답안지

과정명	오픈소스 기반 보안 취약점 분석 실무자 양성	담당교사	홍제준	월차	
과목명	DB 보안구축	훈련생 이름	임서규	평가일자	
평가 방법	문제해결 시나리오				

답안

데이터베이스 보안구축

(주)CARE Security

- 목차 -

1. 웹 서비스 환경

온라인 쇼핑몰 TOP aircon 업체의 웹 어플리케이션 서비스 환경은 다음과 같습니다.

환경	명칭	버전
운영체제	CentOS	4.4
웹 서버	Apache	2.0.52
스크립트	PHP	4.3.9
데이터베이스	MySQL	14.7 Distrib 4.1.20 for redhat-linux-gnu (i686)

2. 데이터베이스 자산 조사 및 정보수집

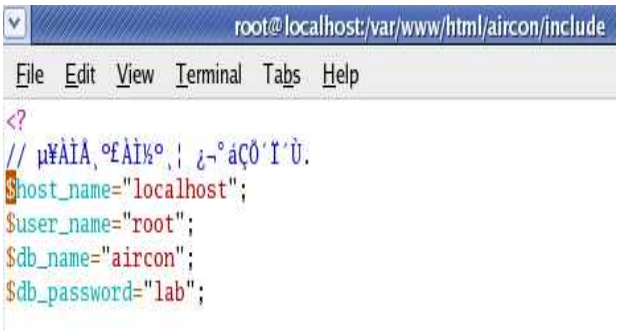
< Database 종류 및 버전 >

```
[root@localhost ~]# mysql -V
mysql  Ver 14.7 Distrib 4.1.20, for redhat-linux-gnu (i686) using readline 4.3
```

위의 그림대로 MySQL버전을 사용하고있습니다.

< Database 계정 >

```
-- phpMyAdmin SQL Dump
-- version 2.6.0
-- http://www.phpmyadmin.net
--
-- 호스트: localhost
-- 처리한 시간: 08-05-14 18:17
-- 서버 버전: 3.23.58
-- PHP 버전: 4.3.10
--
-- 데이터베이스: `testaircon`
```



사이트관리자계정 ID : testaircon

사이트관리자계정 PW : testaircon

hostname : localhost

Database 관리자명 : root

Database 명 : aircon

Databse 패스워드 : lab

< 웹 서버 관련 Database 명 >

```
+----------+
| Database |
+----------+
| aircon   |
| gnuboard |
| mysql    |
| technote |
| test     |
| zero     |
+----------+
```

현재 aircon 이라는 이름의 데이터베이스를 이용하고 있습니다.

< 테이블 및 칼럼 정보 >

```
+------------------+
| Tables_in_aircon |
+------------------+
| admin            |
| brd_customer01   |
| brd_news         |
| brd_qna          |
| cart             |
| category         |
| orders           |
| point            |
| products         |
| products_comment |
| request          |
| users            |
+------------------+
```

aircon 데이터베이스의 테이블 목록입니다. 총 12개의 테이블을 가지고 있습니다.
다음은 각각 테이블들의 칼럼들을 소개합니다.

- admin 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
A_no	int(11)		PRI	NULL	auto_increment
A_id	varchar(20)				
A_pass	varchar(20)				
A_name	varchar(20)				
A_email	varchar(100)				
A_hp	varchar(14)				
A_tel	varchar(20)				
A_bank	text				
A_point	float(4,3)			0.000	
A_baesong	int(11)			0	
A_baesongbi	int(11)			0	
A_usepoint	int(11)			0	
wdate	date			0000-00-00	
A_baesong01	text				
A_baesong02	text				
A_baesong03	text				

- brd_customer01 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
id	int(8)		PRI	NULL	auto_increment
userid	varchar(20)				
name	varchar(20)				
email	varchar(30)				
subject	varchar(255)				
comment	text				
wdate	date			0000-00-00	
uip	varchar(16)				
hits	int(8)			0	
pass	varchar(11)				
votes	int(8)			0	
file1	varchar(255)	YES		NULL	
file1_name	varchar(255)	YES		NULL	
replyno	int(9)	YES		NULL	
reply	varchar(5)			AAAAA	
HTMLYN	enum('t','e','h','b')			t	

- brd_news 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
id	int(8)		PRI	NULL	auto_increment
userid	varchar(20)				
name	varchar(20)				
email	varchar(30)				
subject	varchar(255)				
comment	text				
wdate	date			0000-00-00	
uip	varchar(16)				
hits	int(8)			0	
pass	varchar(11)				
votes	int(8)			0	
file1	varchar(255)	YES		NULL	
file1_name	varchar(255)	YES		NULL	
replyno	int(9)	YES		NULL	
reply	varchar(5)			AAAAA	
HTMLYN	enum('t','e','h','b')			t	

- brd_qna 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
id	int(8)		PRI	NULL	auto_increment
userid	varchar(20)				
name	varchar(20)				
email	varchar(30)				
subject	varchar(255)				
comment	text				
wdate	date			0000-00-00	
uip	varchar(16)				
hits	int(8)			0	
pass	varchar(11)				
votes	int(8)			0	
file1	varchar(255)	YES		NULL	
file1_name	varchar(255)	YES		NULL	
replyno	int(9)	YES		NULL	
reply	varchar(5)			AAAAA	
HTMLYN	enum('t','e','h','b')			t	

- cart 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
c_id	int(10)		PRI	NULL	auto_increment
cartid	varchar(30)		MUL		
p_code	int(10) unsigned zerofill		MUL	0000000000	
p_name	varchar(50)				
p_price	int(11)			0	
p_option	varchar(255)				
p_count	int(10)			0	
p_totalprice	int(10)			0	
i_id	int(10)			0	
regdate	datetime			0000-00-00 00:00:00	

- category 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
UID	int(5)		PRI	NULL	auto_increment
category	int(6) unsigned zerofill			000000	
name	varchar(30)	YES		NULL	
indexs	int(11)			0	

- orders 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
no	int(11)		MUL	NULL	auto_increment
orderno	varchar(31)				
price	int(9)			0	
point	int(8)			0	
use_point	float			0	
product	text				
userid	varchar(20)				
name	varchar(20)				
email	varchar(50)				
tel	varchar(14)				
cell	varchar(14)				
juso	varchar(255)				
rname	varchar(20)				
remail	varchar(40)				
rtel	varchar(14)				
rcell	varchar(14)				
rjuso	varchar(255)				
comment	text				
bank	varchar(50)				
paymethod	int(1)			0	
ordertype	enum('c','b')			c	
state	tinyint(1)			0	
baesong	int(1)			1	
cancel	tinyint(1)			0	
wdate	datetime			0000-00-00 00:00:00	
view_time	datetime			0000-00-00 00:00:00	
tax	enum('y','n')			n	
bz_no	varchar(20)				
companyname	varchar(100)				
name2	varchar(20)				
bz_zip	varchar(8)				
bz_juso1	varchar(255)				
bz_juso2	varchar(255)				
upjong	varchar(100)				
uptae	varchar(100)				

- point 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
po_no	int(11)		PRI	NULL	auto_increment
order_no	varchar(31)			0	
userid	varchar(20)				
product	text				
point	decimal(10,0)			0	
reason	varchar(255)				
wdate	date			0000-00-00	

- products 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
category	int(6) unsigned zerofill		MUL	000000	
p_code	int(10) unsigned zerofill		PRI	0000000000	
p_name	varchar(255)				
p_price	int(11)			0	
make_com	varchar(255)				
make_nation	varchar(255)				
p_option	varchar(255)				
p_option2	text				
p_brand	int(11)		MUL	0	
p_comment	text				
p_baesong	text				
saletype	enum('p','n','s','b')			p	
htmlYN	enum('y','n')			n	
hits	tinyint(4)			0	
wdate	date			0000-00-00	
p_indexs	int(11)			0	
plus01	enum('n','y')			n	
plus02	enum('n','y')			n	
naver_yn	enum('n','y')			n	

- products comment 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
no	int(11)		PRI	NULL	auto_increment
category	int(6) unsigned zerofill		MUL	000000	
name	varchar(100)				
tel	varchar(16)				
cell	varchar(16)				
in_date	date			0000-00-00	
zip	varchar(10)				
address1	varchar(255)				
address2	varchar(255)				
email	varchar(255)				
comment	text				
wdate	date			0000-00-00	

- request 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
no	int(11)		PRI	NULL	auto_increment
category	int(6) unsigned zerofill		MUL	000000	
name	varchar(100)				
tel	varchar(16)				
cell	varchar(16)				
in_date	date			0000-00-00	
zip	varchar(10)				
address1	varchar(255)				
address2	varchar(255)				
email	varchar(255)				
comment	text				
wdate	date			0000-00-00	

- users 테이블 칼럼 목록 -

Field	Type	Null	Key	Default	Extra
no	int(11)		PRI	NULL	auto_increment
userid	varchar(20)		UNI		
pass	varchar(20)				
name	varchar(20)				
jumin	varchar(14)				
tel	varchar(40)				
cell	varchar(40)				
email	varchar(100)				
zip	varchar(8)				
address1	varchar(100)				
address2	varchar(100)				
mailcheck	enum('y','n')			y	
visitcnt	int(11)			0	
ldate	date			0000-00-00	
wdate	date			0000-00-00	
recomment_id	varchar(20)				
comment	text				
company	varchar(255)				
bz_no	varchar(255)				

3. 취약점 체크리스트 및 판단결과

데이터베이스 취약점 분석을 위한 리스트이며 취약점을 조사한 결과 다음과 같습니다.

취약점	피해 범위	점검 결과
DB 계정 관리	권한 남용	취약
디렉터리 리스팅	웹 서버 디렉터리 노출	취약
DB 백업	손실 데이터 복구 불가	취약
SQL Injection	공격자에 의한 DB 덤프, 수정, 삭제 피해	취약
Web서버 불필요한 파일	웹서버의 .php파일을 제외한 노출로 인한 정보(자산) 피해	취약
MySQL 버전 패치 관리	구 버전으로 인한 취약점 문제 발생	취약
DB 원격 접속 관리	네트워크 스캐닝, DB 데이터 노출	안전

4. 모의해킹 및 취약점 대응방안

<DB 계정관리>

MySQL 접속 계정 관리와 계정 별 권한설정 방법에 대해 알아보겠습니다

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4 to server version: 4.1.20

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

먼저 MySQL 계정을 접속을 합니다.

```
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
15 rows in set (0.00 sec)
```

그 다음 스키마를 mysql로 변경후 mysql테이블 구성을 봅니다.

```
mysql> select host,user,password from user;
+-----------------------+------+-------------------+
| host                  | user | password          |
+-----------------------+------+-------------------+
| localhost             | root | 79f6e27f290c4252 |
| localhost.localdomain | root |                   |
| localhost.localdomain |      |                   |
| localhost             |      |                   |
+-----------------------+------+-------------------+
4 rows in set (0.00 sec)
```

계정정보를 조회한 결과 현재 root계정만 사용되고 있는 것을 확인 합니다.

host를 '%'로 해주면 외부에서의 접속을 허용하는 설정이 됩니다. 만약 계정을 추가하실 경우,

create user '계정아이디'@localhost identified by '비밀번호'; 질의를 쓰셨다면

create user '계정아이디'@'%' identified by '비밀번호'; 로 변경하시면 되겠습니다.

특정 IP대역에서만 접속허용을 원하신다면 'IP대역.%'으로 추가하시면 되겠습니다.

현재 root계정은 외부IP로 부터의 접근이 제한된 상태이므로 양호합니다.

※ 확인사항

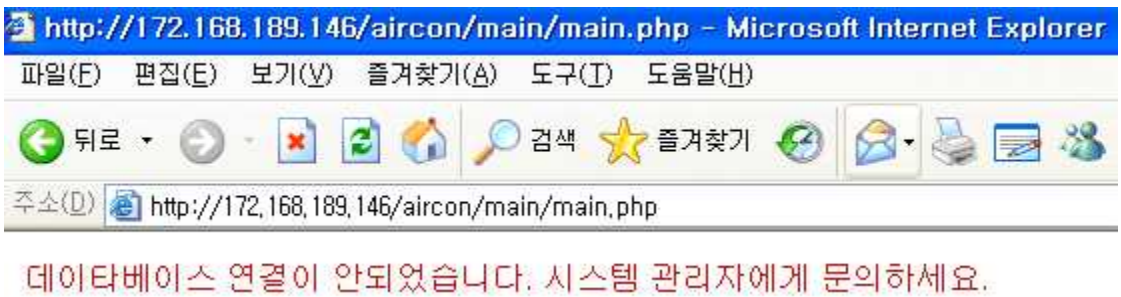
MySQL5.7버전부터 user테이블에 password칼럼이 삭되고 authentication_string컬럼으로 변경 되었습니다. MySQL 5.7 Reference를 참고하십시오.

https://dev.mysql.com/doc/refman/5.7/en/grant-tables.html

하지만 MySQL보안에 가장 중요한 것은 데이터베이스의 root 사용자 패스워드를 디폴트 상태로 운영하지 않았는지 점검해야 합니다. 디폴트로 설정되는 관리자 계정(root)을 무차별 대입공격이나 사전대입 공격을 이용한 Bruteforcing공격에 의해 무너질수 있기 때문에 추측해 내기 어려운 이름으로 변경합니다. 변경해 두면 공격을 당하더라도 공격자는 패스워드뿐 아니라 계정정보도 추측해 내야 하기 때문에 공격이 더 어려워 질수 있습니다. 이 부분에 있어서는 취약하다고 판단됩니다.

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 23 to server version: 4.1.20

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> update user set user='adrootmin' where user='root';
Query OK, 2 rows affected (0.00 sec)
Rows matched: 2  Changed: 2  Warnings: 0

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye
[root@localhost ~]# mysql -u adrootmin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 24 to server version: 4.1.20

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

위와 같이 root계정을 adrootmin이라는 추측하기 힘든 이름으로 계정명을 변경 후 접속을 확인합니다.



변경 후에 사이트를 보시면 데이터베이스와 연동이 되지 않는 것을 탐지 할 수 있습니다.

root@localhost:/var/www/html/aircon/include

File Edit View Terminal Tabs Help

```
<?
// µ¥ÀÌÅ¸º£ÀÌ½º¸¦ ¿¬°áÇÕ´Ï´Ù.
$host_name="localhost";
$user_name="root";
$db_name="aircon";
$db_password="lab";
```

/var/www/html/aircon/include 경로로 들어가시면 config.php 파일이 있습니다.

맨 위에 user_name 변수 값을 수정하여 문제를 해결하실수 있습니다.

root@localhost:/var/www/html/aircon/include

File Edit View Terminal Tabs Help

```
<?
// µ¥ÀÌÅ¸º£ÀÌ½º¸¦ ¿¬°áÇÕ´Ï´Ù.
$host_name="localhost";
$user_name="adrootmin";
$db_name="aircon";
$db_password="lab";
```

-config.php 파일 내용 수정

```
[root@localhost include]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@localhost include]# service mysqld restart
Stopping MySQL:                                            [  OK  ]
Starting MySQL:                                            [  OK  ]
```

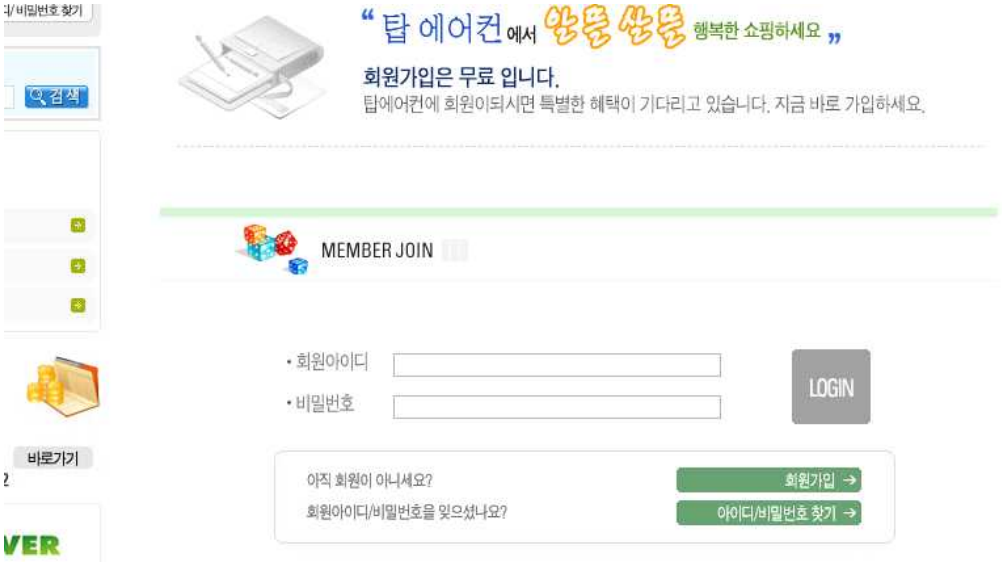
-서비스 재시작

-사이트 정상 동작

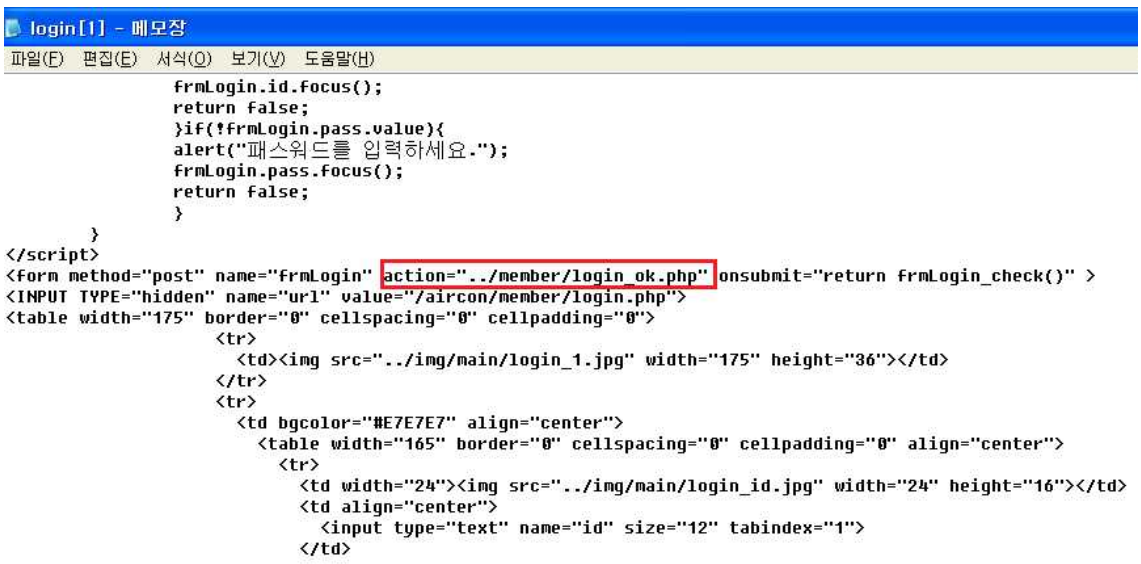
변경된 adrootmin으로 수정하여 다시 서비스를 재시작 하시면 사이트가 정상적으로 동작되는 것을 확인하실 수 있습니다.

<디렉터리 리스팅>

서버내의 모든 디렉토리 혹은 중요한 정보가 포함된 디렉토리에 대해 인덱싱이 가능하게 설정되어 중요 파일 정보가 노출 될 수 있습니다. 디렉토리를 통하여 내부구조 확인이나 웹 서버내의 백업파일 및 소스 코드, 스크립트파일의 유출로 인한 계정정보 유출 등 파일열람이 가능하므로 취약점이 있는지 점검해야합니다.



-회원 로그인 페이지



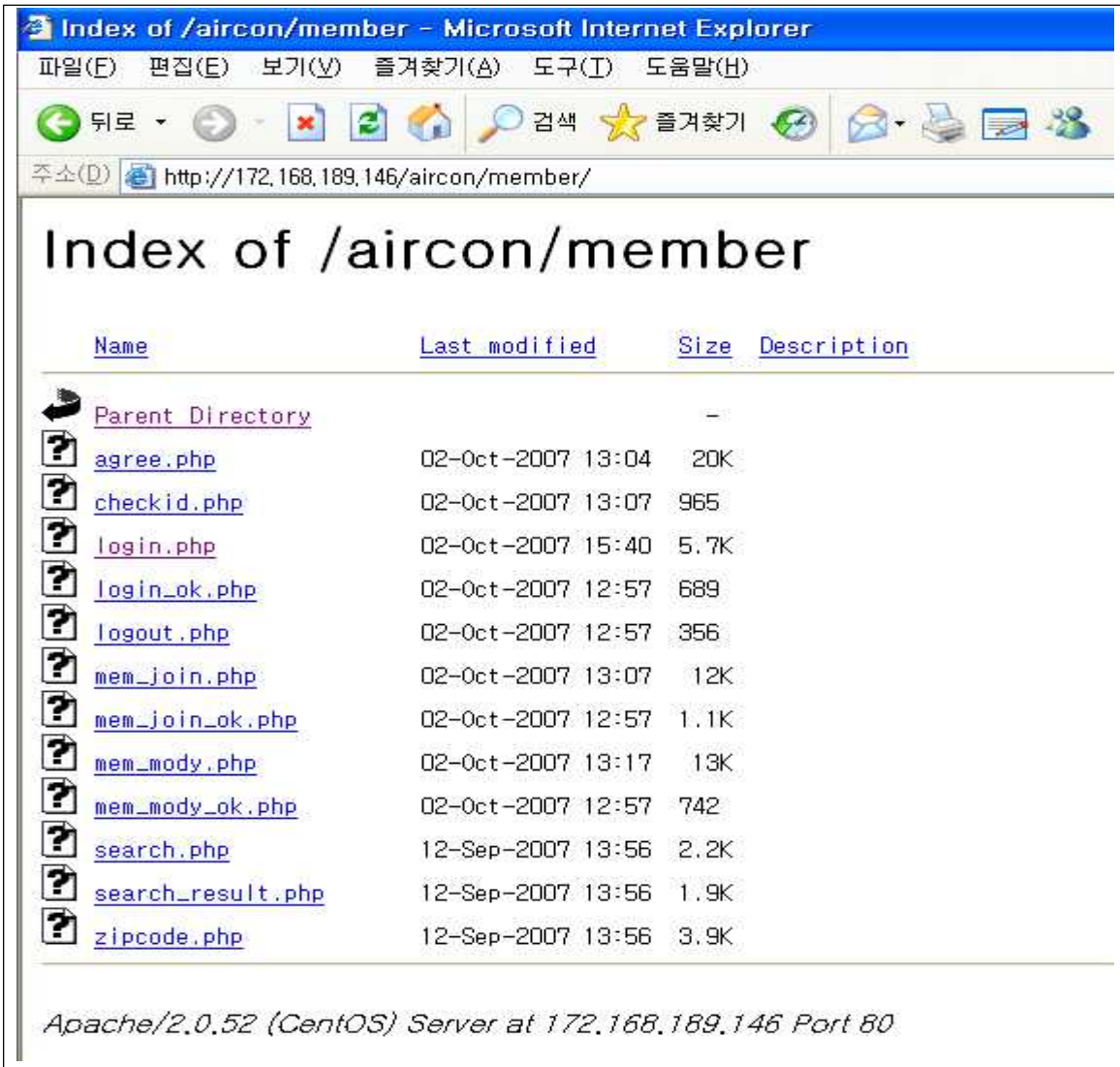
login[1] - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
                frmLogin.id.focus();
                return false;
                }if(!frmLogin.pass.value){
                alert("패스워드를 입력하세요.");
                frmLogin.pass.focus();
                return false;
                }
        }
</script>
<form method="post" name="frmLogin" action="../member/login_ok.php" onsubmit="return frmLogin_check()" >
<INPUT TYPE="hidden" name="url" value="/aircon/member/login.php">
<table width="175" border="0" cellspacing="0" cellpadding="0">
                    <tr>
                      <td><img src="../img/main/login_1.jpg" width="175" height="36"></td>
                    </tr>
                    <tr>
                      <td bgcolor="#E7E7E7" align="center">
                        <table width="165" border="0" cellspacing="0" cellpadding="0" align="center">
                          <tr>
                            <td width="24"><img src="../img/main/login_id.jpg" width="24" height="16"></td>
                            <td align="center">
                              <input type="text" name="id" size="12" tabindex="1">
                            </td>
```

-로그인 페이지에서 소스의 일부분

위와 같이 로그인 페이지로 들어가서 html 페이지의 소스보기를 할 수 있을 때, 이미지 및 파일의 경로나 <form>에서 로그인 액션 과정이 적혀 있는 부분을 쉽게 찾을 수 있습니다. 이에 따라 /member의 경로를 들어가 봅니다.



/member로 들어가니 member디렉토리에 안의 php파일 리스트를 볼 수 있습니다. 이러한 사례를 기반으로 페이지의 소스를 보고 경로를 통하여 악용이 가능하기 때문에 디렉토리 리스팅 접근을 하지 못하도록 설정해야합니다.

따라서 유닉스 및 리눅스 운영체제로서 아파치(Apache)를 이용하는 웹 서버는 아래 작업을 통해 디렉토리 리스팅 취약점을 차단할 수 있습니다. 다음으로 넘어갑니다.

root@localhost:/etc/httpd/conf

File Edit View Terminal Tabs Help

```
287 #
288 # This should be changed to whatever you set DocumentRoot to.
289 #
290 <Directory "/var/www/html">
291
292 #
293 # Possible values for the Options directive are "None", "All",
294 # or any combination of:
295 #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
296 #
297 # Note that "MultiViews" must be named *explicitly* --- "Options All"
298 # doesn't give it to you.
299 #
300 # The Options directive is both complicated and important.  Please see
301 # http://httpd.apache.org/docs-2.0/mod/core.html#options
302 # for more information.
303 #
304     Options Indexes FollowSymLinks
305
306 #
307 # AllowOverride controls what directives may be placed in .htaccess files.
308 # It can be "All", "None", or any combination of the keywords:
309 #   Options FileInfo AuthConfig Limit
310 #
311     AllowOverride all
312
313 #
314 # Controls who can get stuff from this server.
315 #
316     Order allow,deny
317     Allow from all
318
```

서버에서 아파치 서버의 설정 파일인 "httpd.conf" 파일을 검색 후, httpd.conf의 파일 내용 중 Options 항목 뒤 Indexes FollowSymLinks에서 "indexes" 라는 지시어만 지우고 저장합니다.

파일경로 : /etc/httpd/conf

```
[root@localhost conf]# vi httpd.conf
[root@localhost conf]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@localhost conf]#
```

설정한 정보를 적용하기 위해 웹서비스 데몬을 재시작합니다.

설정을 적용한 뒤 디렉토리 리스팅 접근이 차단되는 것을 확인합니다.

< DB 백업 >

데이터베이스 백업파일은 aircon디렉토리 안에 db.sql 로 존재합니다.

```
[root@localhost aircon]# ll
total 2064
drwxr-xr-x   4 root root    4096 Aug 30 21:30 admin
drwxr-xr-x   2 root root    4096 Jan 12  2009 as
drwxr-xr-x   2 root root    4096 Jan 12  2009 basket
drwxr-xr-x   3 root root    4096 Sep  8  2011 board
drwxr-xr-x   2 root root    4096 Jan 12  2009 cart
drwxr-xr-x   2 root root    4096 Jan 12  2009 company
drwxr-xr-x   2 root root    4096 Jan 12  2009 css
drwxr-xr-x   2 root root    4096 Sep  8  2011 customer
-rw-r--r--   1 root root 1982234 May 14  2008 db.sql
drwxr-xr-x   2 root root    4096 Jan 12  2009 ep
```

sql 파일내용을 확인한 결과 aircon데이터베이스의 백업파일입니다.

```
[root@localhost aircon]# cp db.sql dbtest.sql
[root@localhost aircon]# ll
total 4004
drwxr-xr-x   4 root root    4096 Aug 30 21:30 admin
drwxr-xr-x   2 root root    4096 Jan 12  2009 as
drwxr-xr-x   2 root root    4096 Jan 12  2009 basket
drwxr-xr-x   3 root root    4096 Sep  8  2011 board
drwxr-xr-x   2 root root    4096 Jan 12  2009 cart
drwxr-xr-x   2 root root    4096 Jan 12  2009 company
drwxr-xr-x   2 root root    4096 Jan 12  2009 css
drwxr-xr-x   2 root root    4096 Sep  8  2011 customer
-rw-r--r--   1 root root 1982234 May 14  2008 db.sql
-rw-r--r--   1 root root 1982234 Aug 31 18:16 dbtest.sql
drwxr-xr-x   2 root root    4096 Jan 12  2009 ep
```

db.sql을 dbtest명으로 하나 더 복사합니다.

```
[root@localhost html]# mkdir airconbackup
[root@localhost html]# ll
total 72760
drwxr-xr-x  25 root root      4096 Aug 31 18:16 aircon
drwxr-xr-x   2 root root      4096 Aug 31 18:17 airconbackup
```

/var/www/html 폴더안에 airconbackup이라는 백업용 폴더를 하나 생성합니다.

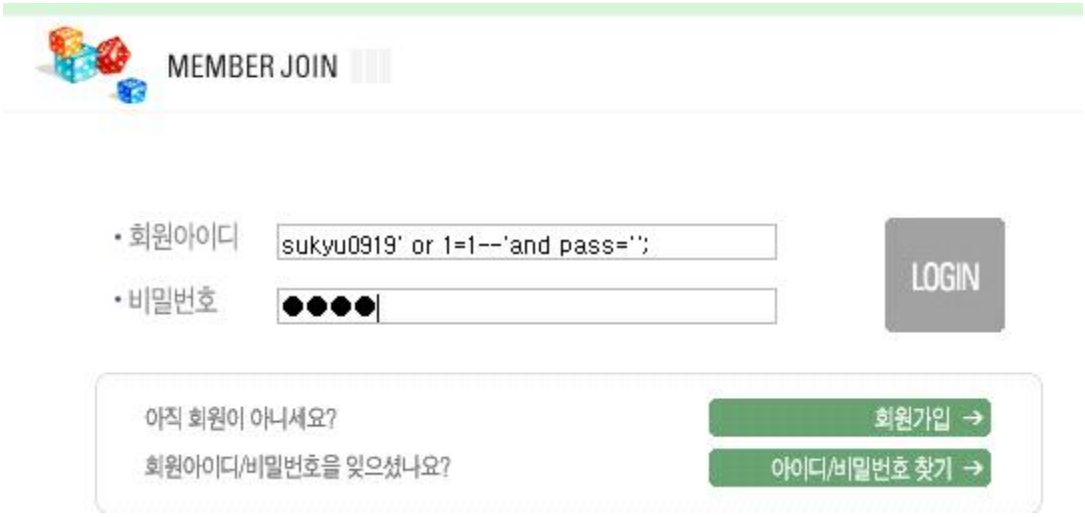
```
[root@localhost aircon]# mv dbtest.sql ../airconbackup
```

move를 통하여 airconbackup파일로 백업파일을 이동합니다.

```
[root@localhost airconbackup]# ll
total 1940
-rw-r--r--  1 root root 1982234 Aug 31 18:20 dbtest.sql
```

백업 디렉토리를 새로 만듬으로써 데이터복구시에 사용합니다.

< SQL Injection >



회원 로그인 게시판입니다. 미리 가입해둔 sukyu0919라는 아이디를 참으로 두고 or(논리합 연산) 1=1을 대입한 후에 주석처리 하여 SQL 구문이 작동되는지 공격합니다.

```
GET http://172.168.189.146/aircon/main/main.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: ko
Cookie: user_id=sukyu0919; user_name=%C0%D3%BC%AD%B1%D4; user_email=sukyu0919%40hanmail.net; user_tel=02-562-1023; user_cell=010-4752-3143
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Paros/3.2.13
Host: 172.168.189.146
Proxy-Connection: Keep-Alive
Content-length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 31 Aug 2018 09:40:16 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Set-Cookie: user_id=sukyu0919; path=/
Set-Cookie: user_name=%C0%D3%BC%AD%B1%D4; path=/
Set-Cookie: user_email=sukyu0919%40hanmail.net; path=/
Set-Cookie: user_tel=02-562-1023; path=/
Set-Cookie: user_cell=010-4752-3143; path=/
Set-Cookie: user_level=deleted; expires=Thu, 31-Aug-2017 09:40:15 GMT; path=/
Content-Length: 84
Connection: close
```

```
<script language=javascript>
document.location.replace('../main/main.php')
</script>
```

Paros 툴을 이용하여 트래픽을 조사결과 공격시도가 성공하였고 실질적으로 로그인이 되는 것을 확인합니다. 이는 SQL injection을 이용한 로그인 우회가 가능하다는 취약점을 가지고 있습니다.

따라서 로그인 우회를 방어하려면 먼저 로그인이 동작하는 과정을 살펴야합니다.

```
</script>
<form method="post" name="frmLogin" action="../member/login_ok.php" onsubmit="return frmLogin_check()" >
<INPUT TYPE="hidden" name="url" value="/aircon/member/login.php">
<table width="175" border="0" cellspacing="0" cellpadding="0">
                  <tr>
                    <td><img src="../img/main/login_1.jpg" width="175" height="36"></td>
                  </tr>
                  <tr>
                    <td bgcolor="#E7E7E7" align="center">
                      <table width="165" border="0" cellspacing="0" cellpadding="0" align="center">
                        <tr>
                          <td width="24"><img src="../img/main/login_id.jpg" width="24" height="16"></td>
                          <td align="center">
                            <input type="text" name="id" size="12" tabindex="1">
                          </td>
```

로그인 페이지에서 소스보기를 한후 login.php를 살펴봅니다.

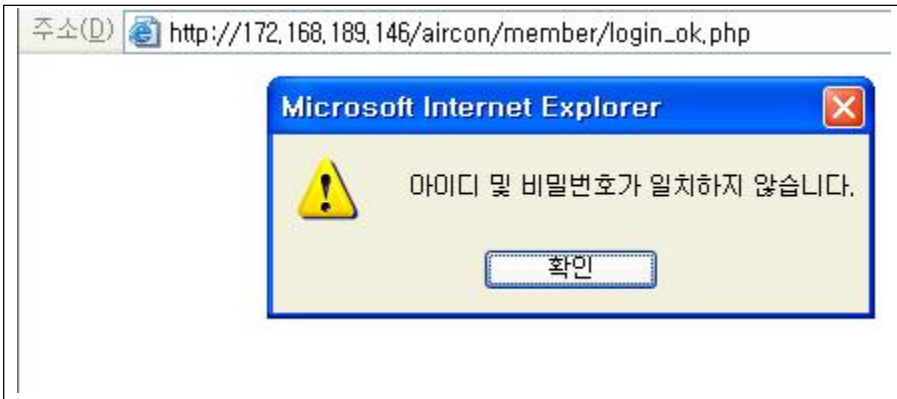
여기서 <form>을 살펴보니 로그인을 하게되면 post형식으로 /member/login_ok.php로 동작하는 것을 확인합니다.

```
<?
include ("../include/config.php");
include ("../include/function.php");
        $row = DBarray("select * from users where userid = '$id' and pass = '$pass'");
        if($row[userid]){       //È¸¿øÀÌ ¸ÂÀ»¶§
                DBquery("update users set visitcnt=visitcnt+1,ldate=now()  where userid = '$id'");
                setcookie("user_id",$row[userid],0,"/");
                setcookie("user_name",$row[name],0,"/");
                setcookie("user_email",$row[email],0,"/");
                setcookie("user_tel",$row[tel],0,"/");
                setcookie("user_cell",$row[cell],0,"/");
                setcookie("user_level",$row[level],0,"/");
                if ($url) redirect1("$url");
                redirect1("../main/main.php");
        } else {        //È¸¿øÀÌ ¾Æ´Ò¶§
                error_check('¾ÆÀÌµð ¹× ºñ¹Ð¹øÈ£°¡ ÀÏÄ¡ÇÏÁö ¾Ê½À´Ï´Ù.');
        }
?>
```

따라서 login_ok.php에서 소스를 수정합니다. 현재 row변수로 아무런 필터링 없이 받아들이고 있기 때문에 SQL 구문이 들어가지 못하도록 특수문자를 차단하거나 일부 특수문자는 허용하는 식으로 코드가 추가되어야 합니다

```
<?
include ("../include/config.php");
include ("../include/function.php");
        $id = preg_replace("/[\r\n\s\t\'\;\"\=\-\-\#\/*]+/","",$id);
        if(preg_match('/(union|select|from|where)/i',$id)){
                $this->Error_popopup('No SQL-Injection!!');
                }
        $row = DBarray("select * from users where userid = '$id' and pass = '$pass'");
        if($row[userid]){       //È¸¿øÀÌ ¸ÂÀ»¶§
                DBquery("update users set visitcnt=visitcnt+1,ldate=now()  where userid = '$id'");
                setcookie("user_id",$row[userid],0,"/");
```

$id 변수에 특수문자를 치환하도록 선언하여 select,form,where,union같은 sql구문 문자열이 오면 경고창을 띄우도록 코드를 추가합니다. 수정 후 에는 httpd서비스를 재시작합니다.



다시 SQL-Injection을 통한 로그인 우회를 시도한 결과 login_ok.php 과정에서 경고창이 뜨면서 정상적으로 접근이 통제되는 것을 확인합니다.

DB와 연관될 수 있는 모든 부분에 이러한 방식으로 확인하여 시큐어코딩을 통해 예방해야합니다.

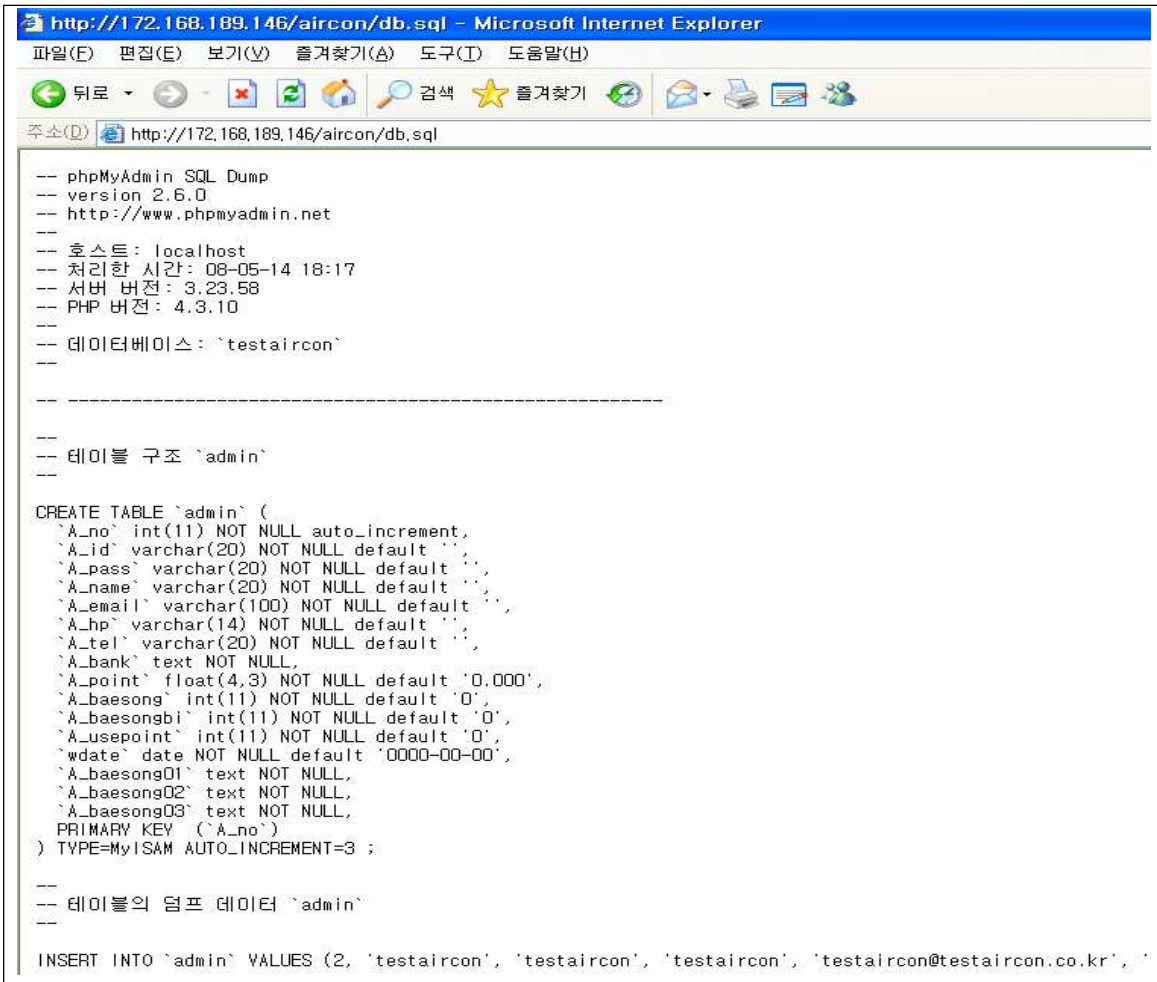
즉 사용자로부터 입력되는 '입력값' 에 대한 철저한 검증과 예외처리가 필요합니다. 예로 들어 ID, PASSWORD, 게시판 제목, 본문, 검색창, 주소검색창 등의 모든 입력란에 특수문자(등호, 부등호, 인용부호 등)를 직접 입력하지 못하도록 웹 서버의 소스코드를 수정해야 할 것입니다.

magic_quotes_gpc를 이용한 특수문자 차단이 있지만 추천하지 않습니다. 이러한 방식보다는 직접적으로 시큐어 코드를 통하여 차단하는 것이 바람직합니다.

< Web서버 불필요한 파일 >

```
[root@localhost html]# cd aircon
[root@localhost aircon]# ll
total 2064
drwxr-xr-x   4 root root    4096 Aug 30 21:30 admin
drwxr-xr-x   2 root root    4096 Jan 12  2009 as
drwxr-xr-x   2 root root    4096 Jan 12  2009 basket
drwxr-xr-x   3 root root    4096 Sep  8  2011 board
drwxr-xr-x   2 root root    4096 Jan 12  2009 cart
drwxr-xr-x   2 root root    4096 Jan 12  2009 company
drwxr-xr-x   2 root root    4096 Jan 12  2009 css
drwxr-xr-x   2 root root    4096 Sep  8  2011 customer
-rw-r--r--   1 root root 1982234 May 14  2008 db.sql
drwxr-xr-x   2 root root    4096 Jan 12  2009 ep
drwxr-xr-x   5 root root    4096 Jan 12  2009 gmEditor
drwxr-xr-x   2 root root    4096 Jan 12  2009 guide
drwxr-xr-x  19 root root    4096 Jan 12  2009 img
drwxr-xr-x   2 root root    4096 Aug 31 20:16 include
-rw-r--r--   1 root root      57 Oct  4  2007 index.html
drwxr-xr-x   3 root root    4096 Jan 12  2009 js
drwxr-xr-x   2 root root    4096 Jan 12  2009 main
drwxr-xr-x   2 root root    4096 Jan 12  2009 member
drwxr-xr-x   2 root root    4096 Jan 12  2009 mypage
drwxr-xr-x   2 root root    4096 Jan 12  2009 news
drwxr-xr-x   3 root root    4096 Jan 12  2009 order
drwxr-xr-x   2 root root    4096 Jan 12  2009 orderinfo
drwxr-xr-x   2 root root    4096 Jan 12  2009 product
drwxr-xr-x   2 root root   28672 Jan 12  2009 product_img
-rw-r--r--   1 root root     196 May 14  2008 readme.txt
drwxr-xr-x   2 root root    4096 Jan 12  2009 swf
```

aircon디렉토리 내용입니다. php이외의 파일들을 보니 db백업파일이 서버 디렉토리내에 존재합니다.



웹에서 접근이 가능합니다. db.sql 내용은 데이터베이스의 각 테이블의 구조나 명칭 들이 모두 나와서 해커가 정보수집 하기 가장 적합한 파일입니다. 그리고 위에서 Index리스팅을 제한하는 방법으로는 막을 수 없습니다. 따라서 airconbackup 디렉토리에 백업복사본이 있으므로 aircon디렉토리내에 존재하는 db.sql은 삭제합니다.


```
1, DB연결파일 수정 public_html/include/config.php

2, myadldump -u유저명 -p비밀번호  DB명 < db.sql

3, 쓰기권한설정
        chmod 707 gmEditor/uploaded
        chmod 707 board/data
        chmod 707 product_img
```

readme.txt 내용입니다. 이 내용 또한 정보가 유출이 되면 안되기 때문에 백업디렉토리로 이동시킵니다.

```
[root@localhost aircon]# mv readme.txt ../airconbackup/
[root@localhost aircon]# cd ../airconbackup
[root@localhost airconbackup]# ll
total 1944
-rw-r--r--  1 root root 1982234 May 14  2008 dbtest.sql
-rw-r--r--  1 root root     196 May 14  2008 readme.txt
[root@localhost airconbackup]# cd ../aircon
[root@localhost aircon]# rm -rf readme.txt
[root@localhost aircon]# ll
total 120
drwxr-xr-x   4 root root  4096 Aug 30 21:30 admin
drwxr-xr-x   2 root root  4096 Jan 12  2009 as
drwxr-xr-x   2 root root  4096 Jan 12  2009 basket
drwxr-xr-x   3 root root  4096 Sep  8  2011 board
drwxr-xr-x   2 root root  4096 Jan 12  2009 cart
drwxr-xr-x   2 root root  4096 Jan 12  2009 company
drwxr-xr-x   2 root root  4096 Jan 12  2009 css
drwxr-xr-x   2 root root  4096 Sep  8  2011 customer
drwxr-xr-x   2 root root  4096 Jan 12  2009 ep
drwxr-xr-x   5 root root  4096 Jan 12  2009 gmEditor
drwxr-xr-x   2 root root  4096 Jan 12  2009 guide
drwxr-xr-x  19 root root  4096 Jan 12  2009 img
drwxr-xr-x   2 root root  4096 Aug 31 20:29 include
-rw-r--r--   1 root root    57 Oct  4  2007 index.html
drwxr-xr-x   3 root root  4096 Jan 12  2009 js
drwxr-xr-x   2 root root  4096 Jan 12  2009 main
drwxr-xr-x   2 root root  4096 Jan 12  2009 member
drwxr-xr-x   2 root root  4096 Jan 12  2009 mypage
drwxr-xr-x   2 root root  4096 Jan 12  2009 news
drwxr-xr-x   3 root root  4096 Jan 12  2009 order
drwxr-xr-x   2 root root  4096 Jan 12  2009 orderinfo
drwxr-xr-x   2 root root  4096 Jan 12  2009 product
drwxr-xr-x   2 root root 28672 Jan 12  2009 product_img
drwxr-xr-x   2 root root _4096 Jan 12  2009 swf
```

airconbackup 디렉토리로 이동 후 확인합니다. 기존에 aircon 서버 디렉토리에 존재하던 readme.txt는 삭제합니다.

더 이상 웹에서 readme.txt 로 접근할수 없는 것을 확인합니다.

또는 chmod 명령을 통해 파일권한을 변경하여 접근을 차단할 수 있습니다.

```
[root@localhost aircon]# chmod 600 db.sql
[root@localhost aircon]# ll
total 2064
drwxr-xr-x    4 root root     4096 Jan 12  2009 admin
drwxr-xr-x    2 root root     4096 Jan 12  2009 as
drwxr-xr-x    2 root root     4096 Jan 12  2009 basket
drwxr-xr-x    3 root root     4096 Sep  8  2011 board
drwxr-xr-x    2 root root     4096 Jan 12  2009 cart
drwxr-xr-x    2 root root     4096 Jan 12  2009 company
drwxr-xr-x    2 root root     4096 Jan 12  2009 css
drwxr-xr-x    2 root root     4096 Sep  8  2011 customer
-rw-------    1 root root  1982234 May 14  2008 db.sql
drwxr-xr-x    2 root root     4096 Jan 12  2009 ep
drwxr-xr-x    5 root root     4096 Jan 12  2009 gmEditor
drwxr-xr-x    2 root root     4096 Jan 12  2009 guide
drwxr-xr-x   19 root root     4096 Jan 12  2009 img
drwxr-xr-x    2 root root     4096 Feb  3  2009 include
-rw-r--r--    1 root root       57 Oct  4  2007 index.html
drwxr-xr-x    3 root root     4096 Jan 12  2009 js
drwxr-xr-x    2 root root     4096 Jan 12  2009 main
drwxr-xr-x    2 root root     4096 Jan 12  2009 member
drwxr-xr-x    2 root root     4096 Jan 12  2009 mypage
drwxr-xr-x    2 root root     4096 Jan 12  2009 news
drwxr-xr-x    3 root root     4096 Jan 12  2009 order
drwxr-xr-x    2 root root     4096 Jan 12  2009 orderinfo
drwxr-xr-x    2 root root     4096 Jan 12  2009 product
drwxr-xr-x    2 root root    28672 Jan 12  2009 product_img
-rw-r--r--    1 root root      196 May 14  2008 readme.txt
drwxr-xr-x    2 root root     4096 Jan 12  2009 swf
[root@localhost aircon]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

db.sql파일의 권한을 시스템관리자만 열어 볼 수 있도록 권한을 변경합니다.

접근 권한으로 인한 차단을 확인할 수있습니다.

< MySQL 버전 패치 관리 >

```
[root@localhost yum.repos.d]# yum info mysql
Setting up repositories
Reading repository metadata in from local files
Installed Packages
Name    : mysql
Arch    : i386
Version: 4.1.20
Release: 1.RHEL4.1
Size    : 5.2 M
Repo    : installed
Summary: MySQL client programs and shared libraries.

Description:
 MySQL is a multi-user, multi-threaded SQL database server. MySQL is a
client/server implementation consisting of a server daemon (mysqld)
and many different client programs and libraries. The base package
contains the MySQL client programs, the client shared libraries, and
generic MySQL files.


Available Packages
Name    : mysql
Arch    : i386
Version: 4.1.20
Release: 2.RHEL4.1
Size    : 2.9 M
Repo    : update
Summary: MySQL client programs and shared libraries.
Description:
 MySQL is a multi-user, multi-threaded SQL database server. MySQL is a
client/server implementation consisting of a server daemon (mysqld)
and many different client programs and libraries. The base package
contains the MySQL client programs, the client shared libraries, and
generic MySQL files.
```

yum info mysql을 실행시켜 mysql버전 info를 확인합니다.

위에 그림대로 현재 설치되어있는 Installed Packages(구버전)과 설치가 가능한 Available Packages(신버전)을 확인 할 수 있습니다.

```
[root@localhost yum.repos.d]# yum update -y mysql*
Setting up Update Process
Setting up repositories
Reading repository metadata in from local files
Resolving Dependencies
--> Populating transaction set with selected packages. Please wait.
---> Downloading header for mysql-server to pack into transaction set.
mysql-server-4.1.20-2.RHE 100% |=========================|  29 kB    00:00
---> Package mysql-server.i386 0:4.1.20-2.RHEL4.1 set to be updated
---> Downloading header for mysql-devel to pack into transaction set.
mysql-devel-4.1.20-2.RHEL 100% |=========================|  25 kB    00:00
---> Package mysql-devel.i386 0:4.1.20-2.RHEL4.1 set to be updated
---> Downloading header for mysql to pack into transaction set.
mysql-4.1.20-2.RHEL4.1.i3 100% |=========================|  35 kB    00:00
---> Package mysql.i386 0:4.1.20-2.RHEL4.1 set to be updated
--> Running transaction check

Dependencies Resolved

================================================================================
 Package                 Arch       Version           Repository         Size
================================================================================
Updating:
 mysql                   i386       4.1.20-2.RHEL4.1  update             2.9 M
 mysql-devel             i386       4.1.20-2.RHEL4.1  update             2.1 M
 mysql-server            i386       4.1.20-2.RHEL4.1  update             9.8 M

Transaction Summary
================================================================================
Install      0 Package(s)
Update       3 Package(s)
Remove       0 Package(s)
Total download size: 15 M
Downloading Packages:
(1/3): mysql-server-4.1.2 100% |=========================| 9.8 MB    00:09
(2/3): mysql-devel-4.1.20 100% |=========================| 2.1 MB    00:01
(3/3): mysql-4.1.20-2.RHE 100% |=========================| 2.9 MB    00:01
warning: rpmts_HdrFromFdno: V3 DSA signature: NOKEY, key ID 443e1821
Public key for mysql-server-4.1.20-2.RHEL4.1.i386.rpm is not installed
Retrieving GPG key from http://vault.centos.org/RPM-GPG-KEY-CentOS-4
Importing GPG key 0x443E1821 "CentOS-4 key <centos-4key@centos.org>"
Key imported successfully
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating  : mysql                       ######################### [1/6]
```

yum update -y mysql*을 실행하여 mysql을 최신버전으로 업데이트합니다.
MySQL 버전패치를 완료 후 서비스를 재시작 해주시면 되겠습니다.

< DB 원격 접속 관리>

```
root@aca8bd83:~
File  Edit  View  Search  Terminal  Help
[root@aca8bd83 ~]# mysql -h172.168.189.146 -uroot -p
Enter password:
ERROR 1130 (HY000): Host 'ACA8BD83.ipt.aol.com' is not allowed to connect to this MySQL server
```

원격접속을 외부IP에서 시도했으나 권한이 없음으로 원격접속을 차단한 것을 확인하였습니다.