Microsoft 2003 SERVER IIS KONTROL LİSTESİ	IP:		Tarih:
	Kontrol Eden:		Kontol Listesi Kayıt No:

N°	Uygulama	KONTROL	ÖNERİLEN DEĞER / AÇIKLAMA	DURUM
OS Service Pack and Hot Fix Denetleme (İşletim sistemi servis paketi ve yama)				
	En son servis paketi ve sonrasında çıkan gerekli tüm yamalar uygulandımı			☐
	Systeminfo, HFNetCHK komutları makine üzerinde çalıştırılıp kayıtlar alınmalı.			☐
	Microsoft Baseline Security Analyzer ile sunucu kontrol edilerek eksik yamalar tamamlanır ve açıklar kapatılır			☐
Rename Local Admin User (Yerel yönetici hesabı isim değişikliği)				
	Administrators hesabının ismi değiştirilmiş mi?			☐
	Guest Account Disable yapılmış mı?			☐
ACCOUNT POLICIES (Local Security Settings/Account Policies)				
+ Password Policy (Parola İlkesi Denetleme)				
	Policy	**Security Setting**		
	Enforce password history	24		☐
	Maximum password age	24		☐
	Minimum password age	1		☐
	Minimum password length	8		☐
	Password must meet complexity requirements	Enable		☐
	Store password using reversible encryption for all users in the domain	Disable		☐
+ Account Lockout Policy (Hesap Kilitleme İlkesi Denetleme)				
	Policy	**Security Setting**		
	Account lockout duration	15		☐
	Account lockout threshold	15		☐
	Reset account lockout counter after	15		☐
AUDIT POLICIES (Local Security Settings/Local Policies/Audit Policy)				
+ Local Policies (Yerel Denetleme ilkeleri)				
	Policy	**Security Setting**		
	Audit account logon events	Success, Failure		☐
	Audit account management	Success, Failure		☐
	Audit directory service access	No Auditing		☐
	Audit logon events	Success, Failure		☐
	Audit object access	Success, Failure		☐
	Audit policy change	Success, Failure		☐
	Audit privilege use	Success, Failure		☐
	Audit process tracking	Success, Failure		☐
	Audit system events	Success, Failure		☐
EVENT LOG SETTINGS (Olay Günlük Ayarları)				
	Log dosyaları düzenli olarak arşivlenmeli ve analiz edilmeli			☐
	Olay Kayıt dosyaları, işletim sisteminden farklı bir sabit disk bölümü üzerinde mi?			☐

	1. Click Start, click Run, type regedt32, and then click OK. 2. On the Windows menu, click HKEY_LOCAL_ MACHINE on Local Machine. • For the System log: a. Click the System\CurrentControlSet\Services\EventLog\System folder, and then double-click the FILE value. b. Type the new drive and path in the String box, include the file name \SysEvent.Evt, and then click OK. The default path is %SystemRoot%\System32\Config\SysEvent.Evt • For the Application log: a. Click the System\CurrentControlSet\Services\EventLog\Application folder, and then double-click the FILE value. b. Type the new drive and path in the String box, include the file name \AppEvent.Evt, and then click OK. The default path is %SystemRoot%\System32\Config\AppEvent.Evt • For the Security log: a. Click the System\CurrentControlSet\Services\EventLog\Security folder, and then double-click the FILE value. b. Type the new drive and path in the String box, include the file name \SecEvent.Evt, and then click OK. The default path is %SystemRoot%\System32\Config\SecEvent.Evt 3. Quit Registry Editor, and then restart the computer.			
+ Application Log (Uygulama logları)				
	Policy	**Security Setting**		
	Maximum Event Log Size	150 MB		☐
	Restrict Guest Access	Enable		☐
+ Security Log (Güvenlik logları)				
	Policy	**Security Setting**		
	Maximum Event Log Size	250 MB		☐
	Restrict Guest Access	Enable		☐
+ System Log (Sistem logları)				
	Policy	**Security Setting**		
	Maximum Event Log Size	150 MB		☐
	Restrict Guest Access	Enable		☐
SECURITY SETTINGS (Local Security Settings/Local Policies/Security Policy)				
+ Major Security Settings				
	Policy	**Security Setting**		
	Network Access: Allow Anonymous SID/Name Translation:	Disable		☐
	Network Access: Do not allow Anonymous Enumeration of SAM Accounts	Enable		☐
	Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares	Enable		☐
+ Minor Security Settings				
	Policy	**Security Setting**		
	Accounts: Guest Account Status	Disable		☐
	Accounts: Limit local account use of blank passwords to console logon only	Enable		☐
	Devices: Allowed to format and eject removable media	Administrators		☐
	Devices: Prevent users from installing printer drivers	Enable		☐
	Devices: Unsigned Driver Installation Behavior	"Warn, but allow…"		☐
	Domain Member: Disable Machine Account Password Changes	Disable		☐
	Domain Member: Maximum Machine Account Password Age	30 Day		☐
	Domain Member: Require Strong (Windows 2000 or later) Session Key	Enable		☐
	Interactive Logon: Do Not Display Last User Name	Enable		☐
	Interactive Logon: Do not require CTRL+ALT+DEL	Disable		☐
	Interactive Logon: Prompt User to Change Password Before Expiration	14 days		☐
	Interactive Logon: Require Domain Controller authentication to unlock workstation	Enable		☐

	Microsoft Network Client: Send Unencrypted Password to Connect to Third-Part SMB Server	Disable	☐
	Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	15 minutes	☐
	Microsoft Network Server: Disconnect clients when logon hours expire	Enable	☐
	Network Access: Do not allow storage of credentials or .NET passports for network authentication	Enable	☐
	Network Access: Let Everyone permissions apply to anonymous users	Disable	☐
	Network Access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\WindowsNT\CurrentVersion	☐
	Network Access: Remotely accessible registry paths and subpaths	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	☐ ☐
	Network access: Restrict anonymous access to Named Pipes and Shares	Enable	
	Network Security: Do not store LAN Manager password hash value on next password change	Enable	☐
	Network Security: LAN Manager Authentication Level	Send NTLMv2, refuse LM and NTLM	☐
	Network Security: LDAP client signing requirements	Negotiate Signing or Require Signing	☐
	Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption	☐ ☐
	Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption	☐
	Recovery Console: Allow Automatic Administrative Logon	Disable	☐
	Shutdown: Allow System to be Shut Down Without Having to Log On	Disable	☐
	System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key	☐
	System objects: Default owner for objects created by members of the Administrators group	Object Creator	☐
	System objects: Strengthen default permissions of internal system objects	Enable	☐

MICROSOFT SECURITY STANDARTS (MMS - Sistem güçlendirmesi için registry değişiklikleri)

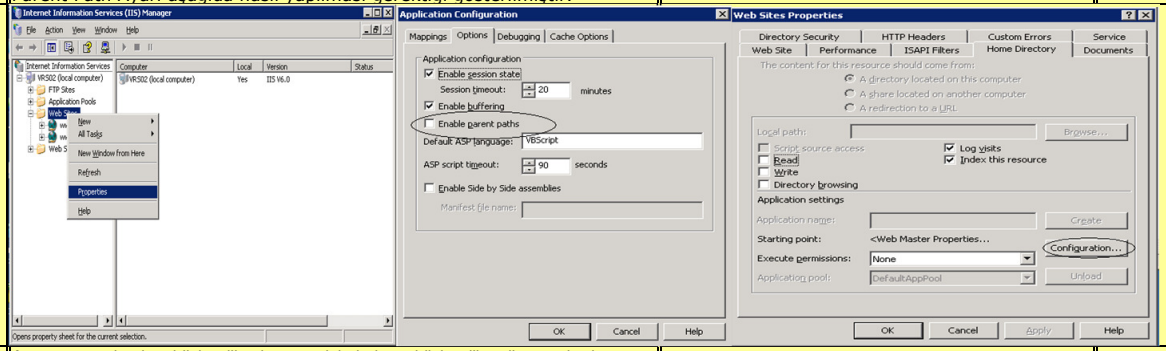
+ Dos Saldırılarından Korunmak İçin Gereken Ayarlar

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

	Name	**Data (REG_DWORD)**		
	EnableDeadGWDetect	0		☐
	EnableICMPRedirect	0		☐
	EnablePMTUDiscovery	0		☐
	EnableSecurityFilters	1		☐
	KeepAliveTime	300000		☐
	NoNameReleaseOnDemand	1		☐
	PerformRouterDiscovery	0		☐
	SynAttackProtect	2		☐
	TcpMaxConnectResponseRetransmissions	3		☐
	TCPMaxPortsExhausted	5		☐
	TcpMaxHalfOpen	200		☐

	TcpMaxHalfOpenRetried	150		
	IpEnableRouter	0		
	DisableIpSourceRouting	2		
+ Çalışan Servis Altyapısını Güçlendirmek için Gereken Ayarlar				
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters				
	Name	**Data (REG_DWORD)**		
	DynamicBacklogGrowthDelta	10		
	EnableDynamicBacklog	Enable		
	MaximumDynamicBacklog	20000		
	MinimumDynamicBacklog	20		
Lanman Şifre Özeti				
REGISTRY [HKLM\System\CurrentControlSet\Control\Lsa]				
	Name	**Data (REG_DWORD)**		
	NoLMHash	1		
DON'T DISPLAY LAST USERNAME ON LOGON SCREEN (Logon ekranında görünen en log on olan kullanıcı isminin kaldırılması)				
REGISTRY [HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System]				
	Name	**Data (REG_DWORD)**		
	DontDisplayLastUsername	1		
TURN OFF DEFAULT SHARES (Default Paylaşımların Kaldırılması)				
REGISTRY [HKLM\System\CurrentControlSet\Services\LanManServer\Parameters]				
	Name	**Data (REG_DWORD)**		
	AutoShareWks	0		
	AutoShareServer	0		
PREVENT ANONYMOUS ACCESS (Ziyaretçi Erişim Hakkının Kaldırılması)				
REGISTRY [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]				
	Name	**Data (REG_DWORD)**		
	restrictanonymous	00000001		
Döküm Dosyasının Saklanması				
REGISTRY (HKLM\System\CurrentControlSet\Control\CrashControl\)				
	Name	**Data (REG_DWORD)**		
	CrashDumpEnabled	0		
TURN OFF AUTORUN CDROM (Otomatik CD-Rom Denetiminin Kaldırılması)				
REGISTRY (HKLM\System\CurrentControlSet\Services\Cdrom\)				
	Name	**Data (REG_DWORD)**		
	Autorun	0		
DELETİNG PAGE FILE ON SHUTDOWN (Takas dosyalarının silinmesi)				
REGISTRY (HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\)				
	Name	**Data (REG_DWORD)**		
	ClearPageFileAtShutdown	1		
ENABLE SAFE DLL SEARCH MODE (Güvenli dll arama Mödülü Kullanımı)				
REGISTRY (HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager\)				
	Name	**Data (REG_DWORD)**		
	Enable Safe DLL search mode	Enable		
Gereksiz Servisleri Kapatma				
SERVICES				
	Service Name	**Startup Status**		
	Allerter	Disabled		
	ClipBook	Disabled		
	Computer Browser	Disabled		
	DHCP Client	Disabled		
	Distributed Link Tracking Server	Disabled		
	Error Reporting Service	Disabled		
	Human Interfeca Device Acces	Disabled		
	IMAPI CD-Burning COM Service	Disabled		

	Intersite Messaging	Disabled		☐
	Kerberos Key Distribution Center	Disabled		☐
	License Logging	Disabled		☐
	Messenger	Disabled		☐
	Netmeeting Remute Desktop Sharing	Disabled		☐
	Network DDE	Disabled		☐
	Temute Acces AutoConnection Manager	Disabled		☐
	Remute Prosedur Call (RPC) Locator	Disabled		☐
	Routing and Remute Access	Disabled		☐
	Server	Disabled		☐
	Telnet	Disabled		☐
	Terminl Services Session Directory	Disabled		☐
	Themes	Disabled		☐
	WebClient	Disabled		☐
	Windows Audio	Disabled		☐
	Windows Image Acquisition (WIA)	Disabled		☐
	Winetd-Windows Inetd	Disabled		☐
	Workstation	Disabled		☐
USER RIGHTS POLICY				
SECURITY [Local Security Settings\Local Policies\User Rights Assignment\]				
	Access this computer from network.	Administrators		☐
	Backup files and directories	Administrators, Backup Operators		☐
	Change system time	Administrators		☐
	Log on locally	Administrators		☐
	Manage auditing and security log	Administrators		☐
	Restore files and directories	Administrators, Backup Operators		☐
	Take ownership of files and other objects	Administrators		☐
	Act as part of the operating system	None		☐
	Debug programs	Administrators		☐
	Generate security audits	Administrators		☐
	Log on as a service	Administrators		☐
	Shut down the system	Administrators		☐
NTFS ACCESS CONTROL LIST (NTFS erişim izinleri)				
Kritik Dizinlere Uygulanacak Erişim Listesi				
	Dosya Yolu	**Access Kontrol Listesi**		
	%SystemRoot%\system32\	Administrators: Full; System: Full		☐
	%SystemRoot%\system32\drwatson.exe	Administrators: Full; System: Full		☐
	%SystemRoot%\system32\drwtsn32.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\edlin.exe	Administrators: Full; System: Full		☐
	%SystemRoot%\system32\eventcreate.exe	Administrators: Full; System: Full		☐
	%SystemRoot%\system32\eventtriggers.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\ftp.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\net.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\net1.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\netsh.exe	Administrators: Full; System: Full;Interactive: Full		☐
	%SystemRoot%\system32\rcp.exe	Administrators: Full; System: Full;Interactive: Full		☐
Yüklü Programları				
	Sunucu üzerinde 3rd party yazılım bulunmakta mı?			☐
Add-Remove Programs Ayarları				
	Add-Remove Programs Ayarlarından gereksiz proğramlar kaldırıldı mı?			☐
Sabit Disk Dosyalama Sistemi				
	Tüm sabit disk NTFS dosyalama sistemi kullanılarak biçimlendirilmiş mi?			☐
Virus Koruma Programının Yüklenmesi (Sunucu yerel network'te ise merkezi AV sunucusuna bağlı, DMZ'te ise internetten Update almalı)				
	Sunucu üzerinde gerçek zamanlı virüs koruması var mı?			☐
	Periyodik tam virüs taraması yapılıyor mu?			☐
	Veritabanı güncel mi?			☐

Backup (Yedekleme)				
	Sunucu üzerinde backup alınıyor mu?			☐
	Hangi dizinler backuplanıyor?			☐
Şifre Korumalı Ekran Koruyucusunun Devreye Alınması				
Display Properties/ScreenSaver/				
	Şifre korumalı ekran koruyucusu 3 dk. içinde devreye girecek şekilde ayarlı mı?	5 dk.		☐
IIS Security				
Ön Tanımlı Kurulum Dosyaları Silinmesi				
	Dosya Yolu	**Startup Status**		
	IISSamples, IISAdmin, IISHelp, ve Scriptler virtual directoriler kaldırılmalı.(\WINNT\Help\IISHelp, \Inetpub\IISSamples).			☐
	/scripts Virtual Directory mapping			☐
	inetpub/scripts/IISSamples			☐
	/iissamples Virtual Directory			☐
	/IISHelp Virtual Directory			☐
	/Printers Virtual Directory			☐
Sites and Virtual Directories				
	Web sitesi dosyaları System Partition'ınından farklı bir Partition da tutulmalı.			☐
	"Parent paths" setting disabled edilmeli. Parent Path Ayarı aşağıda nasıl yapılması gerektiği gösterilmiştir.			☐
				
	Anonymous olarak publish edilen http servislerinde, publish edilen directorylerde intenet Guest Accountunun sadece read hakkı olmadır.			☐
Files and Directories				
	Everyone group hakları kıstlanmalı (\WINNT\system32 ve Web dizininda hakkı olmamalı.)			☐
	Web sitesi root directoryde anonymous Internet accountları denny olmalı			☐
	Remote IIS administration uygulaması kaldırılmalı. (\WINNT\System32\Inetsrv\IISAdmin).			☐
Remote Data Services (RDS) Uzak Veri Servisleri				
	Dosya Yolu	**Kaldırılılma Referansları**		
	MSADC virtual directory (RDS) kaldırılmalı yada güvenli hale getirilmeli.	Delete the MSADC samples located in \Progam Files\Common Files\System\Msadc		☐
Internet Printing Protokolü Kaldırılması				
REGISTRY (HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting)				
	Name	**Data (REG_DWORD)**		
	DisableWebPrinting	1		☐
Hata Mesajları ve Hata Ayıklama				
	Kontol Maddesi	**Kontrol Referansları**		

⊘	Özelleştirilmiş HTTP hata mesajları oluşturulmalı.	1. Open the internet services manager in MMC 2. Right click on the web site / Virtual Directory in question 3. Select Properties on the pop-up menu. 4. Click the "Custom Errors" tab. 5. For each error tab custimeze HTTP error mesagges		☐
⊘	Ele alınmamış hata mesajlarının istemciye gösterilmesi engellenmeli	%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ altında Set the mode of customErrors to "ON" and redirect to a custom error page. *customErrors mode="on" defaultRedirect="ourerrorpage.html"*		☐
⊘	Client-side Application Debugging (AppAllowClientDebug) İstemci Uygulama hata ayıklamamları kapalımı.	1. Open the Internet Service Manager in the Microsoft Management Console. 2. Right-click on the Web site / Virtual Directory in question. 3. Select Properties on the pop-up menu. 4. Click the Home Directory / Virtual Directory tab. 5. Select Configuration in the Application setting box 6. Click the debugging Tab 7. Clear the "Enable ASP client-side script debugging" Setting 8. Click OK twice to return to the Microsoft Management Console.		☐
⊘	Server-side Application Debugging (AppAllowDebug) Sunucu Uygulama hata ayıklamamları kapalımı.	1. Open the Internet Service Manager in the Microsoft Management Console. 2. Right-click on the Web site / Virtual Directory in question. 3. Select Properties on the pop-up menu. 4. Click the Home Directory / Virtual Directory tab. 5. Select Configuration in the Application setting box 6. Click the debugging Tab 7. Clear the "Enable ASP server-side script debugging" Setting 8. Click OK twice to return to the Microsoft Management Console.		☐
⊘	ASP Error Messages Setting (AspScriptErrorSentToBrowser) Asp server scripting hatalarının istemciye gönderilmesi kapatılmalı yada özelleştirilmeli.	1. Open the Internet Service Manager in the Microsoft Management Console. 2. Right-click on the Web site / Virtual Directory in question. 3. Select Properties on the pop-up menu. 4. Click the Home Directory / Virtual Directory tab. 5. Select Configuration in the Application setting box 6. Click the debugging Tab 7. Select the "Send text error message to client" option 7. enter a custom messagein the box below "Send text error message to client" 8. Click OK twice to return to the Microsoft Management Console.		☐
Oturum ve Zaman Aşımı Kontrolü				
	Dosya Yolu	**Security Setting**		
⊘	ASP Session Object Timeout (AspSessionTimeout)	10 minutes Internet Service Manager/Application Settings/Session timeout		☐
⊘	HTTP Connection Timeout (Connection Timeout and ServerListen timeout)	120 Internet Service Manager/web site/Connection timeout		☐
ISAPI Filters				

	Gerekli olmayan yada kullanılmayan ISAPI filterlar remove edilmeli.	idq.dll httpext.dll msw3prt.dll admin.dll ssinc.dll author.dll shtml.dll httpodbc.dll		☐
Accounts				
	ASP.NET uygulama account minumun ayrıcalıkta olmalı.			☐
Auditing and Logging				
	Log dosyaları düzenli olarak arşivlenmeli ve analiz edilmeli			☐
	IIS is configured for W3C Extended log file format auditing			☐
	Log dosyaları farklı bir partitionda tutuluyormu			☐
SQL Security				
	En son servis paketi ve sonrasında çıkan gerekli tüm yamalar uygulanmalı			☐
	sa şifresi kesinlikle boş olmamalı.Enaz 8 karakter ve komplex olmalı.			☐
Kullanılmayan Extension (HTTPForbiddenHandler) ile kapatılması				
%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG				
	Kontol Maddesi	**Kontrol Referansları**		
	Kullanılmayan web extension' ların Microsoft.NET Framework kullanılarak engellenmeli	%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ altında HTTPForbiddenHandler *add verb="*" path="*.asax" type="System.Web HTTPForbiddenHandler"*		☐
DOS SALDIRILARINDAN KORUNMAK İÇİN GEREKEN AYARLAR				
%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG				
	Kontol Maddesi	**Kontrol Referansları**		
	HttpRunTime değeri değiştirilerek büyük boyutlu dosyaların upload edilmesi engellenmeli	%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ altında HTTPRuntime *httpRuntime maxRequestLength="4096000"*		☐
Trace işeleminin kapatılması				
%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG				
	Kontol Maddesi	**Kontrol Referansları**		
	Bilgi sızmasının engellenmesi için trace yöntemi kapatılmalıdır.	%SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ altında Trace *trace enabled="false"*		☐
Other Check Points				
	IIS Lockdown uygulaması kurulumu			☐
	IIS Lock down tool server üzerinde çalıştırılmalı			☐
	Webdav Kullanılmıyorsa kapatılmalı			☐
	FrontPage Server Extensions (FPSE) kaldırılmalı (Uncheck Add/RemovePrograms/Windows ComponentsApplicationServer/IIS service/FrontPage 2002 Server Extensions)			☐
URLScan Uygulaması Kontrolleri				
	URL Scan uygulaması kurulumu			☐
	Kontol Maddesi	**Kontrol Referansları**		
	HTTP istekleri filtrelenmeli. URLScan yüklenmeli.			☐
%SystemRoot%\inetsrv\urlscan\urlscan.ini				
	DenyExtensions:	Consider deny the following extensions: .cer, .cdx,.asa, .exe, .bat, .cmd, .com, .htw, .ida,.idq, .htr, .idc, .stm, .printer, .ini, .log, .pol, .dat		☐

	DenyVerbs:	At a minimum, deny the following verbs: TRACE/TRACK, DELETE, OPTIONS, PROPFIND		☐
	DenyHeaders:	If WebDAV is not required it should be disabled.		☐
	RemoveServerHeaders:			☐
	DenyUrlSequences:	Consider disabling the following Url Sequences: .., :, ./, \, %,&		☐
URLScan.ini ACCESS CONTROL LIST (urlscan erişim izinleri)				
Kritik Dizinlere Uygulanacak Erişim Listesi				
	Dosya Yolu	**Access Kontrol Listesi**		
	..\inetsrv\urlscan\urlscan.dll	Read and Execute (set on IIS 6.0 only): LocalService, IIS_WPG, and NetworkService Full: Administrators, and LocalSystem		☐
	..\inetsrv\urlscan\urlscan.ini	Read (set on IIS 6.0 only): IIS_WPG, LocalService, and NetworkService Full: Administrators, and LocalSystem		☐
	..\inetsrv\urlscan\logs	Read (set on IIS 6.0 only): IIS_WPG, LocalService, and NetworkService Full: Administrators, and LocalSystem		☐
SSL (Secure Socket Layer) Sertifikası Kontrolleri				
	Geçerli bir sayısal sertifika Kullanılmalı			☐
	Sertifikasının geçerlilik süresi kontrol edilmeli			☐
	Haberleşme için kullanılan ssl altyapısı sadece SSLv3 desteklemeli	HKey_Local_Machine\System\CurrentControlSet\Control\ SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Server *Değer Adı: Disable* *Değer Türü: DWORD* *Değer Adı: 00000000 (binary degeri)*		☐
	Zayıf şifreleme algoritmaları kaldırılmalı	Settings and configuration follow this URL: http://support.microsoft.com/kb/245030/ *SSL_RSA_EXPORT_WITH_RC4_40_MD5* *SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5* *SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA* *SSL_RSA_EXPORT1024_WITH_RC4_56_SHA* *SSL_RSA_EXPORT_WITH_RC4_40_MD5*		☐

Lejant	
	Uygulanmasında sakınca yoktur
	Kontrolü Yapılmalı
	Uygulamada Sorun Yaratabilir