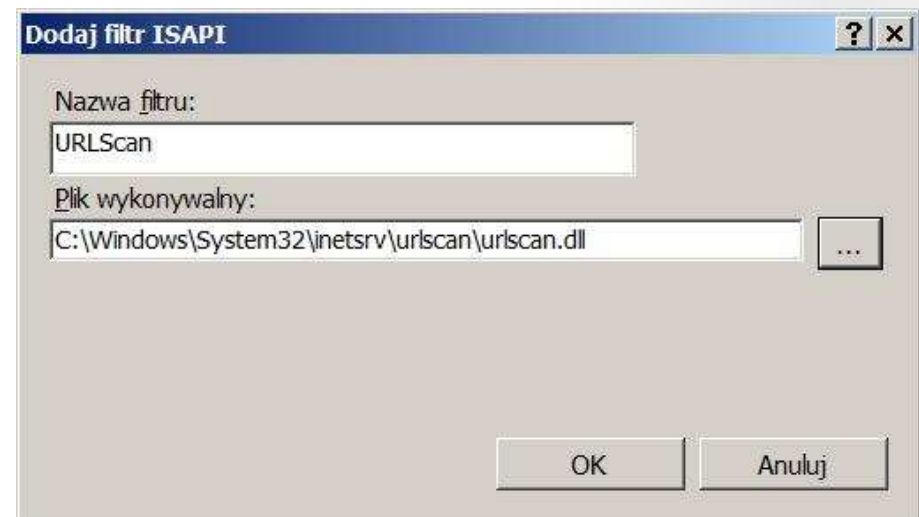
- **NormalizeUrlBeforeScan**
 - Wartość domyślna = 1 – powoduje, że przekazany adres URL jest poddawany odkodowaniu
 - Wartość 0 powoduje, że łatwo ominąć testy rozszerzeń lub URL!
- **VerifyNormalization**
 - Wartość domyślna = 1 – przekazany adres URL jest odkodowany po raz drugi, jeśli wystąpią różnice, żądanie jest odrzucane
 - Wykrywa podwójne kodowanie złośliwych znaków, np. & -> %26 -> %2526

Wybrane opcje (3)

- AllowDotInPath
 - Możliwe wartości: 0/1
 - 0 = żądania plików o ścieżce zawierającej wielokrotne wystąpienie znaku „..” zostaną odrzucone
 - 1 = test nie jest przeprowadzany
- Limity nakładane na żądanie
 - Sekcja [RequestLimits]
 - Długość żądania, długość URL, długość *query string*, ...

Konfiguracja IIS 7.0 dla URLScan-a

- Po instalacji URLScan-a należy poinformować serwer IIS o jego obecności
 - Dodanie filtru ISAPI dla serwera lub witryny
 - Menedżer IIS -> Widok funkcji -> IIS -> Filtry ISAPI -> Akcje -> Dodaj
 - Restart serwera IIS



Własne reguły URLScan-a

```
RuleList=testowa

[testowa]
AppliesTo=.html
DenyDataSection=denied_strings
ScanUrl=1
ScanQueryString=1

[denied_strings]
--
```

- Edycja własnych sekcji pliku konfiguracyjnego
- Zadanie: odrzucić żądania, w których nazwa pliku bądź parametr zapytania zawierają dwa myślniki (--)

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

My czy MS SQL ?

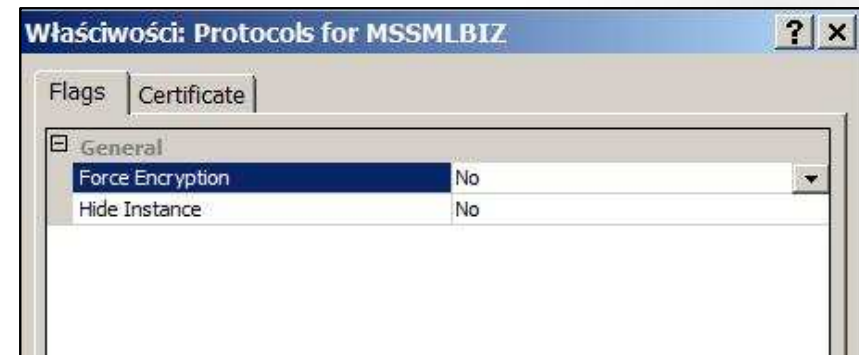
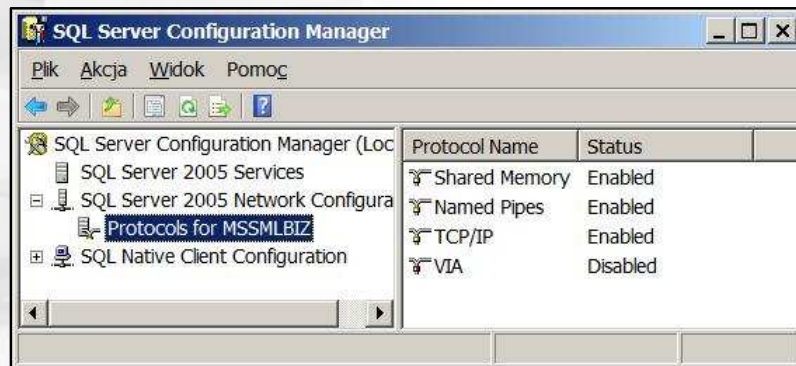
- Kryteria wyboru
 - Wydajność
 - Skalowalność
 - Prostota użytkowania
 - Łatwość migracji
 - Bezpieczeństwo
 - Wykonywanie poleceń systemowych
 - *Multiple statements*
 - Dostęp do plików

PHP i MS SQL

- Możliwe trudności z połączeniem technologii – na co zwrócić uwagę?
 - Uaktywnienie w php.ini rozszerzenia MS SQL
 - `[usunięcie];extension=php_mssql.dll`
 - Odpowiednia wersja biblioteki ntwdblib.dll
 - 2000.80.194.0, nie 2000.2.8.0
 - Mixed authentication mode dla SQL Servera
 - HKLM\Software\Microsoft\Microsoft SQL Server\MSSQL.1\MSSQLServer>LoginMode = 2
 - Umożliwienie logowania się na określone konto
 - ALTER LOGIN sa ENABLE
 - ALTER LOGIN sa WITH PASSWORD <strong_pass>

PHP i MS SQL (2)

- Możliwe trudności - kontynuacja
 - SQL Server Configuration Manager
 - Uaktywnienie odpowiednich protokołów dla SQL Servera
 - Wyłączenie szyfrowania (do testów)



- Lokalny firewall
- Sprawdzenie plików logu SQL Servera
 - [Install_dir]\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\ERRORLOG

Remote Code Execution

- Krótkie przypomnienie
 - Nie chodzi tu o eksploatację innych podatności, dającą w rezultacie dostęp do powłoki
 - Mamy na myśli nadużycie istniejącej funkcjonalności odwołującej się do poleceń systemu operacyjnego
 - Zagrożenia – napastnik działa w systemie z uprawnieniami serwera baz danych
 - Wyciek (bardzo wielu) informacji – podstawa do dalszych ataków
 - Zniszczenie lub modyfikacja bazy danych
 - DoS na serwer bazy danych i/lub system

RCE w MySQL

- Brak bezpośredniego wsparcia dla uruchomienia polecenia systemowego
 - Istnieje jedynie możliwość wykonania komendy z narzędzia linii komend
 - > system <command>
 - Działa tylko w systemach uniksowych

RCE w MS SQL

- Procedura składowana xp_cmdshell
 - Domyślnie wyłączona (duży plus!)
 - Wymaga uprawnień CONTROL SERVER
- Uaktywnienie poprzez:
 - Surface Area Configuration
 - Klienta linii poleceń
 - EXEC sp_configure 'show advanced options', 1
 - EXEC sp_configure 'xp_cmdshell', 1
 - Powinniśmy uaktywnić tylko jeśli jest to absolutnie niezbędne!

RCE w MS SQL (2)



RCE w MS SQL (3)

- Jeżeli niezbędne jest udzielenie prawa wykonania pojedynczemu użytkownikowi
 - Nie poprzez GRANT CONTROL SERVER
 - Lepiej:
 - EXEC sp_grantdbaccess *user*
 - GRANT exec ON xp_cmdshell TO *user*
- Podsumowując
 - Istnieją możliwości wykonania ataku, ale skonfigurowanie serwera zgodnie z zasadą minimalnych przywilejów radykalnie je zmniejsza

SQL Injection – przypomnienie

- Możliwość wpłynięcia na treść zapytania kierowanego do bazy danych
 - Np. Nazwisko = *Kowalski'*; *DROP TABLE users--*
 - Powód: nieodpowiednia konstrukcja zapytań oraz niewystarczająca (lub brak) filtracja danych
- Zagrożenia
 - Nieautoryzowany dostęp do danych
 - Modyfikacja lub zniszczenie danych
 - Ataki DoS
 - Wykonanie poleceń systemowych

Multiple statements

- Możliwość podania kolejnego zapytania po znaku specjalnym (zwykle „;”)
 - Umożliwia wykonanie dowolnego polecenia, do którego użytkownik bazy danych ma uprawnienia
 - Np. `SELECT * FROM users WHERE user='test';
INSERT INTO users (user, pass) VALUES ('hacker',
")--`
- Jak ten mechanizm obsługiwany jest w MySQL oraz MS SQL?

Multiple statements w MySQL

- Domyślnie mechanizm NIE JEST wspierany
 - Bardzo dobre założenie!
- Włączenie obsługi:
 - Dodatkowy parametr `mysql_connect()`
`$dbConn = mysql_connect("db", "user", "pass", FALSE, 65536); //CLIENT_MULTIPLE_STATEMENTS`
 - Uwaga! Z poziomu PHP otrzymamy wynik tylko pierwszego zapytania!
- Z punktu widzenia bezpieczeństwa nie powinniśmy używać tej opcji

Multiple statements w MS SQL

- MS SQL umożliwia domyślnie wykonanie *multiple statements*
 - Brak mechanizmu zabraniającego takiego zachowania
 - Podobnie, jak w przypadku MySQL otrzymamy wynik tylko pierwszego zapytania
 - Jediną formą obrony jest filtrowanie danych i odpowiednia konstrukcja zapytań
 - QUOTENAME

Dostęp do plików w MySQL

- Niebezpieczne możliwości
 - `SELECT LOAD_DATA("c:/boot.ini")`
 - `LOAD DATA INFILE ("c:/boot.ini") INTO table...`
- Warunki powodzenia `LOAD_DATA`
 - Plik na tej samej maszynie, co serwer MySQL
 - Należy podać pełną ścieżkę do pliku
 - Prawa do odczytu dla pliku i ścieżki
 - Uprawnienie `FILE` dla użytkownika bazy danych
 - Wielkość pliku mniejsza od *max_allowed_packets*
 - Uwzględnia parametr *secure_file_priv*

Dostęp do plików w MySQL (2)

- Błędy w konfiguracji powodują zagrożenie wyciekami informacji nawet przy braku *multiple statements*
 - `SELECT id, name FROM user where id = 2 UNION SELECT 1, LOAD_FILE("c:/boot.ini");`
 - Drugi SELECT musi cechować się identyczną liczbą i rodzajem kolumn (można je wykryć metodą prób i błędów)
 - `LOAD_FILE` nie zwróci tutaj więcej znaków niż szerokość odpowiadającej mu kolumny *name* (np. 30) – należy zastosować wymaganą liczbę razy funkcję `SUBSTRING`:
`SELECT id, name FROM user where id = 2 UNION SELECT 1, SUBSTRING(LOAD_FILE("c:/boot.ini"), 30);`

Dostęp do plików w MS SQL

- Wykorzystanie xp_cmdshell
- Mechanizmy OLE Automation
 - Wykorzystanie sp_OACreate, sp_OAMethod
 - Domyślnie wyłączone podobnie jak xp_cmdshell
- Konstrukcja OPENROWSET
 - `SELECT BulkColumn
FROM OPENROWSET (BULK 'c:\boot.ini',
SINGLE_CLOB) MyFile`
 - Wykorzystywane uprawnienia konta serwera SQL

Podsumowanie

- Twórcy obu silników troszczą się o bezpieczeństwo
 - Największym błędem zdaje się możliwość wykonywania wielokrotnych zapytań w MS SQL
- W ujęciu bezpieczeństwa nieco korzystniejszym rozwiązaniem wydaje się MySQL, jednak inne kryteria mogą przeważać na korzyść MS SQL
 - Zwłaszcza odpowiednio skonfigurowanego!

Poznajmy się:
PCSS i MIC

IIS i PHP

Dlaczego
heterogeniczny
hosting?

Bezpieczeństwo
baz danych

Zabezpieczenie
systemu
i serwera

Interpreter języka
stron

ASP / PHP – najnowsze błędy

- Błędy występują w obu rozwiązaniach
 - Microsoft .NET Framework Denial of Service Vulnerability (sierpień 2009):
 - Zdalny atak DoS przy pomocy specyficznemu skonstruowanego żądania HTTP dla IIS + ASP.NET w *integrated mode* – ASP.NET 2.x i 3.x
 - PHP Multiple Vulnerabilities: Zdalny atak o niezdefiniowanych skutkach (wrzesień 2009)
 - Błędy w funkcjach obsługi EXIF, certyfikatów oraz `imagecolortransparent()` – PHP < 5.2.11
 - PHP jest rozwiązaniem o kodzie otwartym – więcej osób może znaleźć błędy

Konfiguracja ASP.NET

- Pliki konfiguracyjne ASP.NET
 - Pliki tekstowe w formacie XML
 - Edycja ręczna lub modyfikacja części opcji w IIS Manager
 - Dla całego serwera
 - machine.config + web.config (katalog %SystemRoot%\Microsoft.NET\Framework\%wersja%\CONFIG)
 - Dla aplikacji webowej
 - web.config (w katalogu głównym i/lub podkatalogach)

Code Access Security

- Aplikacji można przypisać 1 z 5 poziomów zaufania
 - Full, High, Medium, Low, Minimal
 - Konfiguracja: web.config, machine.config
- Możliwe jest także przygotowanie własnej definicji poziomu zaufania
- Domyślnie aplikacje webowe uruchamiane są z poziomem Full
 - Zły pomysł, szczególnie dla współdzielonego hostingu

Poziomy zaufania

- Full – brak ograniczeń (z dokładnością do uprawnień konta, na którym działa aplikacja)
- High – brak możliwości wykonania kodu niezarządzanego (*unmanaged code*)
- Medium – dostęp jedynie do katalogu aplikacji
- Low – blokada odwołań do innych środowisk (sieć, baza danych itd.)
- Minimal – dostępne wyłącznie najprostsze operacje (np. obliczenia)

Błędna konfiguracja

```
<location allowOverride="true">
  <system.web>
    <securityPolicy>
      <trustLevel name="Full" policyFile="internal"/>
      <trustLevel name="High" policyFile="web_hightrust.config"/>
      <trustLevel name="Medium"
policyFile="web_mediumtrust.config"/>
      <trustLevel name="Low" policyFile="web_lowtrust.config"/>
      <trustLevel name="Minimal"
policyFile="web_minimaltrust.config"/>
    </securityPolicy>
    <trust level="Full" originUrl=""/>
  </system.web>
</location>
```

Szybki test

- ASP.NET Security Analyzer (ANSA)
 - Autor: Dinis Cruz, OWASP
 - <http://www.owasp.org/index.php/ANSA>
 - Wersja 0.31 (dawno nie rozwijana, ale wskazuje najważniejsze podatności)
 - Narzędzie uruchamiamy z katalogu wewnątrz witryny
 - http://127.0.0.1/ANSA_V0_31b/default.aspx
 - Uruchomienie na witrynie skojarzonej z niestandardowym portem może generować błędy

Szybki test (2)



Critical Vulnerabilities

SECURITY TEST	STATUS	SCORE	COMMENTS
WSH_Enabled	OK	Critical	The WSH (namelly WSCRIPT.SHELL) object could be created. This object allows the remote should be disabled for normal users and should only be available to administrators
WSH_execute_cmd	OK	Critical	The server allows the remote execution of commands!
WMI_execute_cmd	OK	Critical	The server allows the remote execution of commands by creating a new cmd.exe process!
W32_execute_cmd	OK	Critical	The server allows the remote execution of commands using a direct call to WinExec API!

WMI_list_User_Account	OK	High	Using WMI's Win32_UserAccount It was possible to list the existent user Accounts	More details
-----------------------	----	------	--	------------------------------

Medium Vulnerabilities

SECURITY TEST	STATUS	SCORE	COMMENTS	MORE DETAILS
FSO_Enabled	OK	Medium	The FSO (Scripting.FileSystemObject) could be created	More details
FSO_Create_temp_files	OK	Medium	It was possible to create and read temporary files using FSO	More details
WMI_list_Processes	OK	Medium	Using WMI's Win32_Process It was possible to list the processes currently running in the server	More details
WMI_list_Services	OK	Medium	Using WMI's Win32_Service It was possible to all information available about the Services currently installed in the server	More details
WMI_see_Application_Log	OK	Medium	Using WMI's Win32_NTLogEvent where Logfile='Application' It was possible to list the current Application event log entries	More details
WMI_see_System_Log	OK	Medium	Using WMI's Win32_NTLogEvent where Logfile='System' It was possible to list the current System event log entries	More details
WMI_list_Shares	OK	Medium	Using WMI's Win32_Share It was possible to list of available network shares configured on the server	More details
WMI_list_Logical_Disks	OK	Medium	Using WMI's Win32_LogicalDisk It was possible to list the existent logical Disks	More details

Poprawa konfiguracji

- Obniżenie poziomu zaufania wszystkich lub niektórych aplikacji webowych
 - Element location
- Zabronienie nadpisywania
 - Atrybut allowOverride
- Więcej na temat konfiguracji ASP.NET
 - <http://www.devx.com/dotnet/Article/32493>
- Jest możliwe zastosowanie zabezpieczeń na poziomie systemu operacyjnego

Poprawiona konfiguracja

```
<location allowOverride="false">
  <system.web>
    <securityPolicy>
      <trustLevel name="Full" policyFile="internal"/>
      <trustLevel name="High" policyFile="web_hightrust.config"/>
      <trustLevel name="Medium"
policyFile="web_mediumtrust.config"/>
      <trustLevel name="Low" policyFile="web_lowtrust.config"/>
      <trustLevel name="Minimal"
policyFile="web_minimaltrust.config"/>
    </securityPolicy>
    <trust level="Medium" originUrl=""/>
  </system.web>
</location>
```

Jak to działa?

```
<% @Page Language="VB" Debug="true"%>  
  
<% Response.Buffer="true" %>  
  
<%  
Dim objShell = CreateObject("WScript.Shell")  
Dim objCmd = objShell.Exec("cmd /c dir c:\")  
Dim strResult = objCmd.StdOut.ReadAll()  
  
Response.Write(replace(strResult, vbCrLf, "<br />"))  
>%>
```

- Próba utworzenia groźnego obiektu oraz odwołania się do katalogu spoza aplikacji webowej
- Ustawienie „Debug” tylko dla celów testowych

Jak to działa? (2)

Wyjątek zabezpieczeń - Windows Internet Explorer

http://127.0.0.1:88

Plik Edycja Widok Ulubione Narzędzia Pomoc

Ulubione Wyjątek zabezpieczeń

Błąd serwera w aplikacji '/'.

Wyjątek zabezpieczeń

Opis: Aplikacja usiłowała wykonać operację niedozwoloną przez zasady zabezpieczeń. Aby udzielić tej aplikacji wymaganych uprawnień, skontaktuj się z administratorem systemu lub zmień poziom zaufania aplikacji w pliku konfiguracyjnym.

Szczegół wyjątku: System.Security.SecurityException: Żądanie uprawnienia typu 'System.Security.Permissions.SecurityPermission, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' nie powiodło się.

Błąd źródła:

```
Wiersz 5: <%  
Wiersz 6:  
Wiersz 7: Dim objShell = CreateObject("WScript.Shell")  
Wiersz 8: Dim objCmd = objShell.Exec("cmd /c dir c:\")  
Wiersz 9: Dim strResult = objCmd.StdOut.ReadAll()
```

CAS a wybór języka

- CAS działa jedynie dla kodu zarządzanego
 - Kod zarządzany (.aspx) wykonywany pod kontrolą środowiska CLR (aspnet_wp.exe), kod niezarządzany (.asp) obsługiwany przez asp.dll
 - ASP wymaga konwersji do ASP.NET
 - Nie ma możliwości tworzenia zarządzanego kodu PHP
 - O ograniczonych środkach prewencji za chwilę...

Czy PHP jest bezpieczne?

- *To say PHP has a security problem suggests that it's impossible to develop a secure PHP application, but to say PHP doesn't have a security problem suggests that everything is perfect – neither is true (Chris Shifflet)*
- *PHP is neither inherently secure nor insecure. It is the responsibility of the programmer of a web application, the database administrator and the system administrator to ensure that security is not compromised at several levels (James D. Keeline)*

Konfiguracja PHP

- Plik konfiguracyjny php.ini
 - Położenie: katalog systemowy lub instalacyjny
 - Plik dostarczony z instalacją zawiera szczegółowo opisany zestaw opcji
 - Edycja ręczna – brak narzędzia GUI przygotowanego przez producenta
 - Narzędzie firmy trzeciej (PHPConfig) logicznie grupuje większość dostępnych opcji, ale nie potrafi pracować na istniejącym pliku (tworzy własny z minimalną zawartością)
 - Dla chętnych:
<http://www.analogx.com/contents/download/network/phpconf.htm>

Bezpieczna konfiguracja

- Parametrem ograniczającym inwencję użytkownika na możliwie ogólnym poziomie jest opcja *safe_mode*
 - Przykładowe ograniczenia:
 - Mniejsze możliwości wykonania poleceń systemowych: część funkcji (shell_exec, dl, operator `) jest wyłączonych, inne (exec, passthru) mogą odwoływać się jedynie do wskazanego katalogu
 - Utrudnienie modyfikacji zmiennych środowiskowych
 - Zastrzeżenie znacznej liczby operacji
 - Automatyczne stosowanie funkcji escapeshellcmd()
 - Więcej: <http://pl.php.net/manual/pl/features.safe-mode.functions.php>

safe_mode – zastrzeżenia

- Ogranicza uprawnienia tak znacznie, że wiele aplikacji może przestać działać
- Bezpieczeństwa systemu nie powinno się rozwiązywać na poziomie ustawień PHP
 - Tym bardziej nie powinno się zapominać o zabezpieczaniu innych warstw
- Różne rekomendacje, ale...
 - Opcja oznaczona jako *deprecated* w PHP 5.3.0
 - Będzie usunięta w PHP 6

Inne aspekty bezpieczeństwa

- Unikanie wycieku informacji
 - `error_reporting = E_ALL & ~E_NOTICE`
 - `expose_php = off`
 - `display_errors = off`
 - `log_errors = on`
 - `error_log = [bezpieczna_lokalizacja]`
- Limity na wykorzystanie zasobów
 - `memory_limit = 8M`
 - `max_input_time = 60`
 - `max_execution_time = 120`

Inne aspekty bezpieczeństwa (2)

- Zasada minimalnych przywilejów
 - file_uploads = off
 - register_globals = off
 - magic_quotes_gpc = on
 - allow_url_fopen = off
 - open_basedir = [katalog_źródła]
- Blokada funkcji
 - disable_functions = passthru, exec, chmod, exec, get_cfg_var, getenv, mail, passthru, pcntl_exec, popen, send_mail, shell_exec, system, ...

Szybki test konfiguracji PHP



- Narzędzie PHPSecInfo
 - Autorstwa PHP Security Consortium
 - <http://phpsec.org/projects/phpsecinfo>
 - Wersja 0.2.1 (2007), ale jest nadal pomocna
 - Działa w środowisku Windows
 - Jest napisane w PHP ;)
 - Zawiera kilka specyficznych testów dla systemów Linux/Unix
 - Archiwum instalacyjne należy rozpakować do katalogu aplikacji webowej
 - Np. <http://127.0.0.1/phpsecinfo>

Wynik działania PHPSecInfo

The screenshot displays the PHPSecInfo application interface. At the top, the title bar reads "Security Information About PHP" and "PhpSecInfo Version 0.2.1; build 20070406 · Project Homepage". Below this, the section "Core" is highlighted. A table lists three security tests with their results:

Test	Result
allow_url_fopen	Pass allow_url_fopen is disabled, which is the recommended setting Current Value: 0 Recommended Value: 0 More information »
display_errors	Notice display_errors is enabled. This is not recommended on "production" servers, as it could reveal sensitive information. You should consider disabling this feature Current Value: 1 Recommended Value: 0 More information »
expose_php	Notice expose_php is enabled. This adds the PHP "signature" to the web server header, including the PHP version number. This could attract attackers looking for vulnerable versions of PHP Current Value: 1

In the bottom right corner, there is a logo for "ology it MTS2009".

ASP/PHP - podsumowanie

- CAS jest czynnikiem przemawiającym za zastosowaniem zarządzanego kodu ASP.NET
 - Brak dokładnego odpowiednika w PHP, aby osiągnąć przybliżony efekt, należy włożyć określoną ilość pracy w bezpieczną konfigurację
 - Osoby znające dobrze PHP (także w kontekście bezpieczeństwa) są jednak w stanie przygotować i wykorzystywać bezpieczne środowisko

ASP i PHP w jednym serwisie?

- Jest to możliwe!
- Kiedy?
 - Migracja lub łączenie aplikacji
 - Wiele serwisów
 - Eksperymenty
- Dlaczego?
 - Wymóg uruchomienia serwisu jak najszybciej
 - Zunifikowane sesje dla heterogenicznej aplikacji webowej

Podsumowanie

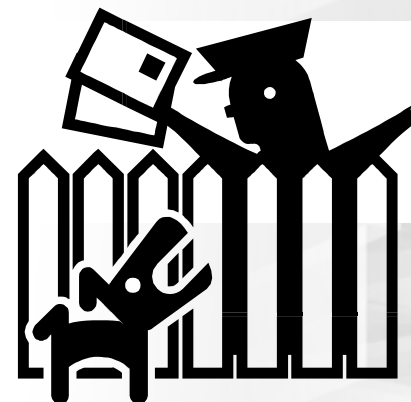
Bezpieczny mieszany hosting?

- Należy wziąć pod uwagę wiele aspektów
- Łączenie możliwości dwóch różnych środowisk – to dziedziczenie podatności ich obu
- Jeżeli budżet, czas poświęcony na migrację, umiejętności programistów nie są czynnikami znaczącymi – solidniejsze będzie środowisko homogeniczne
- Budowa środowiska mieszanego jest realna, ale musimy zwrócić uwagę na więcej problemów bezpieczeństwa

Więcej informacji

- IIS
 - <http://www.iis.net>
- MS SQL
 - <http://www.microsoft.com/poland/sql>
- My SQL
 - <http://www.mysql.com>
- ASP.NET
 - <http://www.asp.net>
- PHP
 - <http://www.php.net>

Informacje kontaktowe



- Autorzy prezentacji
 - gerard.frankowski@man.poznan.pl
 - marcin.jerzak@man.poznan.pl
- Centrum Innowacji Microsoft
 - WWW: <http://mic.psnc.pl>
 - e-mail: mic@man.poznan.pl
- Zespół Bezpieczeństwa PCSS
 - WWW: <http://security.psnc.pl>
 - e-mail: security@man.poznan.pl

Pytania?



Oceń naszą sesję

Ankieta dostępna na stronie www.mts2009.pl

Wygraj wejściówki na następny MTS!

Your potential. Our passion.[®]

Microsoft[®]

© 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

Microsoft, Windows oraz inne nazwy produktów są lub mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Microsoft w Stanach Zjednoczonych i innych krajach. Zamieszczone informacje mają charakter wyłącznie informacyjny. FIRMA MICROSOFT NIE UDZIELA ŻADNYCH GWARANCJI (WYRAŻONYCH WPROST LUB DOMYŚLNIE), W TYM TAKŻE USTAWOWEJ RĘKOJMI ZA WADY FIZYCZNE I PRAWNE, CO DO INFORMACJI ZAWARTYCH W TEJ PREZENTACJI.

Microsoft[®]

