

2005.5

1	1
1	3
2	8	4
2	7
1	9
1.	9
2.	1 0
3.	1 9
2	2 7
1.	2 7
2.	2 8
3.	3 6
3	3 8
1.	3 8
2.	3 8
3.	4 2
4	4 4
1.	4 4
2.	4 5
3.	4 8
5	WebDAV	5 0
1.	5 0
2.	5 1
3.	5 4
6	(Technote)	6 7
1.	6 7
2.	6 9
3.	6 9
7	(Zeroboard)	7 1
1.	7 1
2.	7 2

3.	7 3
8	SQL Injection	7 4
1.	7 4
2.	7 7
3.	7 9
3	8 1

[1]	().....	9
[2]	1 1
[3]	().....	1 2
[4]	().....	1 3
[5]	().....	1 4
[6] URL	INDEX.HTML	1 5
[7] HTTPD.CONF	1 6
[8]	1 7
[9]	().....	1 8
[10]	().....	1 9
[11]	2 0
[12]	가	2 1
[13] HTTPD.CONF	2 2
[14] HTTPD.CONF	INDEXES	2 3
[15]	가	2 4
[16] HTTPD.CONF	2 5
[17] HTTPD.CONF	INDEXES	2 6
[18]	2 7
[19]	2 8
[20]	2 8
[21]	().....	2 9
[22]	().....	3 0
[23]	가	3 1
[24] /ETC/PASSWD	3 6
[25]	3 6
[26]	().....	3 9
[27] XSS	4 0
[28] XSS	().....	4 0
[29] XSS	(1).....	4 1
[30] XSS	(2).....	4 1
[31]	().....	4 4
[32] ASP	().....	4 6
[33] ASP	().....	4 7

[34]	ASP	가 가 ()	4 7
[35]			4 8
[36]	WEBDAV	()	5 0
[37]	HTTPTEXT.DLL		5 1
[38]	"HTTPTEXT.DLL	"	5 2
[39]			5 3
[40]			5 3
[41]	WEBDAV	1	5 4
[42]	DWORD		5 5
[43]	DISABLEWEBDAV		5 6
[44]	DISABLEWEBDAV	DWORD	5 6
[45]	DISABLEWEBDAV	1	5 7
[46]	HTTPTEXT.DLL		5 8
[47]	HTTPTEXT.DLL		5 9
[48]			6 0
[49]			6 0
[50]	WEBDAV	1	6 1
[51]	DWORD		6 2
[52]	DISABLEWEBDAV	DWORD	6 3
[53]	DISABLEWEBDAV	1	6 3
[54]	HTTPTEXT.DLL		6 4
[55]	HTTPTEXT.DLL		6 5
[56]			6 5
[57]			6 6
[58]		()	6 8
[59]			6 9
[60]		()	7 2
[61]		(SQL INJECTION)	7 5
[62]			7 5
[63]	가		7 6
[64]	SQL INJECTION	가	7 6
[65]	SQL INJECTION		7 7

1

1

가

가

가

가 2004

2005 1 7

2 1

가

가

가

가

가

가

8

가

가

2

8

1.

- ‘httpd.conf’ , ‘Indexes’ ON (IIS ()),
- 가 가 .

2.

- ‘..’ ,
- URL ‘../’
/etc/passwd .
- , 가 .

3.

-
- 가 PC .

4.

- .php, .jsp
- 가

5. WebDAV

- WebDAV
가 가 , WebDAV
- 가 WebDAV ,

6. (Technote)

- CGI 가 ‘|’
-
- ‘ , ‘Perl’

7. (Zeroboard)

- PHP PHP ‘ , ’
-

- ‘ ‘ , ‘PHP’가

8. SQL Injection

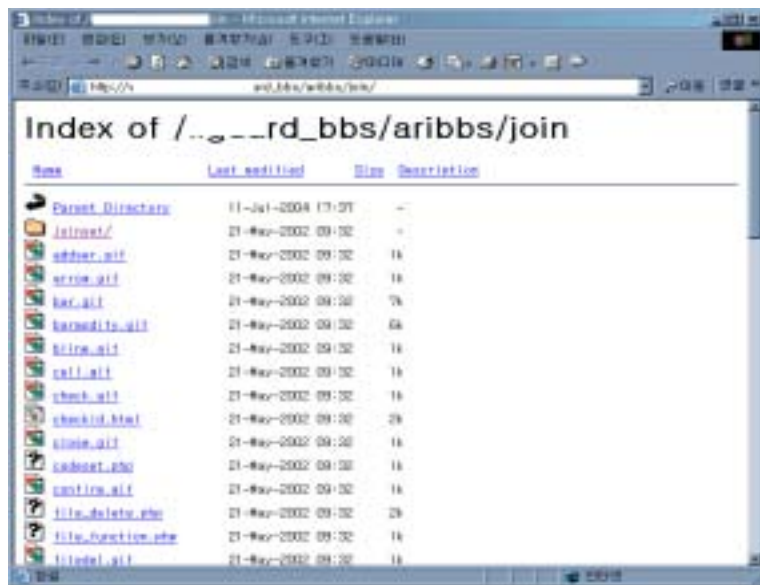
- (URL) ID (‘ “) SQL
- 가 SQL ,

2

1



1.



[1] ()

[1] URL .

. [1]

, 가 ,
.

2.

○ (WebRoot)

: <http://www.sample.co.kr/>
가 URL , <http://www.sample.co.kr/file/>
file/
file/
(
'/').

:

(가).

○

○ (WebRoot)

가.

○

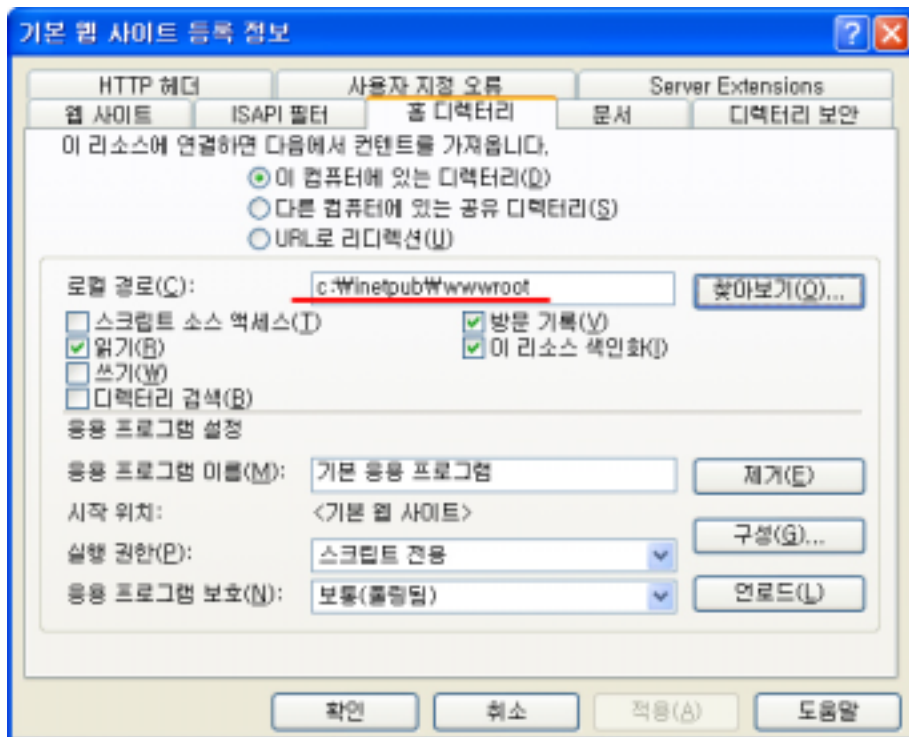
IIS

.

○

[] => [] => [] ([, ' ,
) , ['가 , IIS
,

○

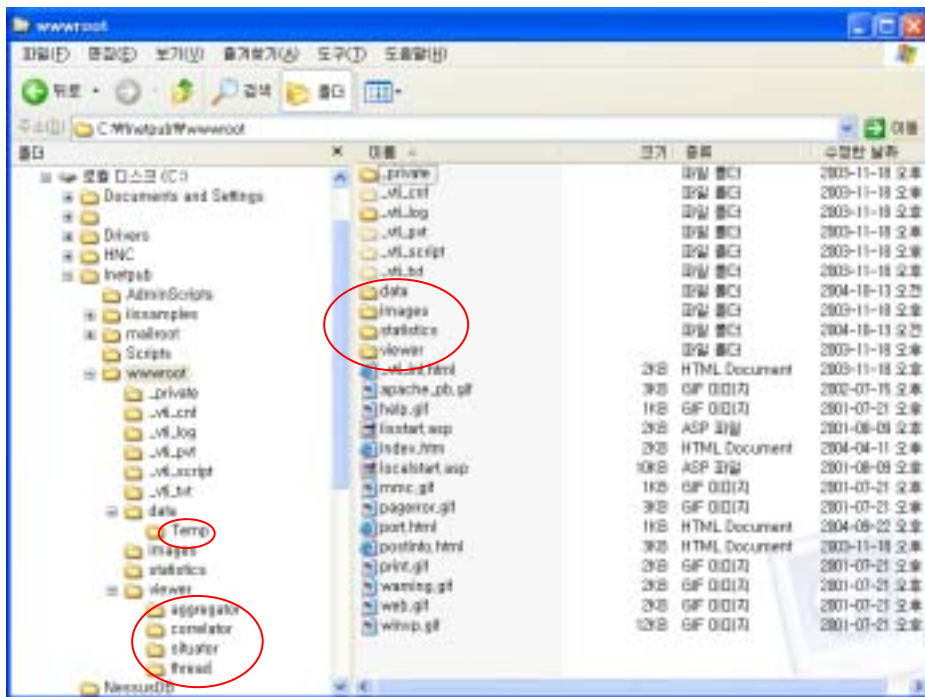


[2]

○ [2] ,
([2] 'c: \ inetpub \ wwwroot').

○ IIS 'c: \ inetpub \ wwwroot'가

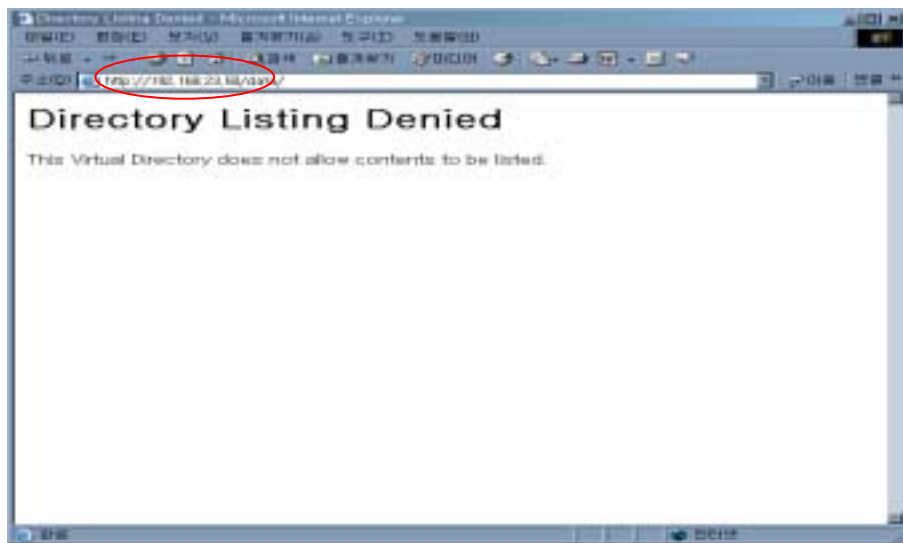
○ 가
([3]).



[3] ()

- [3] , c: \ inetpub \ wwwroot data, images, statistics, viewer 가 Temp, aggregator, correlator, situater, thread 가 . ('/').

URL: <http://servername.com> ,
<http://servername.com/data/>
<http://servername.com/data/Temp/>
<http://servername.com/images/>
<http://servername.com/statistics/>
<http://servername.com/viewer/aggregator/>
<http://servername.com/viewer/correlator/>.

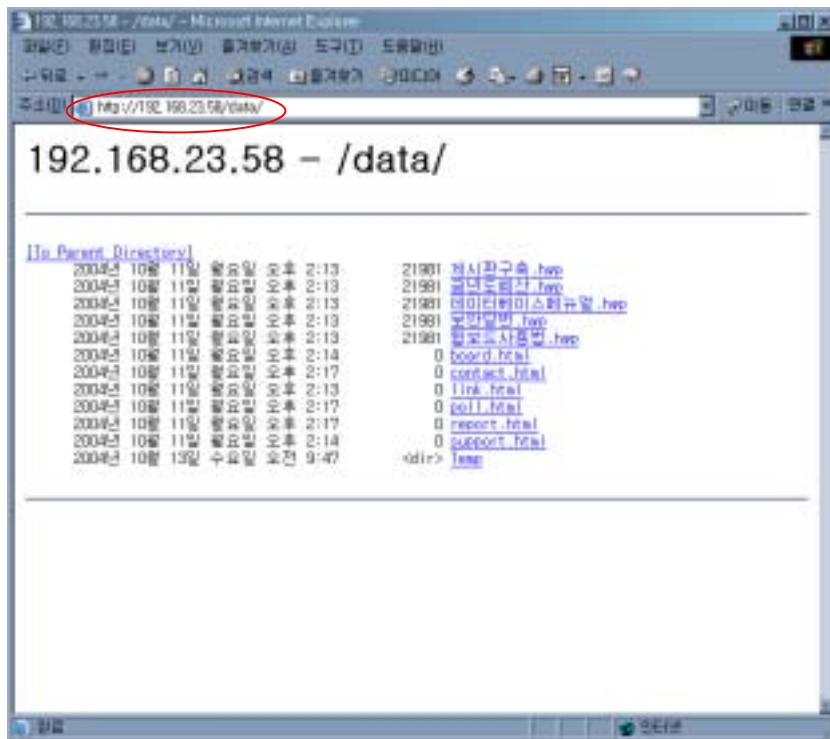


[4] ()

○ [4]

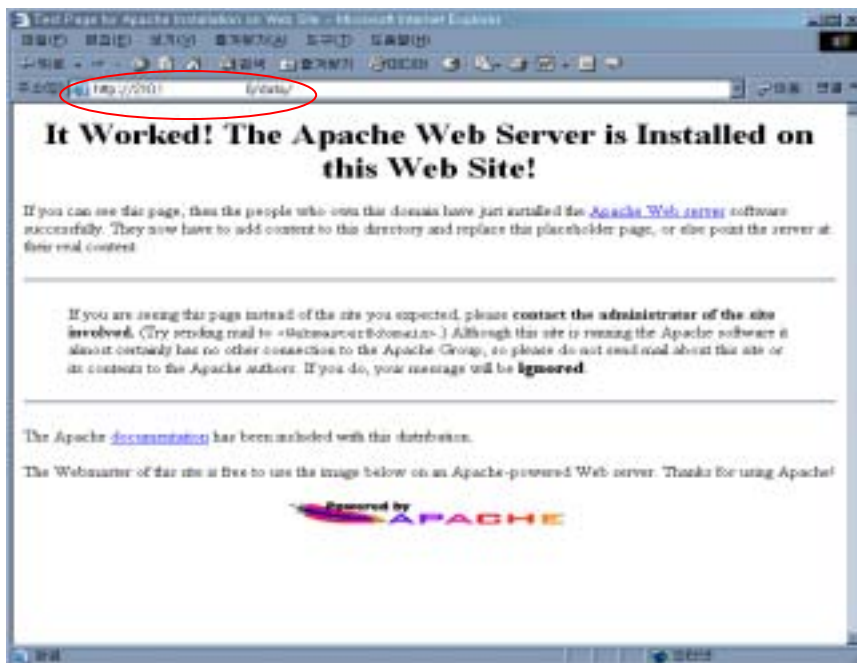
○ [4]

○ [5]



[5] ()

[5] data/ html
Temp/ 가
:
(html)가
가 index.html(index.jsp, index.php,
index.asp, index.htm) main.html(main.jsp, main.php, main.asp,
main.htm) , URL
index.html main.html () 가
 , <http://www.sample.com/file/> <http://www.sample.com/file/index.html>
[6]



[6] URL index.html

.

○ (apache)

httpd.conf 가 httpd.conf

/etc/httpd/conf/httpd.conf
 /etc/apache/httpd.conf
 /usr/apache/conf/httpd.conf
 /usr/local/apache/conf/httpd.conf
 /usr/lib/apache/conf/httpd.conf

○ 가 5가

apache httpd.conf

- httpd.conf DocumentRoot

([7]).

```

# 127.0.0.1 is the TCP/IP local loop-back address. often named localhost. Your
# machine always knows itself by this address. If you use apache strictly for
# local testing and development, you may use 127.0.0.1 as the server name.
#
#ServerName new.host.name

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#DocumentRoot "/var/apache/htdocs"

#
# Each directory to which Apache has access, can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# permissions.
#
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>

```

[7] httpd.conf

- * : httpd.conf ‘#’ .

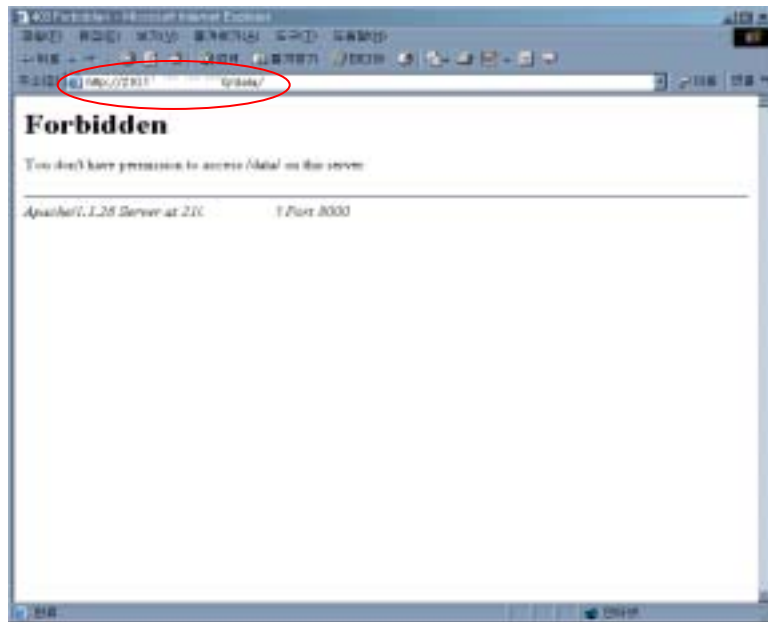
- [7] DocumentRoot /var/apache/htdocs

 /var/apache/htdocs/ .

- 가 ‘ls’

 ls -F ,
 ‘/’ 가 [8] .

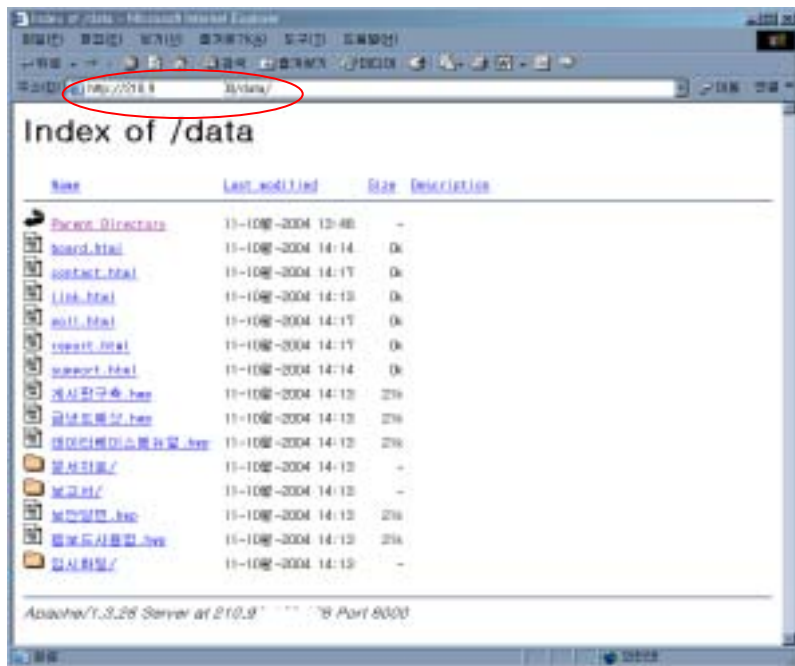
○ [9]



[9] ()

○ [9]

○ [10]



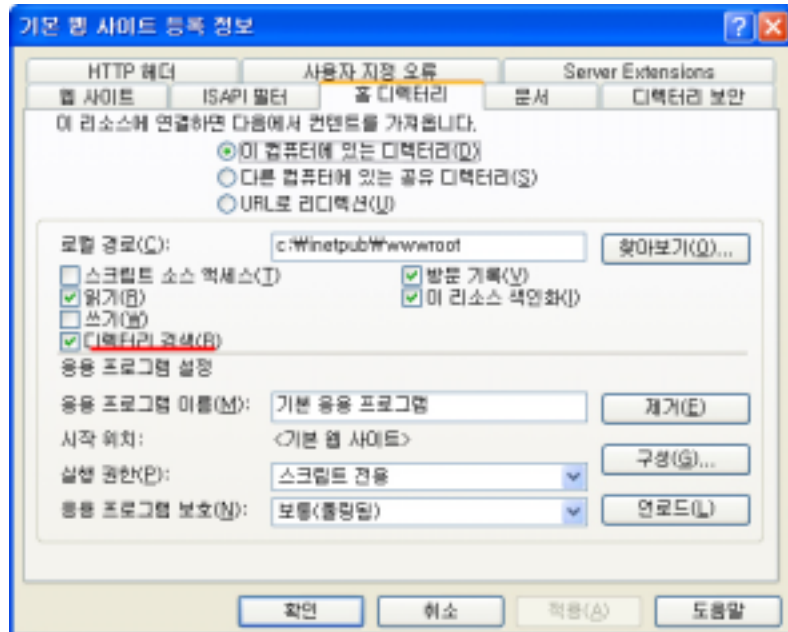
[10] ()

: (html)가

가 index.html(index.jsp, index.php, index.asp, index.htm) main.html(main.jsp, main.php, main.asp, main.htm) , URL index.html main.html () 가 , <http://www.sample.com/file/sample.com/file/index.html> ([6]).

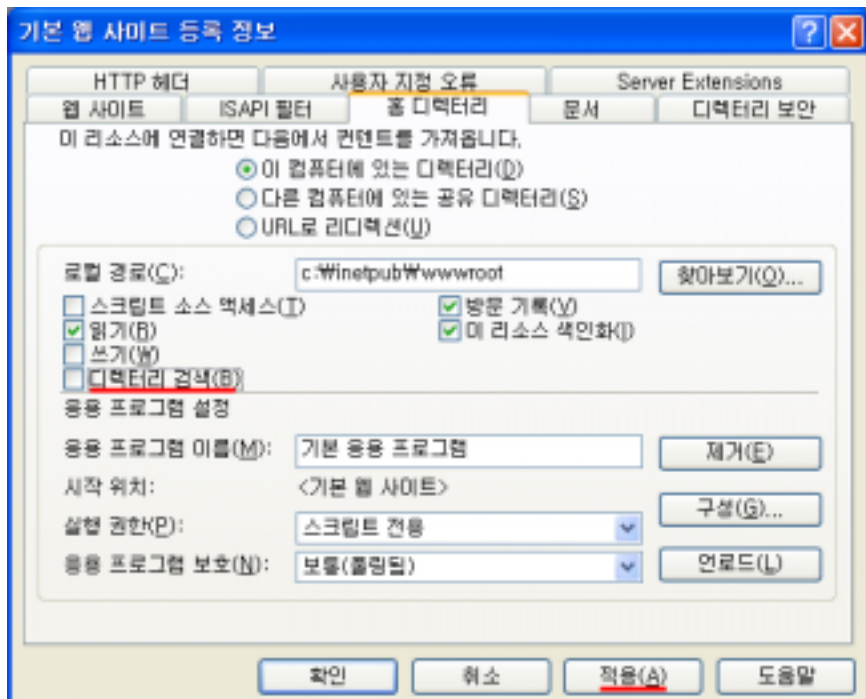
3.

가.



[11]

- [] => [] [] ([, ' ,]) , [] '가 .
- ' , , , , [11] .
- [11] ' (B)' 가 , [12] .



[12]

가

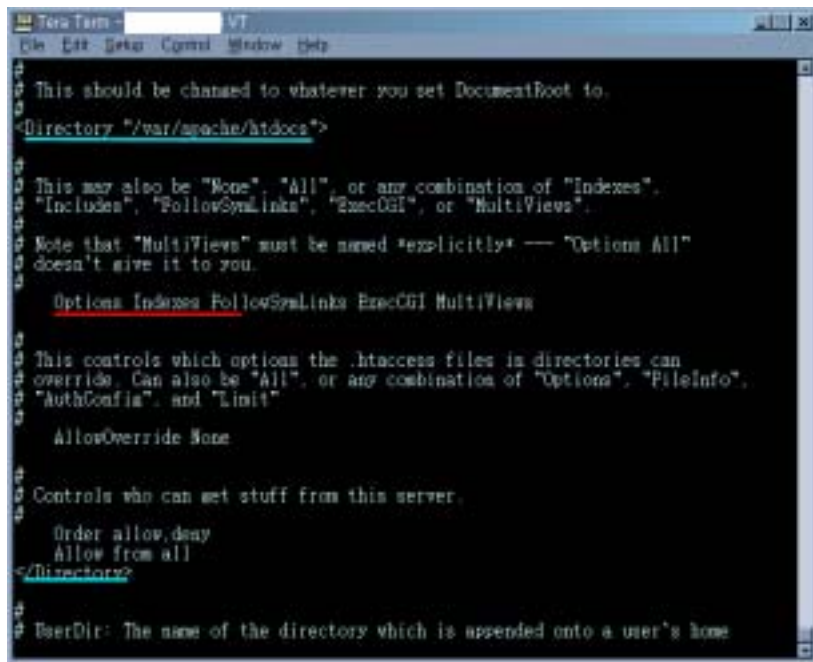
:
[12]

.

○ httpd.conf 가 .
httpd.conf

```
/etc/httpd/conf/httpd.conf
/etc/apache/httpd.conf
/usr/apache/conf/httpd.conf
/usr/local/apache/conf/httpd.conf
/usr/lib/apache/conf/httpd.conf
```

○ 가 5가
 apache httpd.conf



[13] httpd.conf

○ [13] Options Indexes
 가 . Indexes
 Indexes
 : Options
 [13] Directory "/var/apache/htdocs"
 Options .
 Options Indexes가
 .

```

#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/var/apache/htdocs">
#
# This may also be "None", "All", or any combination of "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
Options FollowSymLinks ExecCGI MultiViews
#
# This controls which options the .htaccess files in directories can
# override. Can also be "All", or any combination of "Options", "FileInfo",
# "AuthConfig", and "Limit"
#
AllowOverride None
#
# Controls who can get stuff from this server.
#
Order allow,deny
Allow from all
</Directory>
#
# UserDir: The name of the directory which is appended onto a user's home

```

[14] httpd.conf Indexes

: httpd.conf

/etc/rc.d/init.d/httpd restart

kill

kill PID 'ps -ef | grep httpd'

kill

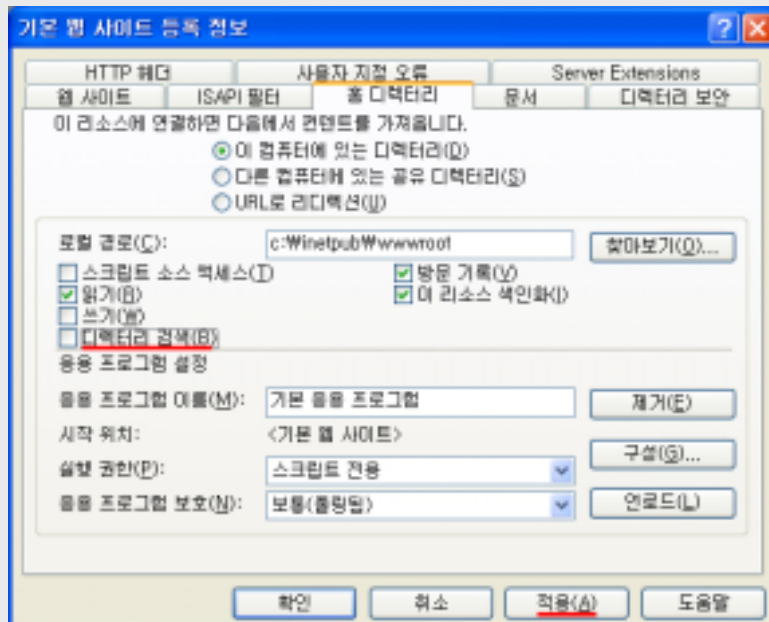
rc

/etc/rc3.d/S50apache start

가 , 가
rc

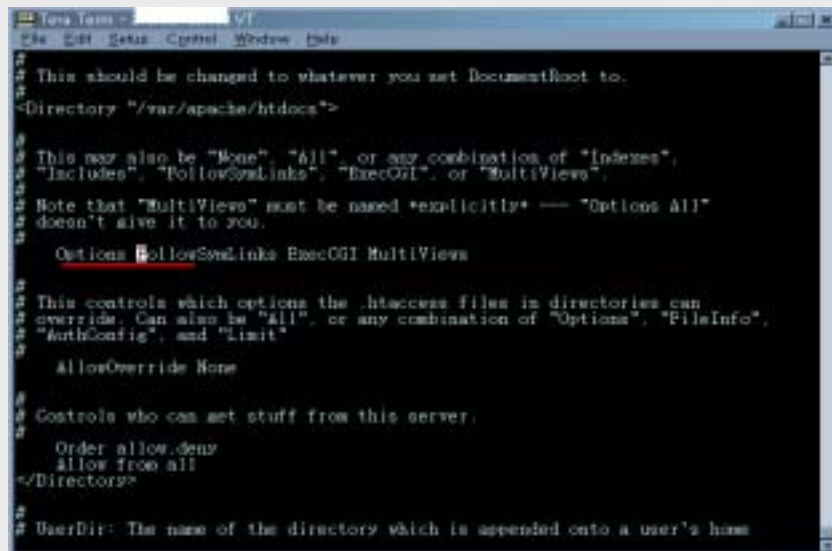
가.

1. [] => [] [] ([, ,
=> '가 .
2. ' , , , .



[15] 가

3.



```
# This should be changed to whatever you set DocumentRoot to.
<Directory "/var/apache/htdocs">

# This may also be "None", "All", or any combination of "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
# Options FollowSymLinks ExecCGI MultiViews

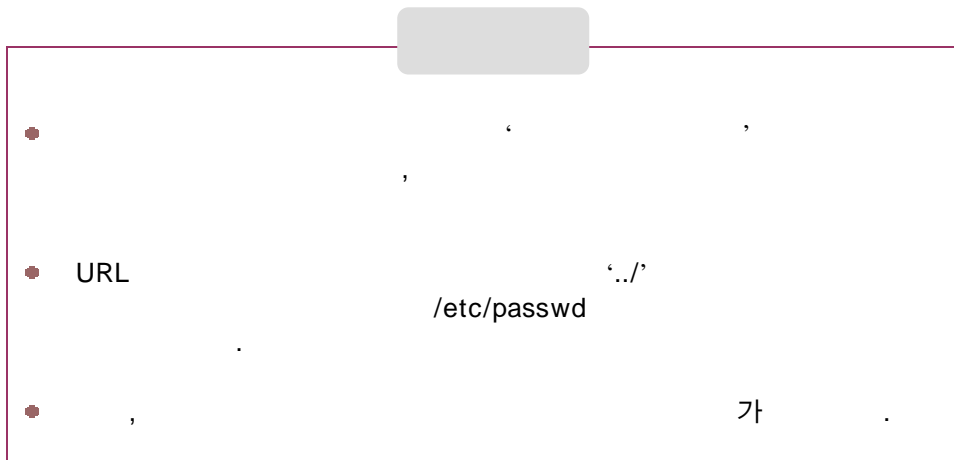
# This controls which options the .htaccess files in directories can
# override. Can also be "All", or any combination of "Options", "FileInfo",
# "AuthConfig", and "Limit"
# AllowOverride None

# Controls who can set stuff from this server.
# Order allow,deny
# Allow from all
</Directory>

# UserDir: The name of the directory which is appended onto a user's home
```

[17] httpd.conf Indexes

2



1.

가
/etc/passwd
가

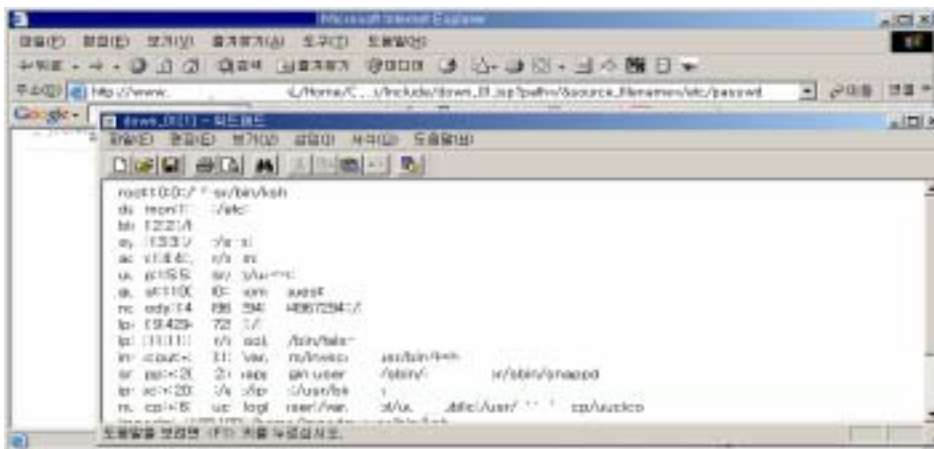
순위	제목	URL	내용
1	가	http://www.google.com	가
2	가	http://www.google.com	가
3	가	http://www.google.com	가
4	가	http://www.google.com	가
5	가	http://www.google.com	가
6	가	http://www.google.com	가
7	가	http://www.google.com	가
8	가	http://www.google.com	가
9	가	http://www.google.com	가
10	가	http://www.google.com	가

[18]



[19]

[18, 19, 20] “ ” /etc/passwd



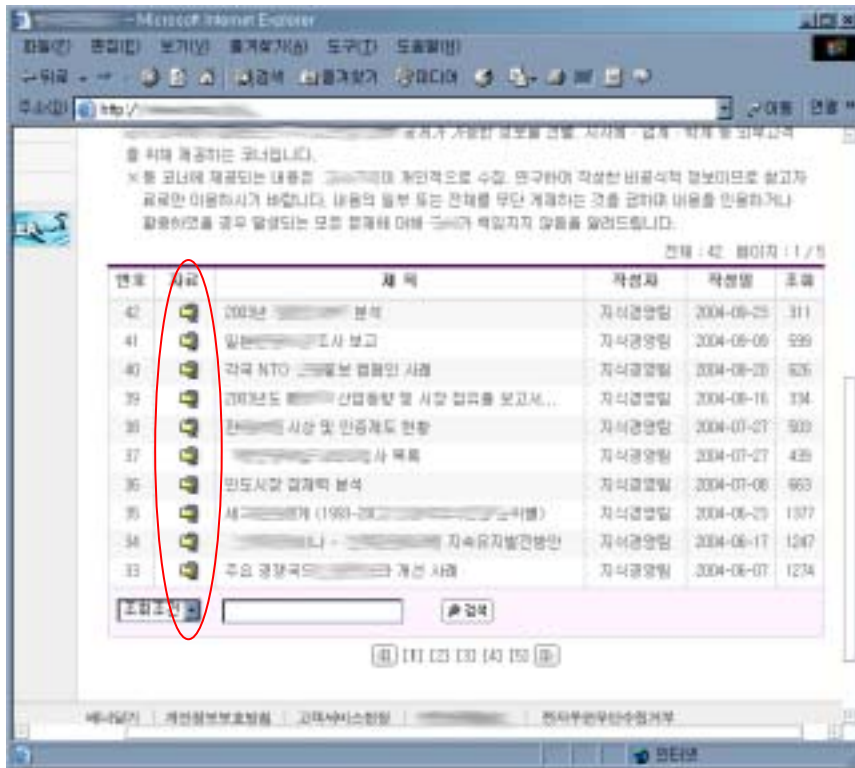
[20]

2.

가.

○

([21]).



[21] ()

○ _____ 가 _____ , _____ 가 _____ , _____ .

_____ .

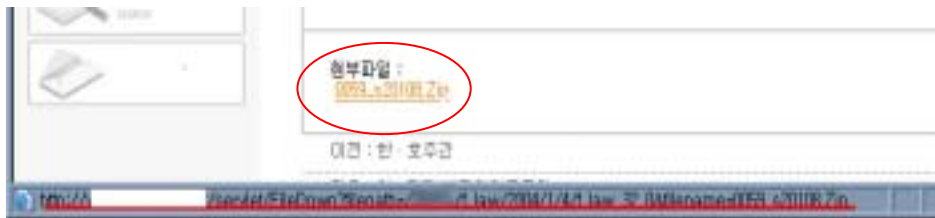
2가

_____ 가 _____ URL _____ . 2가 _____ .

< URL >
<http://servername.com/test/filedown.down?file=3.hwp&path=download>

URL

○ , ([22] 0059_s20108.Zip)
가
가 .

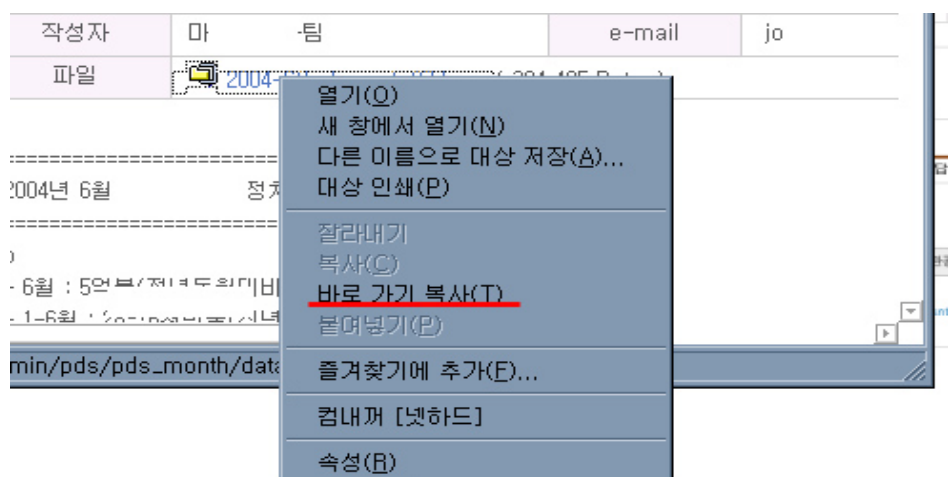


[22] ()

○ , 가 가

[23]

가 (T)



[23]

가

가



○ _____ URL _____
 _____ 가 _____

○

http://servername/.../ ? 1= & 2=

○

* : _____ /etc/passwd '../'
 _____ /etc/passwd

 _____ '../'

Case 1

< >

http://servername.com/pr/download.asp?filename=_____ .hwp

< >

☐ filename _____ ,
 _____ '../'
 _____ ,
 /etc/passwd _____

<http://servername.com/pr/download.asp?filename=/etc/passwd>
<http://servername.com/pr/download.asp?filename=../../../../../../../../../../../../etc/passwd>

☐ download.asp

<http://servername.com/pr/download.asp?filename=../pr/download.asp>
<http://servername.com/pr/download.asp?filename=../../pr/download.asp>
<http://servername.com/pr/download.asp?filename=../../../pr/download.asp>

Case 2

< >

http://servername.com/includes/download.php?sub_path=upfiles&filename=_____.doc

< >

☐ /etc/passwd .

http://servername.com/includes/download.php?sub_path=../../../../../../../../../../../../etc&filename=password
http://servername.com/includes/download.php?sub_path=upfiles&filename=../../../../../../../../../../../../etc/passwd

☐ includes/download.php .

http://servername.com/includes/download.php?sub_path=includes&filename=download.php
http://servername.com/includes/download.php?sub_path=upfiles&filename=../includes/download.php
http://servername.com/includes/download.php?sub_path=upfiles&filename=../../includes/download.php

Case 3

< >

http://servername.com/servlet/Down?path=/DATA/docu/2004/03/13&name=_____.hwp

< >

○ path /DATA/ (/)

‘/../.’ ‘/DATA/..’

<http://servername.com/servlet/Down?path=/../../../../../../../../../../../../etc&name=passwd>
<http://servername.com/servlet/Down?path=/DATA/../../../../../../../../../../../../../../../etc&name=passwd>

Case 4

< >

http://servername.com/include/down.jsp?upfile=_____.hwp&dir=/data

< >

○ down.jsp

<http://servername.com/include/down.jsp?upfile=down.jsp&dir=/include>

○ /etc/passwd

<http://servername.com/include/down.jsp?upfile=passwd&dir=/etc>
<http://servername.com/include/down.jsp?upfile=passwd&dir=/data/../../../../../../../../etc>
<http://servername.com/include/down.jsp?upfile=passwd&dir=../../../../../../../../etc>

Case 5

< >

http://servername.com/webapp/data_07.asp?fn=c:\upload\200408_.exe

< >

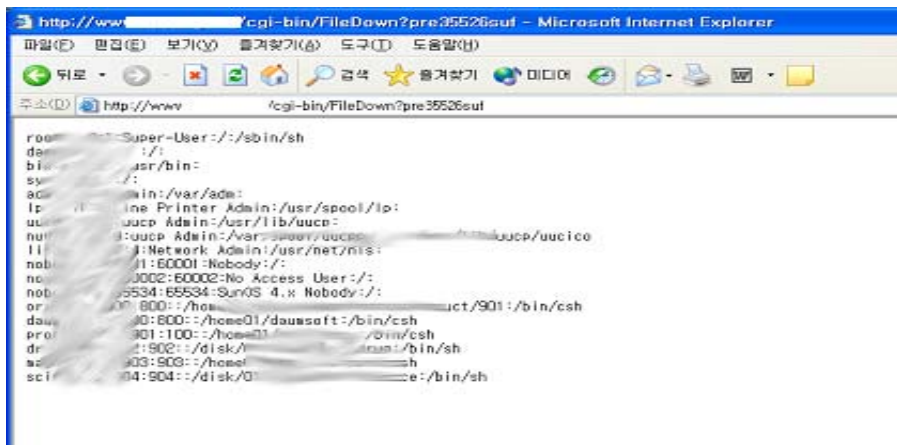
○

http://servername.com/webapp/data_07.asp?fn=c:\inetpub\wwwroot\webapp\data_07.asp

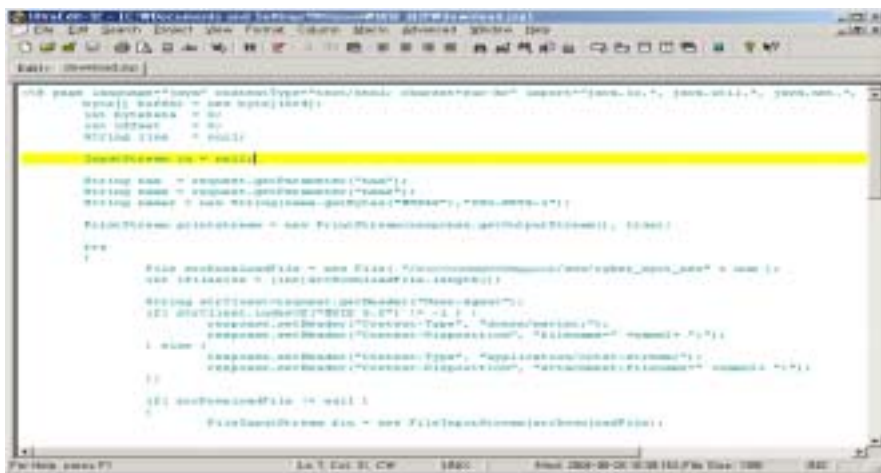
() 가

가

가 , , 가 ([24, 25]).



[24] /etc/passwd



[25]

3.

○ “..”, “/”, “ \ ”

○ (

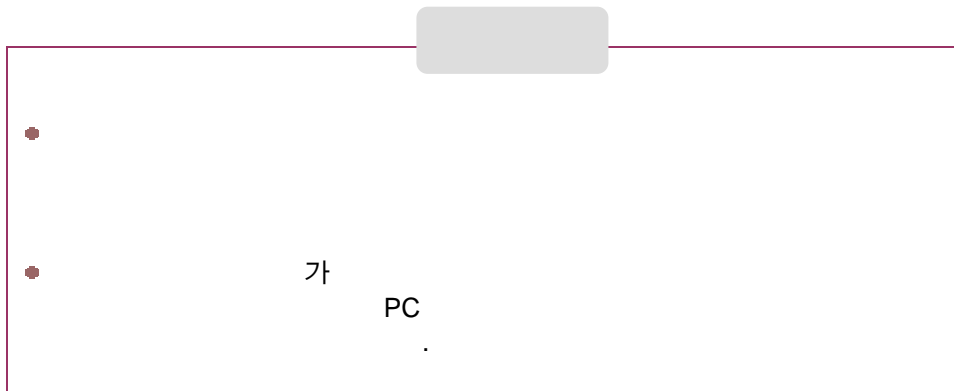
).).



1. “..”, “/”, “ \ ”

2. URL

3



1.

(XSS: Cross Site Script)

가

가

VBScript

가

XSS

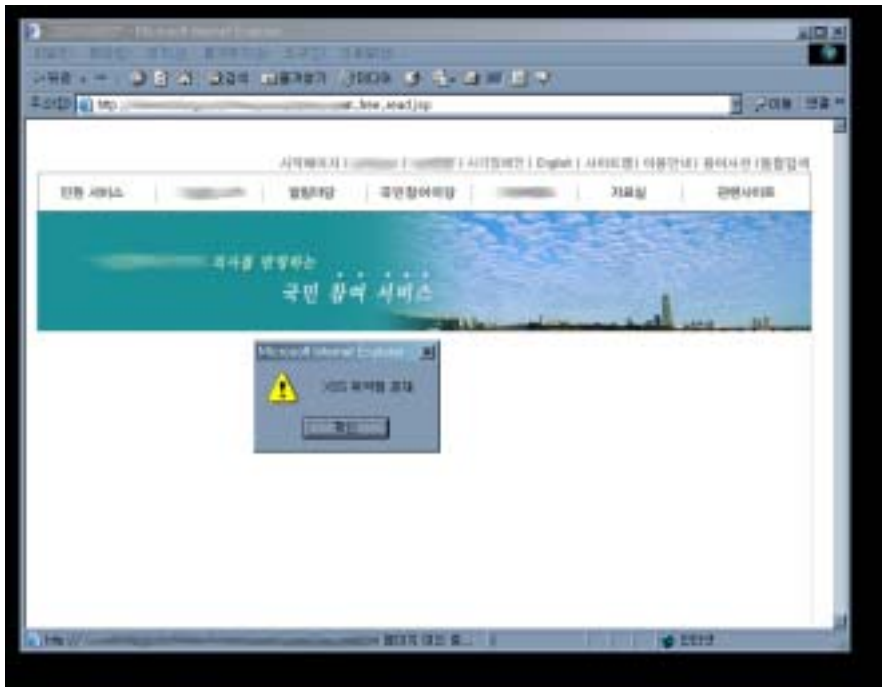
2.

가.

○ , , , , .

○ ‘XSS’

XSS



[27] XSS

○ [28]



[28] XSS ()

○ ,

[29]

XSS

여론광장

여론광장은 []에 대한 고객여러분의 다양한 의견을 게재할 수 있는 게시판으로서
 심정의 고객님만 게재할 수 있으며, 별도의 답변이 있는 게시판이 아닙니다.
 답변이 필요한 경우에는 [Q&A] 또는 [민원광장]을 이용해 주시기 바랍니다.

구

• 성명 | [] • 등록일 | 2004-10-18 • 조회 | 1

• 제목 | 테스트

원장

보상제도

<script>alert('XSS 취약점 존재');</script>

• 이전 | 마지막은 []에...

• 다음 |

답변 수정 인쇄 목록

[29] XSS (1)

○ [30]

시민참여 자유게시판

• 이곳은 시민여러분의 글을 자유롭게 게시하는 공간으로 시에서는 글에대한 답변은 하지 않습니다.
 • 본 란을 통하여 게시한 각종 의견 등에 대하여는 민원사무로 접수되지 아니하므로, [민원사무]를 통하여 신청하시기 바랍니다.
 • 광고성 글 및 사실이 확인되지 않은 허위성글에 대해서는 사전 예고 없이 관리자에 의해 삭제됩니다.

제목 | 테스트

작성자 | [] 등록일 | 2004-10-18 조회수 | 1

script>alert('XSS 취약점 존재');script

다름글 삭제 수정 목록

[30] XSS (2)

.

○ . XSS

가 .

3.

○ XSS . 가 가

input

○ script

< → <
> → >
(→ (
) →)
→ #
& → &

○ 가

○ .



1.

가 .

✓
✓

가

✓

2.

4

-
- 가
- .php, .jsp

1.

- ‘ , 가 가 .



[31] ()

[31]

[31] , 'cat /etc/passwd'
passwd 가
.

2.

가 .

가 가 .

가.

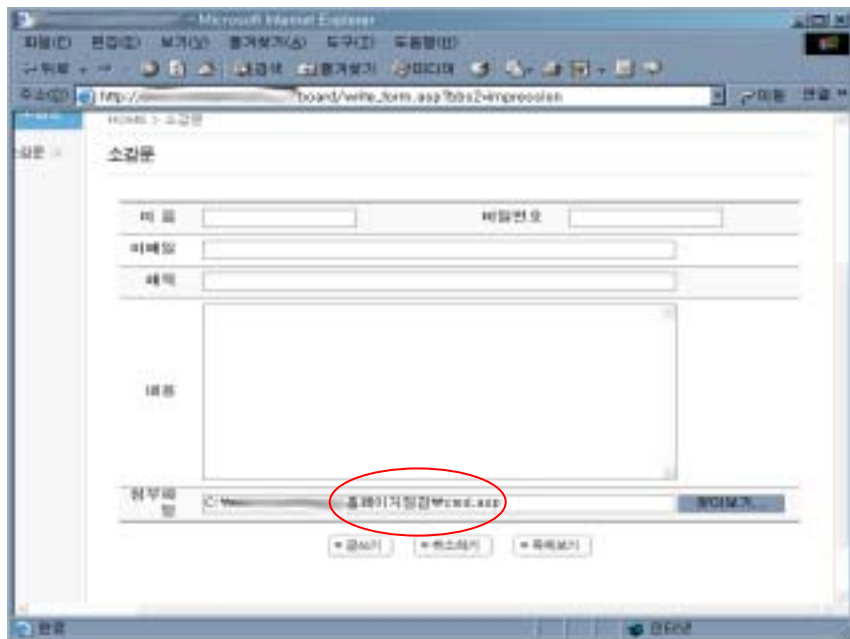
○ 가 가 , ,
.

○ , ,
.
, ,
.

. 가 가

○ php, php3, asp, jsp, cgi, inc, pl 가 ,
, 가
가 가
.

○ 가 가 [32] php, php3,
asp, jsp, cgi, inc, pl .



[32] asp ()

- 가 .
- [33] 가 . [33]
cmd.asp .



[33] asp ()

○



[34] asp 가 가 ()

○ [34] . cmd.php

가 php, php3, asp, jsp, cgi, inc, pl
가

[34]

○

가

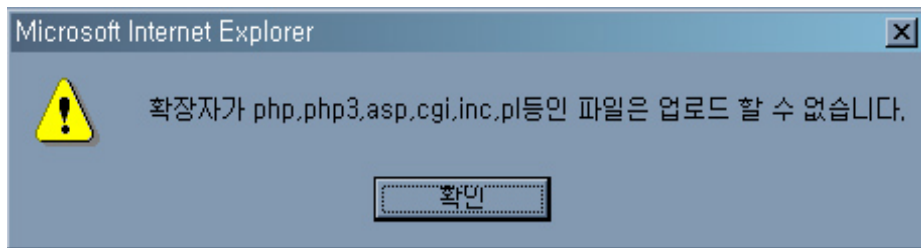
3.

○

()

○

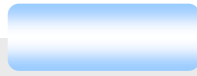
가 php, php3, asp, jsp, cgi, inc, pl
[35]



[35]

: 가 ,
Php, phP, AsP, jSp
가 “- -.txt.asp” 2

○



1. (가 : php, php3, asp, jsp, cgi, inc, pl)
2. (가)

5 WebDAV

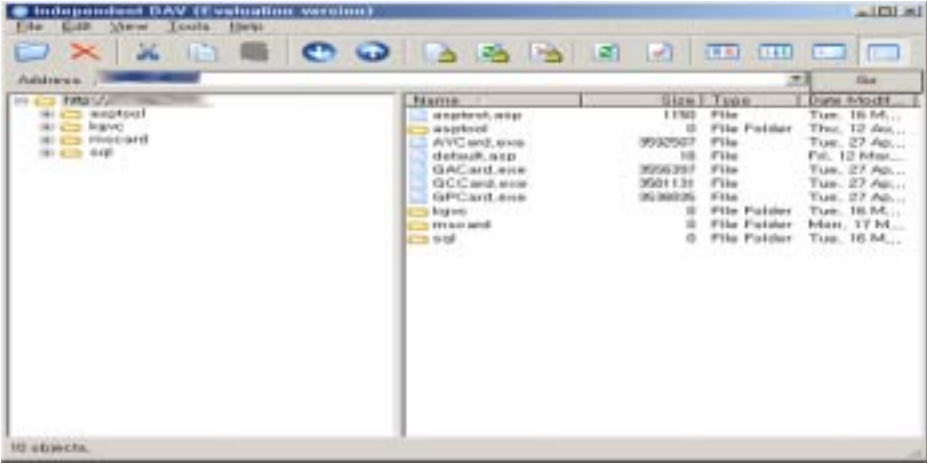
- 가 가 , WebDAV
- 가 WebDAV ,

1.

(WebDAV) “Web Distributed Authoring and Versioning”
가

IIS

가 .



[36] WebDAV ()

. [36]

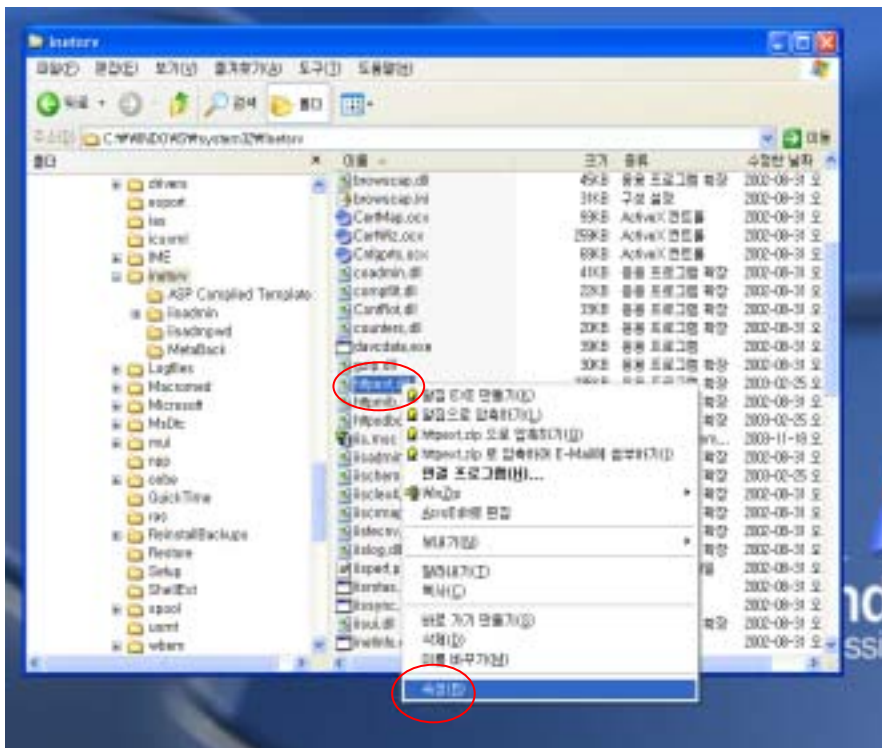
2.

가. WebDAV

- ```

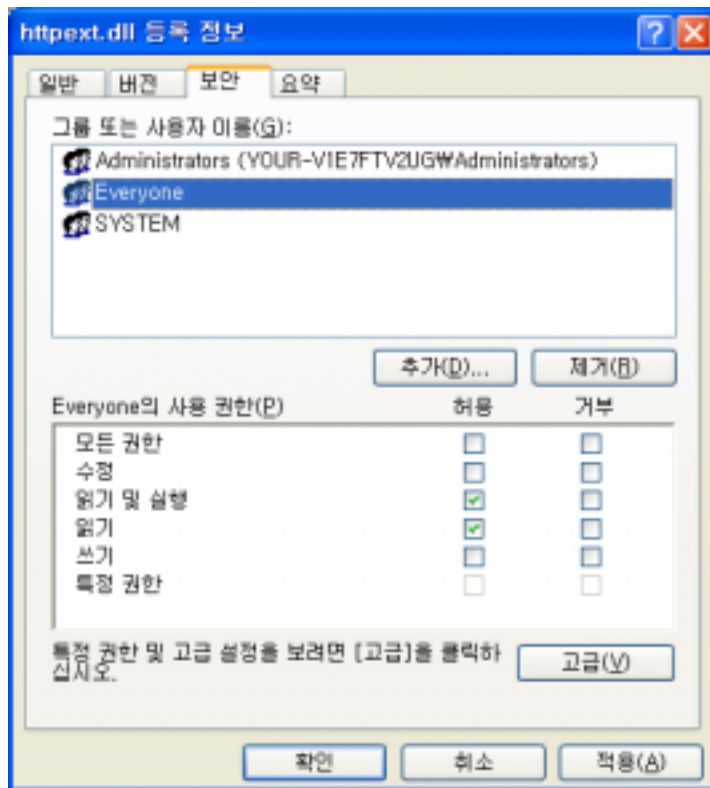
○ httpext.dll
 \ winnt \ system32 \ inetsrv \ httpex
t.dll \ WINDOWS \ system32 \ inetsrv \ httpex
t.dll .
○ . [37]

```



[ 37] httpext.dll

- [ 38] 'httpext.dll' , 'Everyone' 가 .

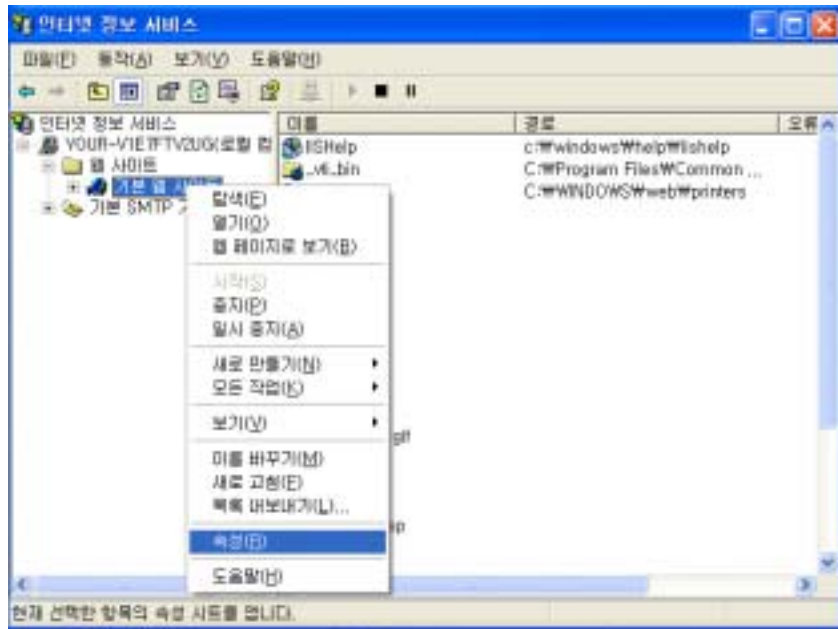


[ 38] “httpext.dll ”

: Everyone httpext.dll  
가 가 .

- [ ] => [ ] [ ] ( [ ]

1) [ 39 ] '가 .



[ 39 ]

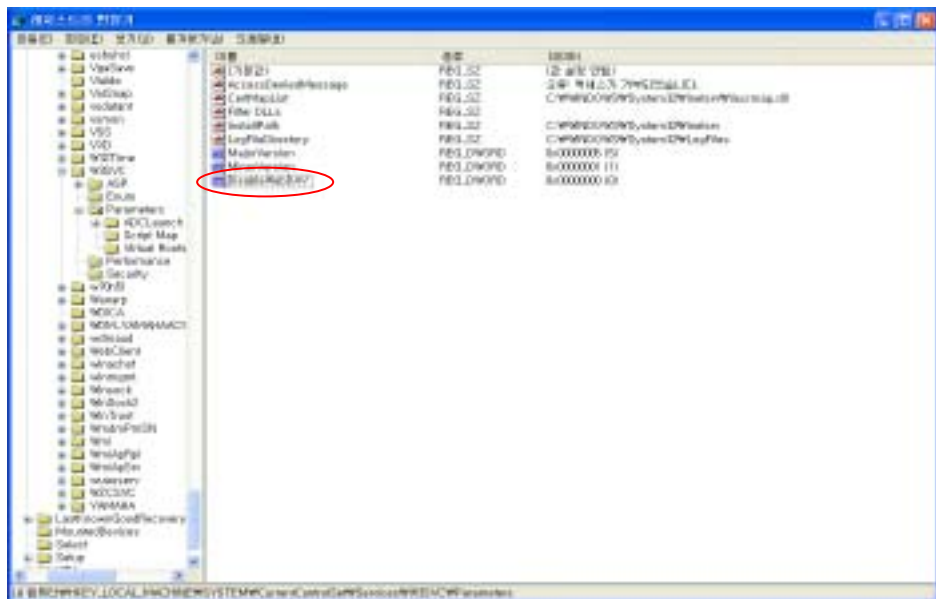


[ 40 ]



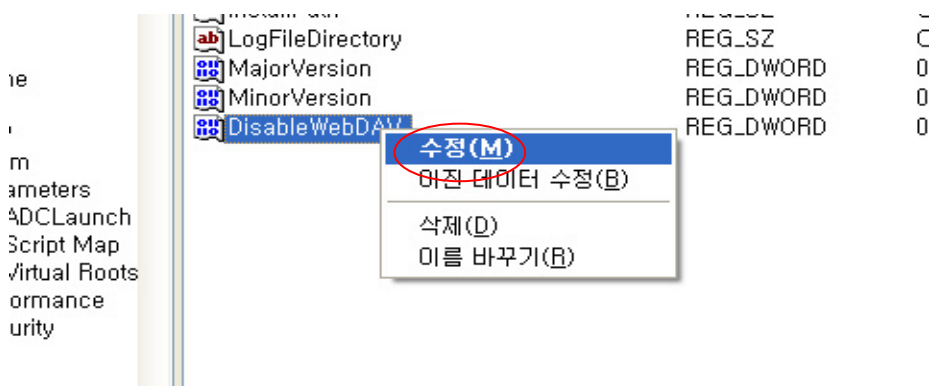


○ [ 43] 'DisableWebDAV' ( )



[ 43] DisableWebDAV

○ [ 44] 'DisableWebDAV'



[ 44] DisableWebDAV DWORD

○ ' ' [ 45] 'DWORD' ,

DWORD 값 편집

값 이름(N):  
DisableWebDAV

값 데이터(V):  
1

단위

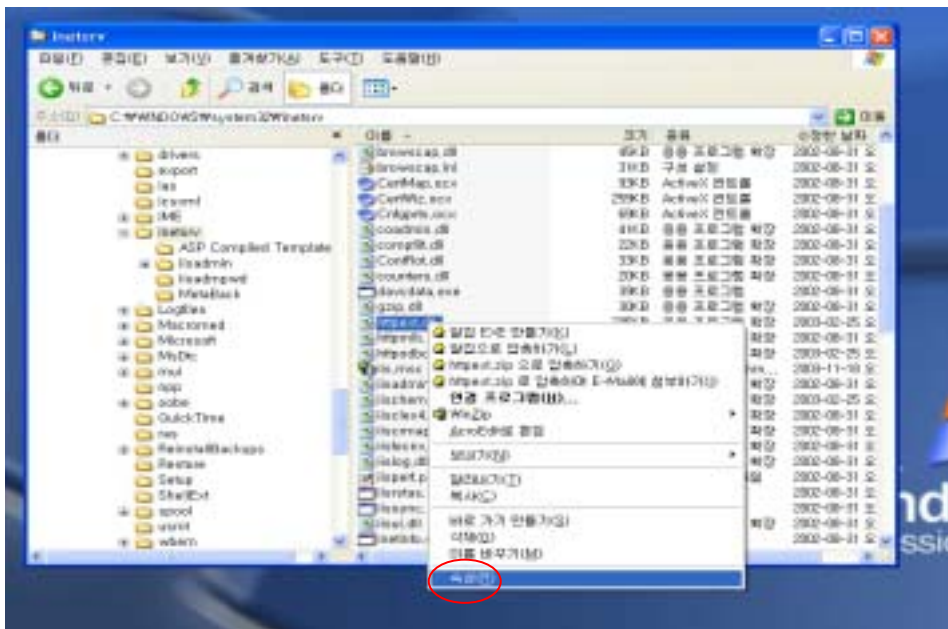
☒ 16진수(H)  
☐ 10진수(D)

확인 취소

○ \_\_\_\_\_

2

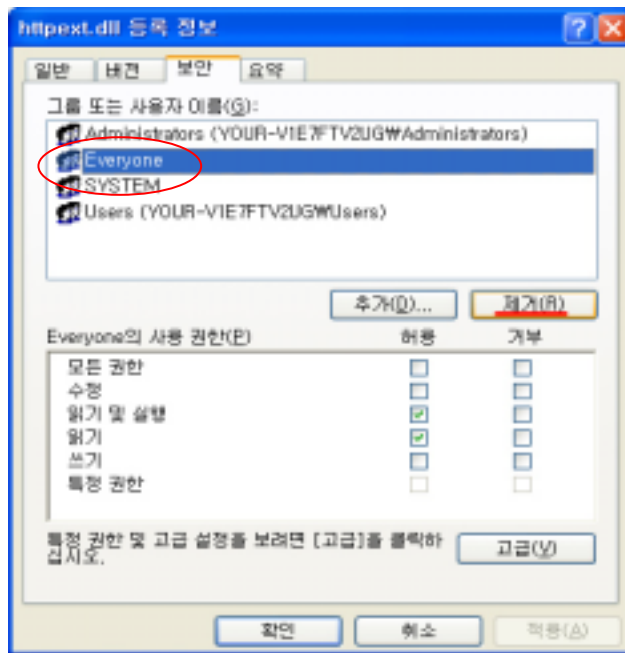
```
○ Httpext.dll \ winnt \ system32 \ inetsrv \ httpext.dll
 \ WINDOWS \ system32 \ inetsrv \ httpext.dll
 . [46]
```



[ 46] httpext.dll

○ [ 47] 'httpext.dll', Everyone  
Everyone



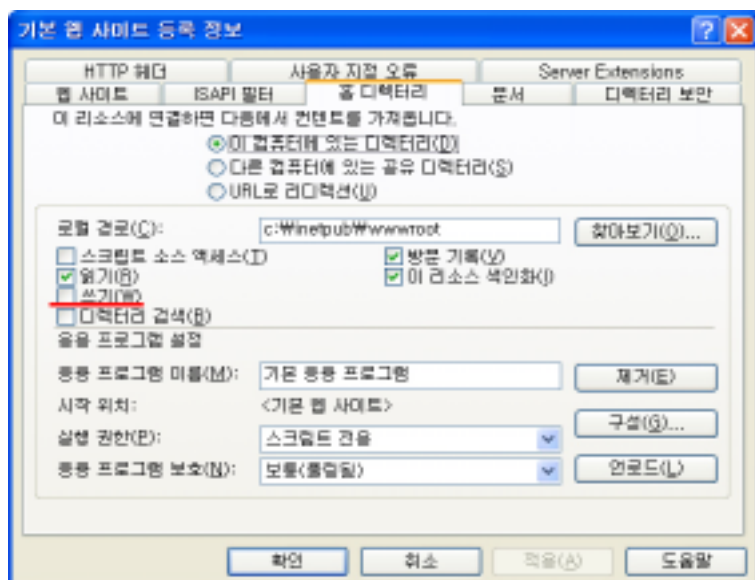
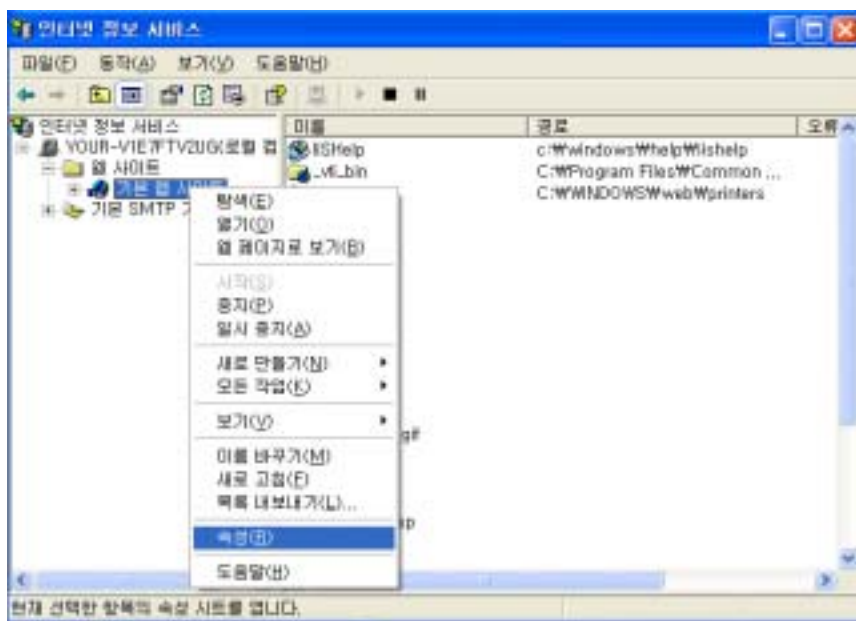


[ 47] httpext.dll

.

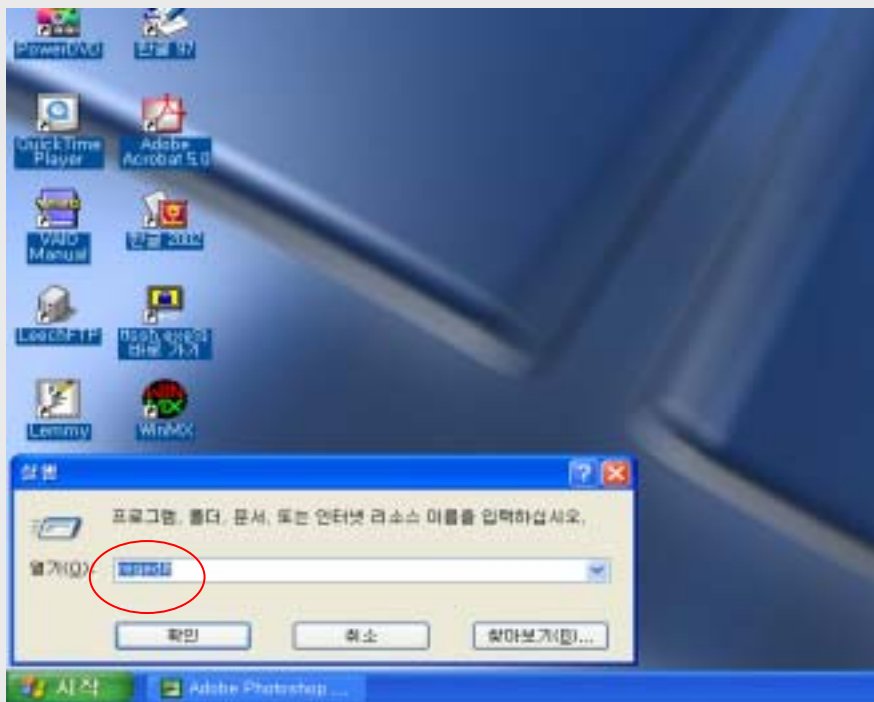
.

○ [ ] => [ ] [ ] ( [ , ' , ] )  
 ([ 48] ) , '가 .



가. (WebDAV) ( )

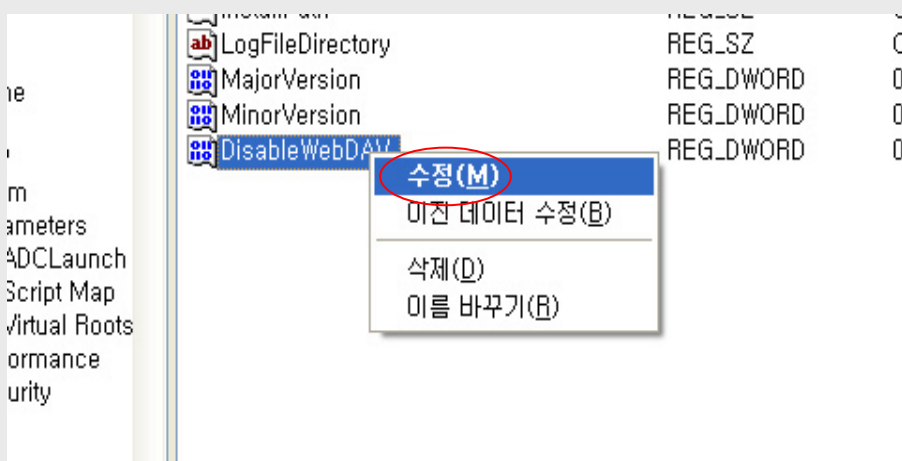
1. [ 50] 'regedit'



[ 50] WebDAV 1

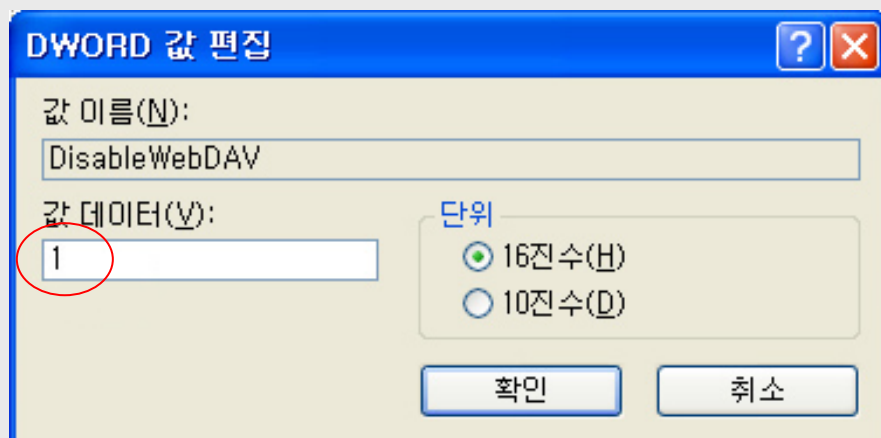
2. 'regedit'  
'HKEY\_LOCAL\_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W3SVC \ Parameters'





[ 52] DisableWebDAV DWORD

4. [ 53] 'DWORD' (V)  
'1'

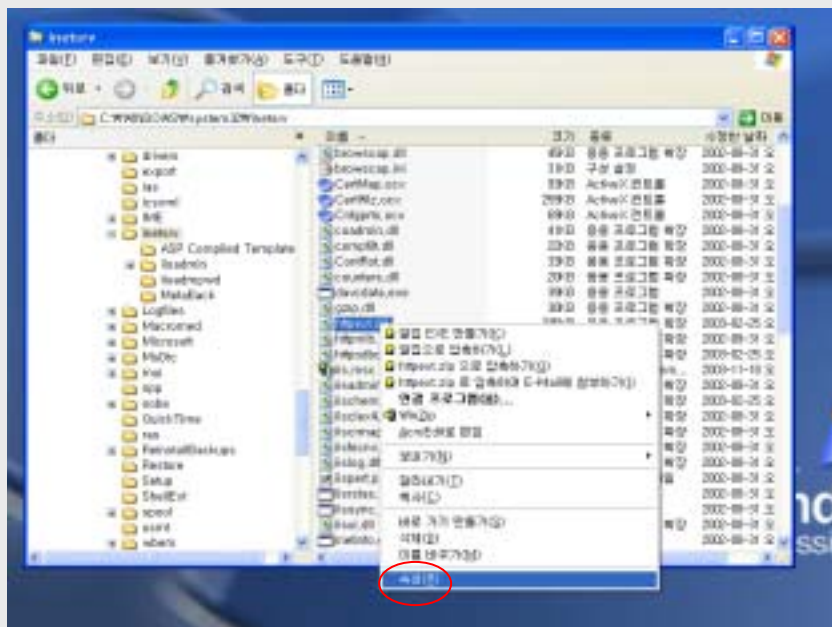


[ 53] DisableWebDAV 1

5. '\_\_\_\_\_'

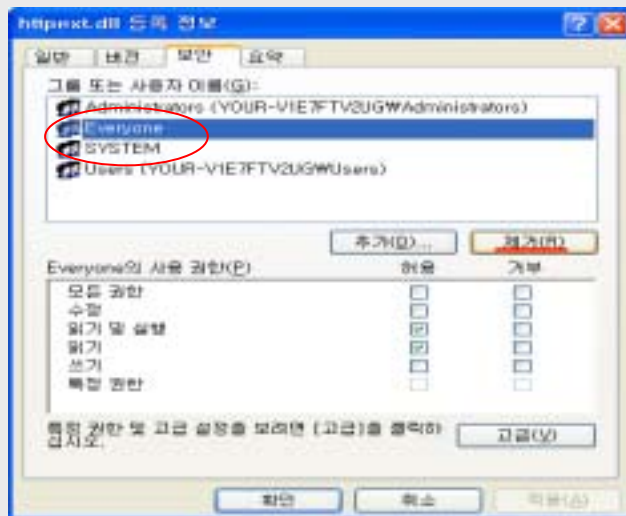
. httpext.dll Everyone

1. Httpext.dll \ winnt \ system32 \ inetsrv \ httpext.dll  
 \ WINDOWS \ system32 \ inetser \ httpext.dll  
 . [ 54]



[ 54] httpext.dll

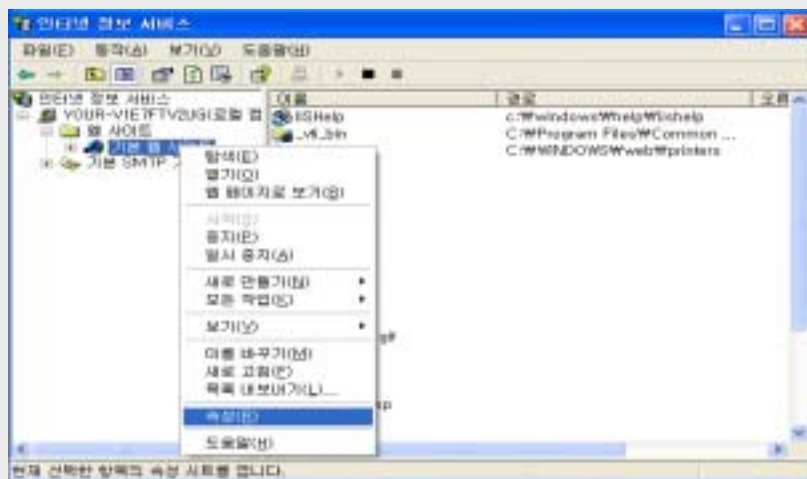
2. [ 55] 'httpext.dll',  
 Everyone  
 Everyone



[ 55] httpext.dll

.

1. [ ] => [ ] [ ] ( [ , , ] ) [ ] ([ 56] ) , '가 .



[ 56]

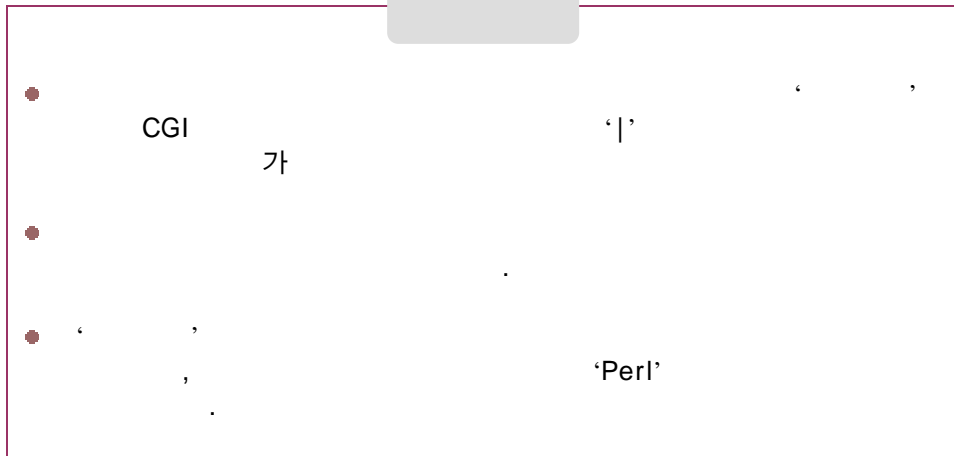
2. ([ 57] ).

[ 57]





## 6 (Technote)



### 1.

✓

CGI(print.cgi, lib-5.cgi)

, , .  
가 가 가

(Sucurityfocus.com) 2000 12 5

가 , .  
가 ([www.ncsc.go.kr](http://www.ncsc.go.kr))  
2004 11 , 5

1

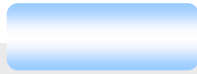
, 00 7 19 가  
가 [ 58]  
, 7

[ 59] 가



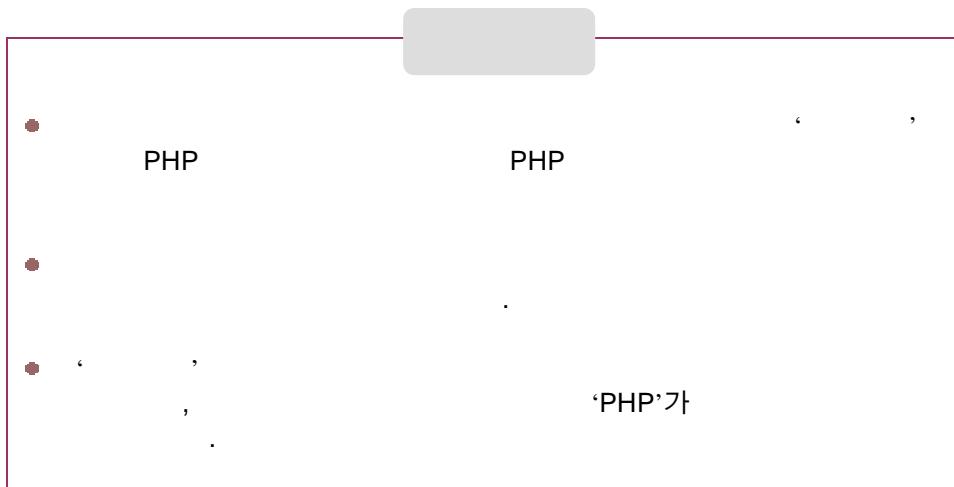
[ 58] ( )



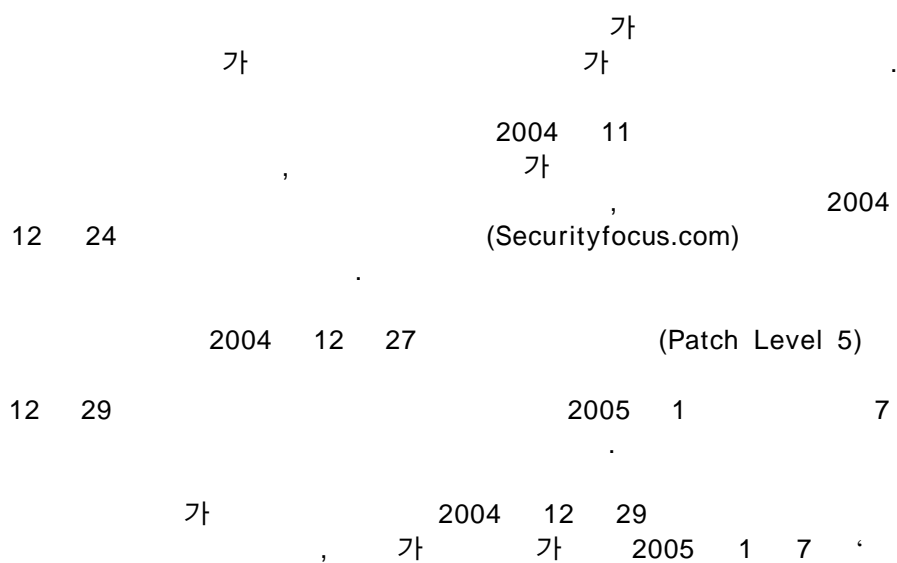


- 1.
2. 2004 11 Tech-note  
2000, Tech-note 2001, Tech-note Pro, Tech-note Top CGI
3. 가  
([www.technote.co.kr](http://www.technote.co.kr))

## 7 (Zeroboard)



1.



✓

(write.php)



[ 60] ( )

([ 60] ).

cdzr0x.zip.net

2.

○ ZeroBoard 4.1 PL5

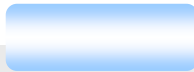
○ (2005 3 4.1 PL6)

○ 4.1 PL5

**3.**

○ ([www.nzeo.com](http://www.nzeo.com))  
( ).

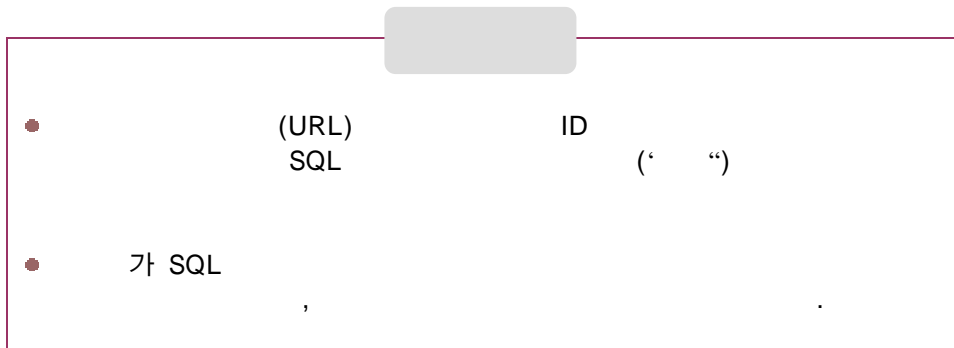
:



1. 4.1 PL5

2. 가 , ([www.nzeo.co](http://www.nzeo.co))  
[m](#)) ( ).

## 8 SQL Injection



1.

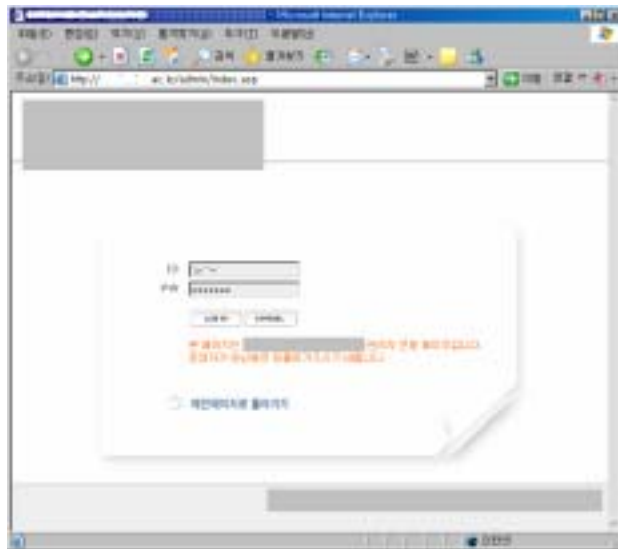
✓

가

|      |   |     |
|------|---|-----|
| 2004 | 3 | 170 |
|------|---|-----|

## SQL Injection



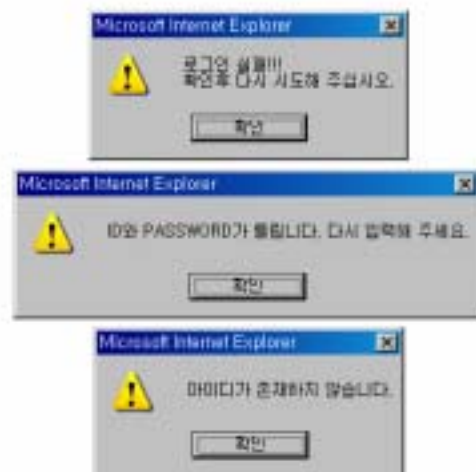


[ 61] (SQL Injection )

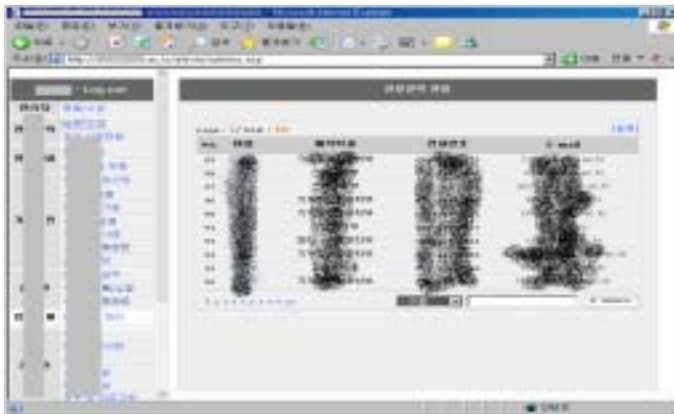
SQL Injection [

61] .

[ 62] .



[ 62]



[ 63] 가

, [ 63]

[ 64]  
가

가

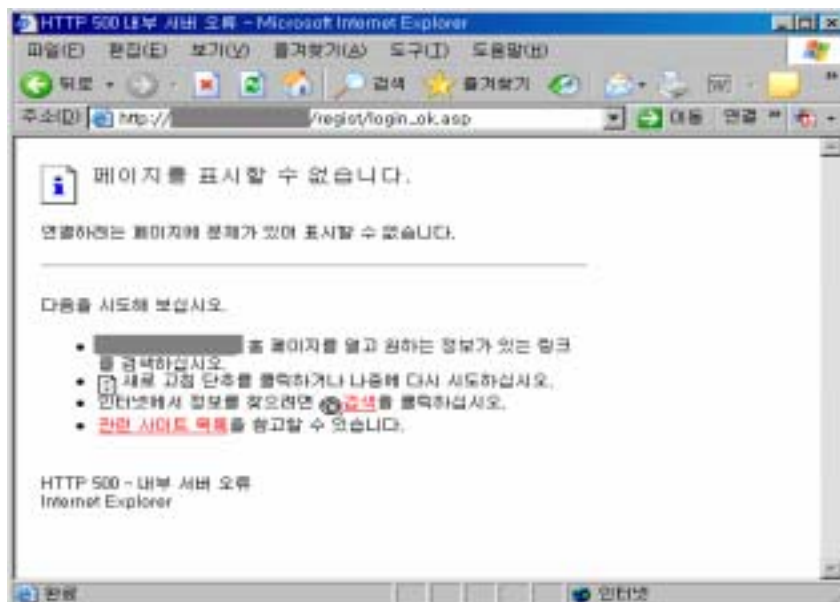
SQL

DB

SQL

Injection

가

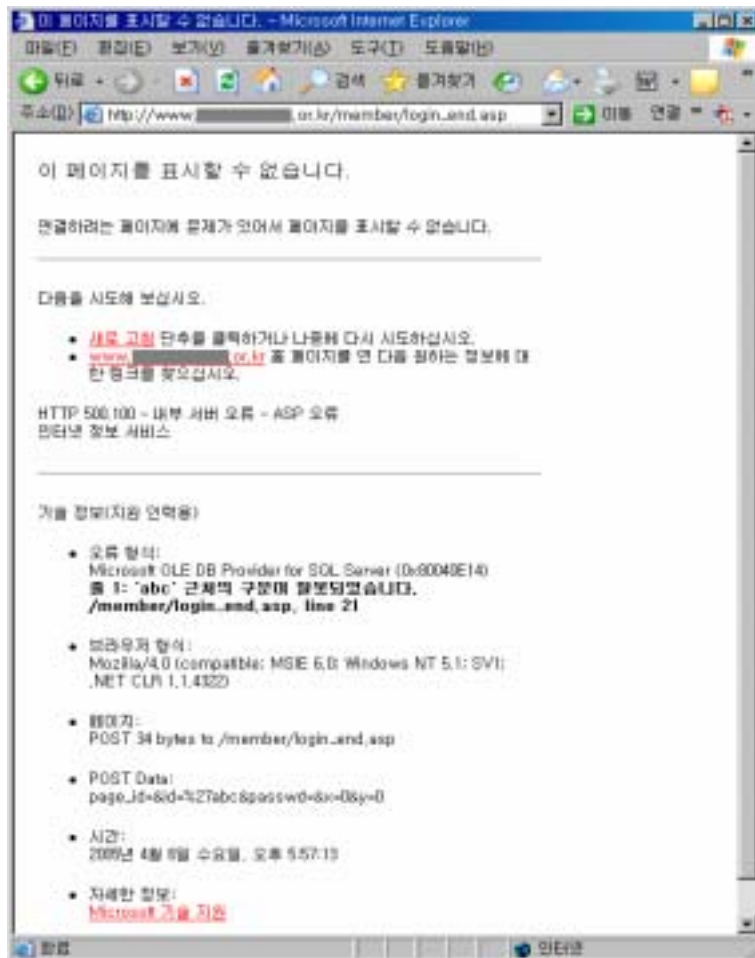


[ 64] SQL Injection

가

, [ 65] SQL

->DB SQL  
[ 64]



[ 65] SQL Injection

## 2.

SQL Injection  
가

SQL Injection

가

○

○

```
 : ' or 1=1;--
 : ' or 1=1;--
```

○

- (1) 가 ,
  - (2) , SQL Injection
  - (3) 가 ,
- SQL Injection 가

○

가 가

```
' ' or 1=1 --
" or 1=1 --
or 1=1 --
' or 'a'='a
" or "a"='a
') or ('a'='a
sql' or 1=1—
sql" or 1=1 --
+ or 1=1 --
';--
```

3.

○ SQL Injection

ID Password ( ;

)



1. SQL Injection  
( , )

, ID Password



3





가

8

가

가

가

가

가

가

가

**이 시에바에 사고 신고** ▶ 문의/입력입력

|          |                                   |                                   |                     |
|----------|-----------------------------------|-----------------------------------|---------------------|
| ▶ 사고종목   | <input type="text"/>              |                                   |                     |
| ▶ 사고유형   | <input type="text" value="비고유형"/> | <input type="button" value="선택"/> |                     |
| 비고거인     | <input type="text"/>              |                                   |                     |
| 부서       | <input type="text"/>              |                                   |                     |
| ▶ 담당자/성명 | <input type="text"/>              |                                   |                     |
| ▶ 연락처    | <input type="text"/>              | <input type="text"/>              | ▶ 연락처는 2~3번으로 입력하세요 |
| ▶ E-mail | <input type="text"/>              |                                   |                     |

**사고(비밀)시스템**

|                    |                                                             |                      |                      |                      |                                        |
|--------------------|-------------------------------------------------------------|----------------------|----------------------|----------------------|----------------------------------------|
| 장소                 | <input type="text"/>                                        | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/>                   |
| 호스트명               | <input type="text" value="호스트명"/>                           |                      |                      |                      |                                        |
| 운영체제               | <input type="text" value="운영체제"/>                           |                      |                      |                      |                                        |
| 출처파일               | <input type="text"/>                                        |                      |                      |                      | <input type="button" value="찾아보기..."/> |
| ▶ 상세정보<br>(사고관련정보) | <div style="border: 1px solid black; height: 100px;"></div> |                      |                      |                      |                                        |

8 4

- 3) , 가 ‘ 가
- 4) 가 ‘ , ,
- 5)
- : 02-3432-0462 ( 111)  
02-557-0716  
: 02-3432-0463  
: info@ncsc.go.kr



---

---

: 2005 5

: 가

---

---

( )



: <http://www.ncsc.go.kr>



: 02-3432-0462



: 02-3432-0463



: [info@ncsc.go.kr](mailto:info@ncsc.go.kr)



: [www.nis.go.kr](http://www.nis.go.kr)