



# ***URLScan Tools Optimization***

***Feb, 2007***

***by Yoon, Young (Coderant@gmail.com)***

# URLScan Tools Optimization 방법

## 1. 개요

URLScan은 ISAPI Filter(urlscan.dll)이며 우선순위를 맨 위로 로드시켜 웹 서버에 요청되는 불특정 문자 또는 URL 인코딩된 것을 분석하여 HTTP 리퀘스트를 반환시키는 역할을 한다.

- HTTP request 분석
- 심각한 공격에 노출을 줄임

다음과 같은 기준으로 요청을 거부할 수 있도록 IIS설정이 가능하다.

### 1.1 URLScan.ini 파일 수정

URLScan 의 모든 구성은 \WINDOWS\System32\Inetsrv\URLscan 폴더에 URLScan.ini 파일과 urlscan.dll 을 통해 수행된다.

URLScan 을 구성하려면 텍스트 편집기에서 이 파일을 열고 적절히 변경한 후 파일을 저장된다.

**참고** 변경 사항을 적용하려면 인터넷 정보 서비스(IIS)를 다시 시작해야 한다. 수행하는 방법은 명령 프롬프트에서 **IISRESET** 명령을 실행한다.

URLScan.ini 파일에는 다음과 같은 구역이 포함되어 있다.

- UrlScan 의 작동은 UrlScan.ini 에 의해 제어됨
- UrlScan.ini 은 UrlScan.dll 과 같은 디렉터리 내에 존재해야 함
- UrlScan 은 초기 동작 시 단지 ini 파일만 읽어 들임(성능 저하)
- ini 파일에 변경이 있기 전에 웹 서비스를 중지했다 재 시작하는 작업이 필요함
- UrlScan.dll 내의 기본 설정은 해당 서버로의 모든 요청을 거부하도록 되어 있다.
- 서비스 요청을 넘길 있도록 UrlScan 에 UrlScan.ini 을 제공하도록 해야 함
- 예제 UrlScan.ini 파일이 제공됨
- 잘 알려진 IIS 공격을 막아내도록 설정

### 1.2 URLScan 설치 및 확인법

URLScan 2.0은 IISLockdown(IISLockd.exe,)과 함께 설치를 하거나 URLScan만 별도로 설치할 수 있다.

가. IISLockdown 동작과 같이 URLScan를 설치하는 경우

URLScan 2.0은 IIS Lockdown Wizard(IISLockd.exe)의 한 부분으로 설치할 수 있다.

나. IISLockdown 동작 없이 URLScan 설치하기

IISLockdown 동작 없이 설치하려면, IIS Lockdown Tool에서 수동으로 압축을 풀어야 한다

다. 첫번째로 디렉터리에 IISLockd.exe를 저장한다. 그리고 나서 URLScan setup 파일을 푼다.

IISLocked.exe 설치하려고 하는 디렉터리에 아래 명령어를 실행한다.

```
C:\IISLockdown\iislockd.exe /q /c
```

다. URLScan 2.5 설치

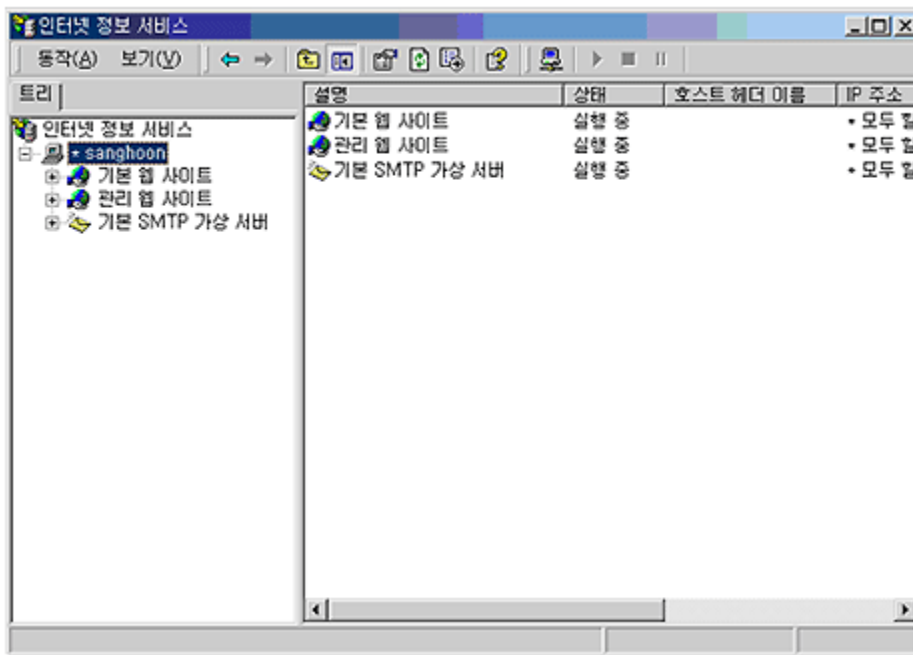
현재 URLScan 2.5버전이 가장 최신이다.

만약 URLScan 2.5를 설치하려면 먼저 URLScan 1.0 또는 URLScan 2.0이 먼저 설치되어 있어야 한다. 디폴트로 설치되는 디렉터리는 %windir%\system32\inetsrv\urlscan이며 이 디렉터리에는 Urlscan.dll, URLScan.ini 그리고 URLScan logs가 저장된다. URLScan.dll는 ISAPI 필터로 설정해주어야 한다.

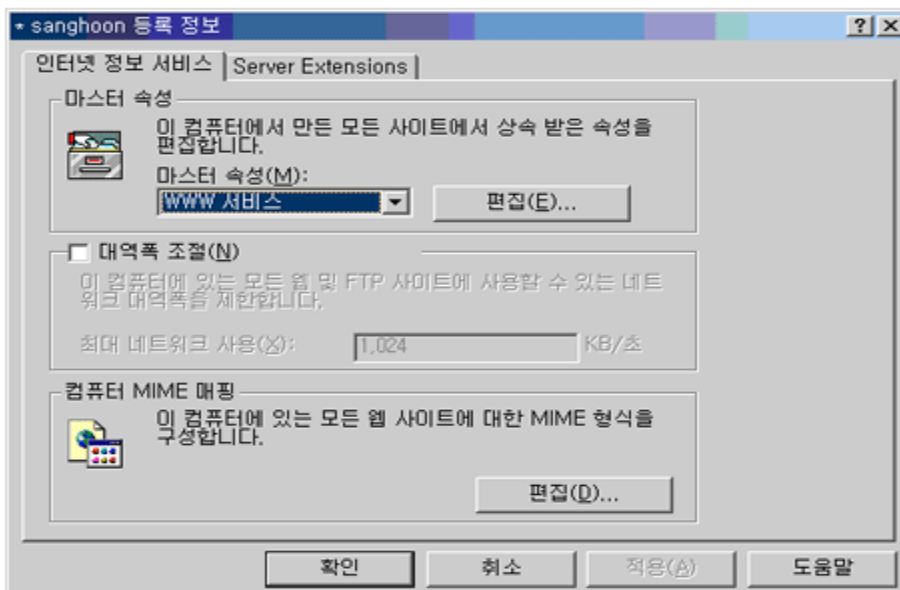
라. URLScan 제거는 Internet Services Manager의 대화상자 속성의 웹 서버의 ISAPI 필터 설정부분을 제거해주면 된다.

마. 인터넷 서비스 관리자로 Urlscan의 ISAPI 필터 확인하는 방법

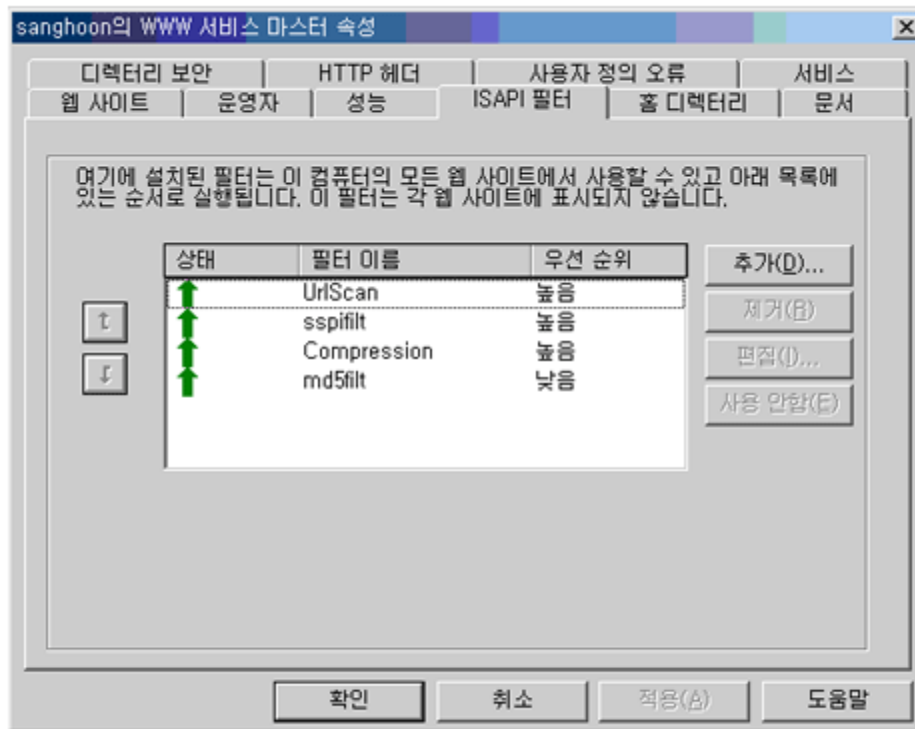
- 1) 시작 -> 프로그램 -> 관리도구 -> 인터넷 서비스 관리자를 실행한다.
- 2) 여기서 서버이름이 sanghoon으로 가정되어 있다고 봅니다. 좌측화면의 컴퓨터 이름에서 마우스 우측버튼을 클릭하여 등록정보를 확인한다.



3) 마스터 속성에서 WWW 서비스를 선택 후 우측에 있는 편집버튼을 클릭한다.



4) ISAPI 필터 탭을 선택하면 아래와 같이 Urlscan의 우선순위가 맨 위로 올라가 있는 것을 확인한다.



### 1.3 URLScan.ini 설명

```

[Options]
UseAllowVerbs=1          : if 1, use [AllowVerbs] section, else use [DenyVerbs] section
UseAllowExtensions=0    : if 1, use [AllowExtensions] section, else use [DenyExtensions] section
NormalizeURLEscape=1    : if 1, canonicalize URL before processing
VerifyNormalization=1  : if 1, canonicalize URL, twice and reject request if a change occurs
AllowHighBitCharacters=1 : if 1, allow high bit (ie, UTF8 or MBCS) characters in URL
AllowDotInPath=0        : if 1, allow dots that are not file extensions
RemoveServerHeader=0   : if 1, remove "Server" header from response
EnableLogging=1         : if 1, log UrlScan activity
PerProcessLogging=0     : if 1, the UrlScan.log filename will contain a PID (ie, UrlScan.123.log)
AllowLateScanning=0    : if 1, then UrlScan will load as a low priority filter.

: If RemoveServerHeader is 0, then AlternateServerName can be
: used to specify a replacement for IIS's built in 'server' header
AlternateServerName=

[AllowVerbs]
:
: The verbs (aka HTTP methods) listed here are those commonly
: processed by a typical IIS server.
:
: Note that these entries are effective if "useAllowVerbs=1"
: is set in the [options] section above.
:
GET
HEAD
POST
:OPTIONS : FrontPage Server Extensions requires OPTIONS.  If you need to enable
: it, uncomment the OPTIONS verb and set "AllowLateScanning=1" in the
: [options] section above.  Additionally, after changing this file and
: restarting the web service, you should go to the "ISAPI Filters" tab
: for the server's properties in MMC and ensure that urlscan is listed
: lower than fpxed11.dll.

[DenyVerbs]
:
: The verbs (aka HTTP methods) listed here are used for publishing
: content to an IIS server via WebDAV.
:
: Note that these entries are effective if "useAllowVerbs=0"
: is set in the [options] section above.
:
PROPFIND
PROPPATCH
MKCOL
DELETE
PUT
COPY
MOVE
LOCK
UNLOCK
    
```

사용자가 필요한 확장명을 가진 것을 웹 서비스에서 사용하려면 URLScan.ini안에 있는 [DenyExtentions] 섹션 밑에서 필요한 확장명을 주석으로 처리하면 해당된 파일을 사용할 수 있다. 구체적인 정보는 \Winnt\system32\inetrv\urlscan\urlscan.txt 파일을 참조하시면 각 섹션에 대한 정보를 보실 수 있다. [Options] 섹션은 IIS 서버가 유효한 웹 요청과 유효하지 않은 웹 요청을 처리하는 방법을 정의할 수 있으며 옵션은 다음과 같다.

### [Options] 섹션 부분

[Options]에서는 많은 URLScan 옵션을 구성할 수 있다. 이 구역의 각 줄은 다음 형식으로 되어 있다.

*OptionName=OptionValue* 사용 가능한 옵션과 기본값은 다음과 같다.

UseAllowVerbs
<ul style="list-style-type: none"><li>● 기본값인 1로 설정할 경우 UrlScan은 UrlScan.ini의 [AllowVerbs] 섹션에 허용된 HTTP 메소드를 사용하는 요청만 허용한다. [AllowVerbs] 섹션은 대/소문자를 구분한다. ("GET", "HEAD", "POST" requests만 허용할 것)</li><li>● 기본값이 0으로 설정되면 UrlScan은 UrlScan.ini의 [DenyVerbs] 섹션에 있는 정의된 HTTP 메소드가 포함된 요청을 차단한다. [DenyVerbs] 섹션은 대/소문자를 구분하지 않는다.</li></ul>

UseAllowExtensions
<ul style="list-style-type: none"><li>● 기본값이 1로 설정할 경우 UrlScan은 UrlScan.ini의 [AllowExtensions] 섹션에 정의된 파일 확장명을 가진 파일 요청만 허용한다. ( "1"로 셋팅될 확장자 명은 "asp", ".aspx", ".cer", ".cdx", ".asa", ".html", ".js", ".htm", ".jpg", ".jpeg", ".gif")</li><li>● 기본값인 0으로 설정되면 UrlScan은 UrlScan.ini의 [DenyExtensions] 섹션에 정의된 파일 확장명 요청만을 차단한다. [AllowExtensions]과 [DenyExtensions] 섹션은 모두 대/소문자를 구분하지 않는다.</li></ul>

NormalizeUriBeforeScan
<ul style="list-style-type: none"><li>● 기본값이 1로 설정할 경우 UrlScan은 먼저 IIS가 디코딩한 즉, %기호로 특정 문자를 대체할 수 있다는 의미이다. 예를 들어 %20은 공백에 해당하므로 http://myserver/My%20Dir/My%20File.htm에 대한 요청은 http://myserver/My Dir/My File.htm에 대한 요청과 동일하다.</li><li>● 기본값이 0으로 설정되면 UrlScan은 클라이언트가 보낸 원시 URL을 모두 분석한다. URL 분석에 대해 잘 알고 있는 고급 관리자만 이 옵션을 0으로 설정해야 한다. 그렇지 않으면 IIS 서버가 URL 확장명의 정확한 분석을 무시하는 정형화(canonicalization) 공격에 노출될 수 있다.</li></ul>

### VerifyNormalization

- 기본값이 1로 설정할 경우 UriScan은 URL을 두번 정규화 한다. 이 동작은 URL에 이중 인코딩된 문자열이 들어 있을 때 정형화 공격을 방어한다. 예를 들어, %252e 문자열은 이중 인코딩된 '.' 문자로, %25는 '%' 문자로 디코딩된다. %252e의 첫 번째 디코딩은 결국 %2e가 되고 두 번째에 '.'로 디코딩될 수 있습니다.
- 기본값이 0으로 설정되면 이 확인이 수행되지 않는다.

### AllowHighBitCharacter

- 기본값이 1로 설정할 경우 UriScan은 URL에 있는 바이트를 허용한다.
- 기본값이 0으로 설정되면 UriScan은 URL에 ASCII 문자 이외의 문자가 포함된 요청을 거부한다. 이 기능은 유니코드 또는 UTF-8 기반 공격을 방어할 수 있지만 ASCII가 아닌 코드 페이지를 사용하는 IIS 서버에 대한 정당한 요청을 거부하기도 한다. 단, 이렇게 하면 특정 종류의 공격을 방지할 수는 있지만 한글 파일명에 대한 요청도 차단할 수 있다.

### AllowDotInPath

- 기본값이 0으로 설정할 경우 UriScan은 점(.) 문자가 여러 개인 요청을 거부한다. URL의 경로 정보나 쿼리 문자열 부분에 안전한 파일 확장명을 넣어 위험한 파일 확장명에 대한 요청을 가장하는 공격을 차단할 수 있다.(Path Traversal 공격 "../..../")  
UriScan은 마침표가 포함된 디렉터리에 대한 요청도 거부할 수 있다.("/./")
- 기본값이 1로 설정되면 UriScan은 이 테스트를 수행하지 않는다. UriScan은 아직 IIS가 URL을 분석하기 전에서 작동하기 때문에 어떤 경우에도 점 문자가 확장명을 나타내는지 또는 URL의 디렉터리 경로나 파일 이름의 일부인지를 판단할 수 없다.  
UriScan은 "http://servername/BadFile.exe/SafeFile.htm"와 같은 요청을 허용할 수 있다.  
이 때 URL은 문자열의 마지막 점 뒤에서 시작하고 점이나 문자열 끝 뒤의 첫 번째로 오는 물음표나 슬래시 문자로 끝난다. [AllowDotInPath]를 0으로 설정하면 공격자가 경로 정보를 사용해서 요청의 진짜 확장명(예: /path/TrueURL.asp/BogusPart.htm)을 숨길 경우에 방어할 수 있다.  
**[참고]** : [AllowDotInPath]를 0으로 설정하면 UriScan이 디렉터리 이름에 점이 포함된 요청도 거부할 수 있다.

### RemoveServerHeader

- 기본값이 1로 설정할 경우 UrlScan은 모든 모든 IIS 서버로 식별하는 헤더를 클라이언트에 보내지 않는다.
- 기본값이 0으로 설정하면 UrlScan은 이 동작을 수행하지 않는다. 이 기능은 IIS 4.0 이상에 설치되어 있어야 사용할 수 있다.

### EnableLogging

- 기본값이 1로 설정할 경우 %WINDIR%\System32\Inetsrv\URLScan에 차단되는 모든 요청의 전체 로그를 저장한다.
- 기본값을 0으로 설정하면 로깅을 저장하지 않는다.

### PerProcessLogging

- 기본값을 1로 설정할 경우 UrlScan은 UrlScan.dll을 호스트하는 IIS의 각 프로세스에 대해 별도의 로그를 만든다.(예: UrlScan.1234.log)
- 기본값이 0으로 설정하면 모든 프로세스가 같은 파일(UrlScan.log)에 기록된다.

### AlternateServerName(기본적으로 지정되지 않음)

- [RemoveServerHeader]가 0으로 설정할 경우 **AlternateServerName** 옵션에서 문자열을 지정하여 서버 헤더에서 전달되는 내용을 지정할 수 있다.
- [RemoveServerHeader]가 1로 설정되면 이 옵션은 무시된다. 이 기능은 UrlScan이 IIS 4.0 이상에 설치되어 있어야 사용할 수 있다.(IIS 서버임을 모르게 이름을 변경할 수 있다)

### AllowLateScanning

- 기본값이 1로 설정할 경우 UrlScan은 낮은 우선 순위 필터로 실행되므로 UrlScan이 분석을 수행하기 전에 다른 필터가 URL을 수정할 수 있다.  
FrontPage Server Extensions(FPSE)에서는 이 옵션을 1로 설정해야 한다.
- 기본값이 0으로 설정되면 UrlScan은 높은 우선 순위 필터로 실행된다. 즉, 서버에 설치되어 있는 다른 ISAPI(Internet Server Application Programming Interface) 필터보다 먼저 실행된다.

### PerDayLogging

- 기본값이 1로 설정할 경우 UrlScan은 매일 새 로그 파일을 만들고 각 로그 파일 이름은 Urlscan.MMDDYY.log로 기록된다.(예: UrlScan.101501.log).
- [PerDayLogging=1]과 [PerProcessLogging=1]이 모두 설정되면 로그 파일 이름에 날

짜와 프로세스 ID가 포함한다(예: UrlScan.101501.123.log). UrlScan 동작이 발생하지 않는 날에 대해서는 로그가 만들어지지 않는다.

- 기본값이 0으로 설정하면 UrlScan은 날짜에 관계없이 모든 로깅을 같은 날짜에 저장한다.

### RejectResponseUri(기본적으로 지정되지 않음)

- 이 옵션은 URLScan이 요청을 차단할 때 실행되는 파일에 대한 가상 경로를 지정한다. 이 옵션을 사용하면 차단된 요청에 대해 클라이언트에 보내는 응답을 사용자 지정할 수 있다. **[RejectResponseUri]**을 /Path/To/RejectResponseHandler.asp처럼 해당 파일에 대한 가상 경로로 지정해야 한다. Active Server Pages(ASP) 페이지와 같이 URLScan이 일반적으로 차단하는 파일을 지정할 수 있다. 해당 서버 변수를 사용할 수도 있다.

→ **HTTP\_URLSCAN\_STATUS\_HEADER**: 요청을 차단한 이유를 지정한다.

→ **HTTP\_URLSCAN\_ORIGINAL\_VERB**: 차단된 요청의 원래 메소드(GET, POST, HEAD 또는 DEBUG)를 지정

→ **HTTP\_URLSCAN\_ORIGINAL\_URL**: 차단된 요청의 원래 URL을 지정한다.

- **[RejectResponseUri]**을 /~\*의 특수한 값으로 설정하면 URLScan은 로깅 전용 모드를 사용한다. 따라서 IIS는 모든 요청을 제공할 수 있지만 일반적으로 차단되는 요청에 대해 URLScan 로그에 항목을 추가한다. 이것은 URLScan.ini 파일을 테스트하려는 경우 유용하다.
- **[RejectResponseUri]**의 값을 지정하지 않으면 URLScan은 /<Rejected-By-UrlScan>의 기본값을 사용한다.

### UseFastPathReject

- 기본값이 1로 설정할 경우 UrlScan은 **[RejectResponseUri]**을 무시하고 클라이언트에 404 오류 응답을 브라우저에 반환한다.
- 이 옵션은 **[RejectResponseUri]**을 모두 처리하는 것보다 빠르지만 이 옵션이 사용되면 IIS가 사용자 정의 404 응답을 반환하거나 요청의 여러 부분을 IIS 로그에 기록할 수 없다.
- 기본값이 0으로 설정하면 URLScan은 **[RejectResponseUri]** 설정을 사용하여 요청을 처리한다.

### DenyUriSequences

- 이 옵션은 URL 상에 차단될 특정 특수 문자열들을 정의한다.
- 디폴트 옵션은 ".", "/", "\", ":", "%", "&" 이고 부가적으로 "#", "<", ">", "\$", "@", "!", ",", and "~"를 추가할 수 있다.
- 이 옵션은 URL상에서 크로스 사이트 스크립트를 포함하는 공격등을 차단할 수 있다.

### [AllowVerbs] 섹션

**[Options]** 섹션의 **[UserAllowVerbs]** 옵션값이 1로 설정할 경우 UrlScan은 여기에 정의된 메소드 요청만을 허용한다. 이 섹션의 항목은 대/소문자를 구분하지 않는다.

### [DenyVerbs] 섹션

**[Options]** 섹션의 **[UserAllowVerbs]** 옵션값이 0으로 설정할 경우 UrlScan은 여기에 정의되어 있는 메소드가 포함된 요청을 거부한다. 이 섹션의 항목은 대/소문자를 구분하지 않는다.

### [AllowExtensions] 및 [DenyExtensions] 섹션

대부분의 파일에는 파일 형식을 나타내는 파일 확장명이 있다. 예를 들어, 일반적으로 Word 문서의 파일 이름은 .doc, HTML 파일 이름은 .htm이나 .html, 일반 텍스트 파일 이름은 .txt로 끝난다. **[AllowExtensions]** 및 **[DenyExtensions]** 섹션에서 URLScan이 차단하는 확장명을 정의할 수 있다. 예를 들어, 웹 사용자가 시스템에서 응용 프로그램을 실행하는 것을 방지하려면 .exe 파일에 대한 요청을 거부하도록 URLScan을 구성할 수 있다.

**[참고]** : UrlScan.ini 파일을 변경할 경우에는 ISA PROXY3 서비스를 다시 시작하여 ISAPI 필터를 다시 로드해야 한다.

- Urlscan의 로그파일이 생성되는 위치: \Winnt\system32\inetrv\urlscan\의 폴더 밑에 urlscan.log라는 로그파일이 생성된다. 그리고 지난 날짜의 로그파일은 자동적으로 urlscan.122701.log와 같이 생성이 된다.
- 현재 Urlscan의 로그파일의 위치를 변경하는 옵션이 없기 때문에 저장공간에 대해서 고려를 해야 한다.

URLScan을 적용하게 되면 웹로그는 아래처럼 로깅되고 상세 로그는 URLScan 로그에 남게된다.

<b>웹로그 예제</b>
2002-03-15 05:45:28 211.111.82.11 - 211.111.113.1 80 GET /<Rejected-By-UrlScan> ~/scripts/root.exe 404 -

<b>URLScan 로그 예제</b>
[03-15-2002 - 14:45:28] Client at 211.111.82.11: URL contains extension '.exe', which is disallowed. Request will be rejected. Site Instance='1', Raw URL='/scripts/root.exe'

Options 섹션	값	URLScan 동작
UseAllowExtensions	0	[DenyExtensions]에 정의된 파일 확장자 요청만 거부한다.
		[DenyExtensions]에 정의되지 않은 파일 확장자 요청은 허용된다.
		[AllowExtensions] 섹션은 무시
	1	[AllowExtensions]에 정의된 파일 확장자 요청만 허용한다.
		[AllowExtensions]에 정의되지 않은 파일 확장자 요청은 거부된다.
		[DenyExtensions] 섹션은 무시

**[DenyHeaders] 섹션**

이 섹션에는 받은 요청에 포함된 경우 거부될 요청 헤더의 목록이 들어 있다. 이 섹션의 항목은 대/소문자를 구분하지 않는다.

클라이언트가 웹 서버에서 페이지를 요청하면 일반적으로 요청에 대한 추가 정보가 들어 있는 일부 HTTP 헤더를 보냅니다. 일반적인 HTTP 헤더는 다음과 같다.

**[DenyHeaders] 섹션**

URLScan이 거부할 HTTP 헤더를 정의한다. URLScan은 이 섹션에 정의된 헤더를 포함하고 있는 요청을 받으면 요청을 거부한다. 이 섹션은 HTTP 헤더 목록으로 구성되어 있으며 각 헤더는 자체 줄에 나타난다. 헤더 이름 다음에는 콜론(:)이 와야 한다.(예: **Header-Name:**).

**[DenyUriSequences] 섹션**

URL에서 특정 문자 시퀀스가 포함된 요청을 차단하도록 URLScan을 구성할 수 있습니다. 예를 들어, 디렉터리 액세스 보안 문제에 자주 사용되는 두 개의 연속된 마침표(..)가 포함된 요청을 차단할 수 있다. 문자 시퀀스를 차단하도록 지정하려면 **[DenyUriSequences]** 구역의 해당 줄에 이 시퀀스를 넣는다.

URLScan.ini 파일은 % 기호와 & 기호가 포함된 요청을 차단하기 때문에 사용자가 "Sales

increase by 100%" 또는 "Bob & Sue are coming to town" 같은 제목 줄이 있는 메시지를 열려고 하면 404 오류 메시지가 표시된다.

이 문제를 해결하려면 **[DenyUrlSequences]** 섹션에서 이 시퀀스를 제거하면 된다. URLScan은 IIS 서비스 응용 프로그램에 대한 HTTP 요청을 필터링을 차단하여 웹 서버를 보호한다. 기본 Urlscan.ini 파일은 그래픽 파일을 포함하는 정적 HTML 파일만 받아들이고 다음과 같은 요청 유형은 거부하도록 구성되어 있다.

- CGI(Common Gateway Interface) .exe 페이지
- WebDAV(World Wide Web Distributed Authoring and Versioning)
- FrontPage Server Extensions
- Index Server
- 인터넷 인쇄
- Server-side Include

### 1.4 URLScan 로그 파일

URLScan은 거부된 요청에 대한 로그를 생성하며 저장위치는 다음과 같다.

```
%windir%\system32\inetutils\urlscan
```

Log files 이름은 URLScan<date>.log 형태로 생성된다.

### 1.5 URLScan의 Request Size 조정(URLScan 2.5 버전)

URLScan에서는 서비스 거부공격에 대한 방어책으로 Request 사이즈를 조정할 수 있다. MaxAllowedContentLength, MaxUrl과 MaxQueryString 속성에서 제한 값을 셋팅할 수 있다.

URLScan.ini에서 다음과 같이 설정을 추가하면 된다.

```
[[RequestLimits]
; The entries in this section impose limits on the length
; of allowed parts of requests reaching the server.
; MaxAllowedContentLength=2000000000(2GB)
; MaxUrl=16384(16KB)
; MaxQueryString=4096(4KB)
```