대외유출주의

웹 보안 취약성 분석 결과보고서

㈜XXXXXX

www.XXXXX.co.kr

Revision History

Date	Version	Description	Author
2011.01.13	1.0	웹 취약점 보고서	홍 길 동

목 차

1. 개요

웹 취약점 진단은 고객사에서 운영중인 XXXXXX.co.kr사이트의 주요 서비스와 관련된 정보 자산들에 대한 보안 운영상의 취약점과 개선 사항을 파악하기 위한 것으로서, 웹 애플리케이션에 대한 분석을 통해 서버의 인증을 우회하거나 조작할 수 있는 가능성, 또는 주요정보를 유출할 수 있는 가능성이 존재하는지 점검한다.

외부의 공격자에 의해 악용될 수 있는 취약점을 찾아내고 해킹에 성공하였을 경우 이를 바탕으로 내부 시스템으로의 침입이 어느 정도까지 가능한지 알아보고 내부 기밀정보, 고객정보와 같이 최근 이슈화 되고 있는 개인정보 등의 주요 DB정보를 외부로 유출 시킬 수 있는지에 대해 점검한다.

1.1 점검 대상

대 상	IP 주 소
www.XXXXX.co.kr	192.168.1.234

1.2 진단 일정

구 분	일 자
웹 취약점 진단 점검기간	2011년 1월 10일 ~ 1월 13일

1.3 점검 인원

소 속	성 명 / E-Mail
솔데스크 ESPC 4기	홍 길 동 / test@test.com

2. 웹 취약점 점검 방법

2.1 수행 환경

- 외부 임의의 침입자가 대상 시스템에 대해 제한된 정보(IP,URL)만을 아는 상황이라고 가정한다.
- 테스트 수행자는 대상 시스템의 어떠한 특정 권한도 할당 받지 않은 상태이며, 따라서 외부 임의 사용자와 동일한 환경 아래에서 테스트를 수행한다.

2.2 수행 항목

본 웹 취약점 진단 테스트는 OWASP(Open Web Application Security Project)에서 지정한 '10대 웹애플리케이션 취약점(The Ten Most Critical Web Application Security Vulnerabilities)' 을 기준으로 실시하였다.

점검항목		내 용
OWASP 10	인젝션	· SQL, OS, LDAP인젝션과 같은 인젝션 결함은 신뢰할 수 없는 데이터가 명령어나 질의어의 일부분으로써 인터프리터에 보내질 때 발생한다.
	XSS	· XSS결함은 적절한 확인이나 제한 없이 어플리케이션이 신뢰할 수 없는 데이터를 갖고, 그것을 웹 브라우저에 보낼 때 발생한다.
	취약한 인증과 세션 관리	· 인증과 세션 관리와 연관된 어플리케이션 기능이 취약하여 권한 획득이 가능한 취약점
	안전하지 않은 직접 객체참조	· 파일, 디렉터리, 데이터베이스 키와 같이 내부적으로 구현된 객체에 대해 개발자가 참조를 노출할 때 발생한다.
	CSRF	· 사용자가 의도하지 않은 요청으로 인해 사용자 권한의 임의의 행위를 수행할 경우 발생한다.
	보안 설정상의 오류	· 보안을 위한 설정이 구현되어 있는지, 소프트웨어의 버전이 보안에 안전한 최신버전을 유지하는지 확인한다.
	안전하지 않은 암호 저장	· 신용카드 번호, 주민등록번호, 계정의 비밀번호와 같은 민감한 데이터에 대하여 안전한 암호화 저장을 지원하는지 확인한다.
	Redirect URL 접속 실패	· 감춰진 페이지에 접근하기 위하여 URL변조를 이용한 접근이 가능한지 확인한다.
	불충분한 전송 계층 보호	· 네트워크 트래픽의 인증,암호화, 비밀성과 무결성이 안전하게 보호되는지 확인한다.
	검증되지 않은 Redirect와 Forward	· 애플리케이션이 유효하지 않은 리다이렉트나 전송(Forward)을 보유하고 있는지 점검한다.

OWASP TOP 10 체크리스트

2.3 점검 도구

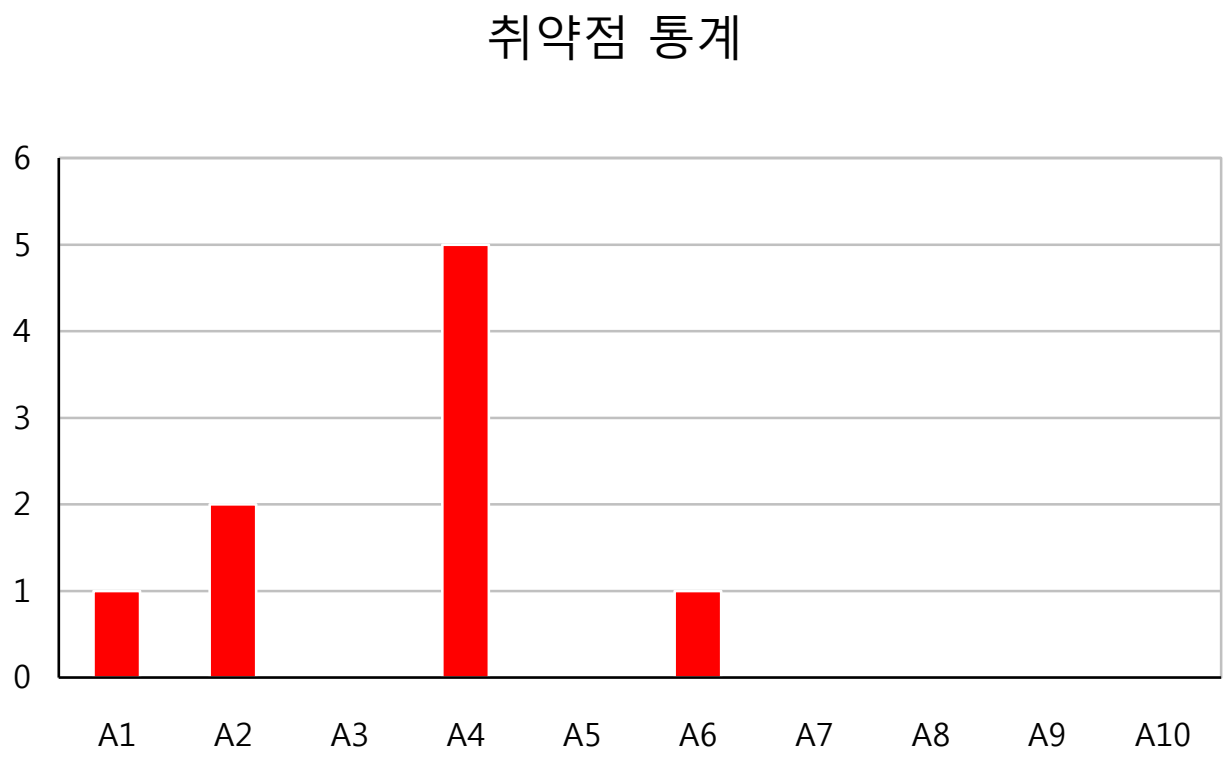
웹 취약점 진단 시에 다양한 취약점 점검 및 분석도구를 병행하여 사용하게 된다. 프로그램 및 용도는 다음과 같다.

명 칭	내 용
acunetix	웹 취약점 스캐너

3. 웹 취약점 진단 수행결과(요약)

3.1 총평

웹 취약점 진단은 www.xxxx.co.kr에 대하여 점검을 실시하였으며 OWASP TOP 10 취약점에 비중을 두어 웹 스캐너 도구 및 수작업 진단을 통해 다양한 취약점을 도출하는 방식으로 수행하였다.



해당 홈페이지에서는 XSS, SQL Injection, 직접객체 참조 등에서 취약점이 발견되었다.
SQL Inejction을 통하여 DB의 데이터를 획득할 수 있었고, XSS 취약점을 통하여 게시판에 악성 스크립트의 수행이 가능하였다. 또한, 관리자 페이지가 기본 설정인 admin, webmail, phpMyAdmin 등으로 설정되어 쉽게 발견되었다. 특히 phpMyAdmin의 경우 인증과정 없이 mysql root계정으로 연결되어 있어 해당 페이지에 접속한 공격자는 데이터 베이스의 열람 및 수정, 추가, 삭제가 가능하여 신속한 조치가 필요하다. 원격 서비스인 SSH, FTP, MySQL 서비스가 외부로 Open되어 있어 공격자로부터의 접속 가능성이 존재하며 특히 SSH서비스의 경우 예측 가능한 계정정보를 입력하여 SSH 쉘을 획득할 수 있었다.

3.2 웹 취약점 진단 결과요약

xxxxx.co.kr의 취약점 진단 결과를 요약하면 다음과 같다.

대상 서버	취약점 항목
www.xxxxx.co.kr	1. 커뮤니티 게시판 XSS 취약점 2. 커뮤니티 게시판 SQL Injection 취약점 3. 직접 객체 접근 취약점 4. 보안설정 오류로 인한 Directory Listing취약점 5. 원격 서비스(SSH)접속 가능

4. 웹 취약점 수행결과(상세)

4.1 www.xxxxx.co.kr

해당 홈페이지에서는 XSS, SQL Injection 직접객체 접근 등의 취약점이 발견되었다.
XSS를 통하여 악성 스크립트를 게시판에 업로드할 수 있으며, SQL Injection공격으로 서버의 주요정보를 알아낼 수 있다. 또한 직접객체를 호출하여 인증절차 없이 스팸등의 게시글을 등록할 수 있는 취약점이 존재한다.

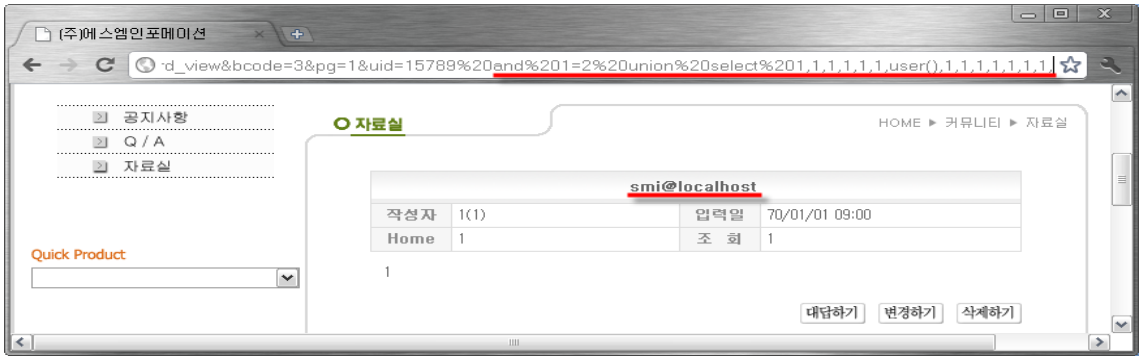
4.1.1 SQL Injection 취약점

■ **HOME > 커뮤니티 > 게시판(공지사항/QA/자료실)**

- **http://xxxx.co.kr/user_brd/bjboard.php?req=brd_write&mode=new&bcode=[Injection Point]**

  홈페이지의 게시판 분류코드 파라미터 값의 변조를 통해 SQL Injection공격이 가능하다.
  공격을 통해 데이터베이스의 정보를 획득할 수 있다.

- **취약점 상세화면**



➢ **해결방안**

사용자 입력 값에 유해 패턴(SQL 쿼리, 스크립트 HTM태그 등) 삽입여부를 검사한다.

PHP환경의 예

```
$query=sptintf("SELECT id,password,username FROM user_table WHERE id='%s';",addslashes($id));
// id 변수를 문자형으로 받고, id 변수의 특수문자를 일반문자로 변환한다.

// @로 php에러 메시지를 막는다.
$result=@OCIParse($conn, $query);
if(!@OCIExecute($result))
error("SQL 구문 에러");
exit;
```

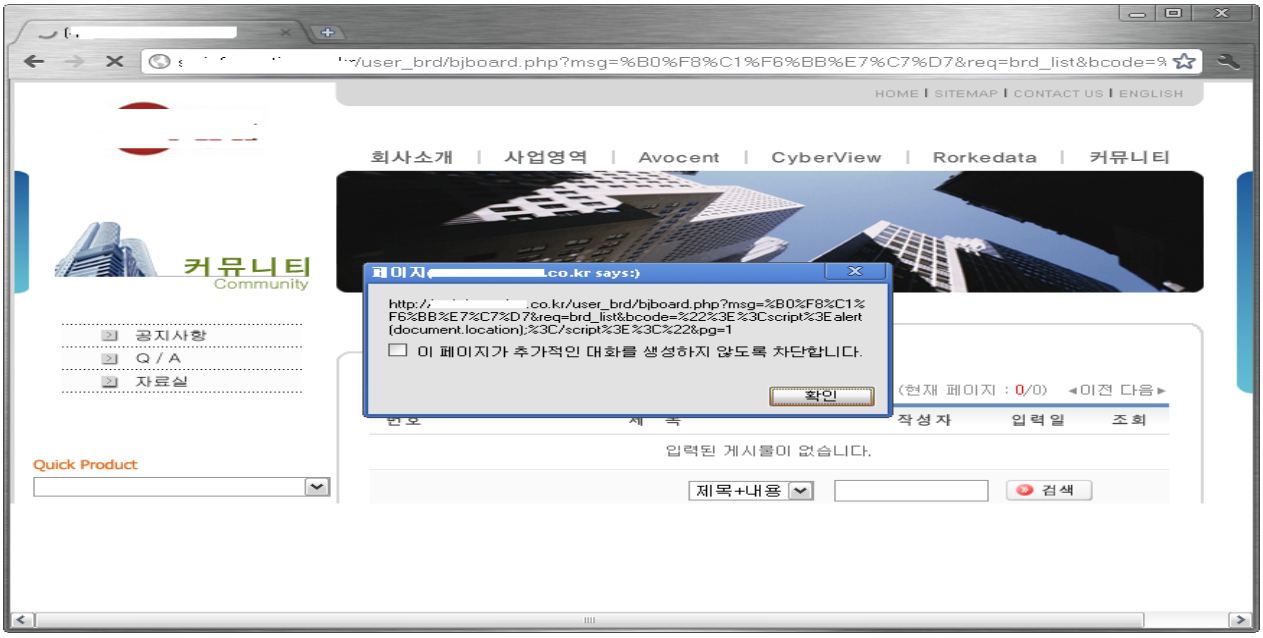
4.1.2 XSS(Cross Site Scripting)취약점

■ **HOME > 커뮤니티 > 게시판(공지사항/QA/자료실)**

- **http://xxxx.co.kr/user_brd/bjboard.php?bcode=[Injection Point]**

  홈페이지의 게시판 분류코드 파라미터 값의 변조를 통해 임의의 스크립트 실행이 가능하다.

- **취약점 상세 화면**

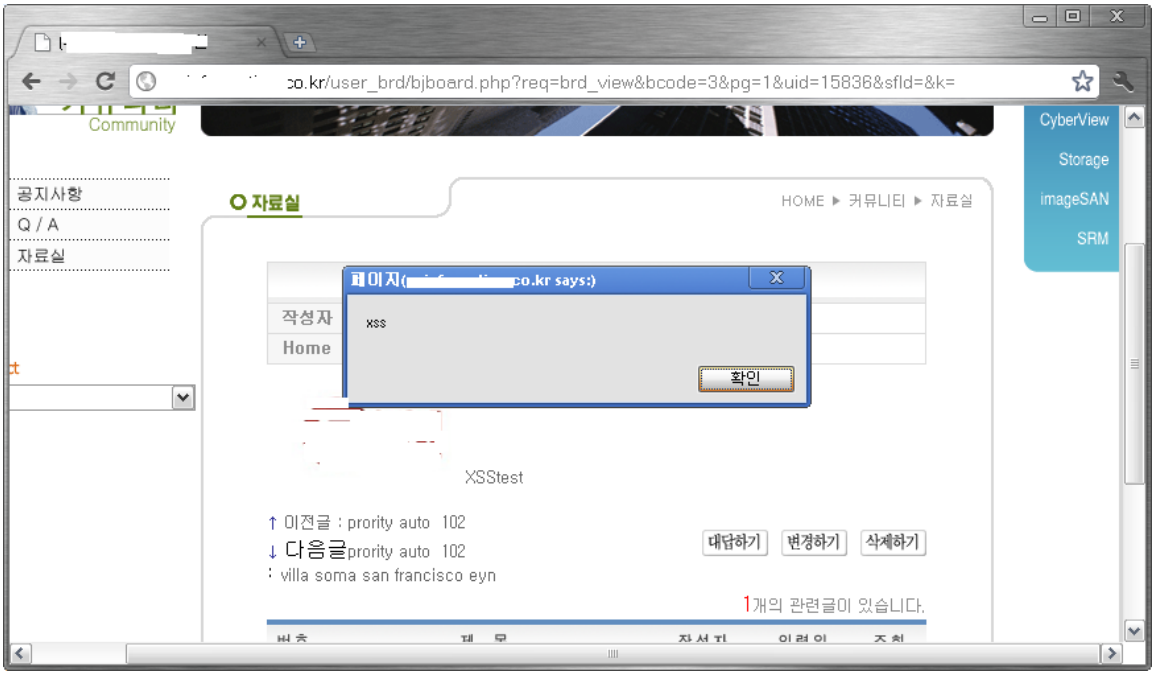


■ **HOME > 커뮤니티 > 자료실**

- **http://xxxx.co.kr/user_brd/bjboard.php?req=brd_write&mode=new&bcode=3**

  자료실 게시판에 스크립트 입력시 해당 스크립트가 실행된다.

- **취약점 상세화면**



➢ **해결방안**

사용자 입력 값 내에 유해 태그의 포함 여부를 검사하여, 차단 또는 태그가 실행되지 않도록 변환하여 처리한다.

PHP환경의 예

```
$use_tag="img,font,p,br";    //허용할 HTML tag
if($use_html==1)    //HTML tag를 사용하게 할 경우 부분 허용
$memo=str_replace("<", "&lt;", $memo);    //HTML TAG를 모두 제거
$tag=explode(",", $use_tag);
for($i=0; $i<count($tag); $i++)    //허용할 TAG만 사용 가능하게 변경
$memo=eregi_replace("&lt;".$tag[$i]." ", "<".$tag[$i]." ", $memo);
$memo=eregi_replace("&lt;".$tag[$i].">", "<".$tag[$i].">", $memo);
$memo=eregi_replace("&lt;/".$tag[$i],"</ ".$tag[$i], $memo);
else    //HTML tag를 사용하지 못하게 할 경우
// $memo=htmlspecialchars($memo);
// htmlspecialchars() 사용시 일부 한글이 깨어지는 현상이 발생할 수 있음.
$memo=str_replace("<", "&lt;", $memo);
$memo=str_replace(">", "&gt;", $memo);
```

4.1.3 직접객체 접근 취약점

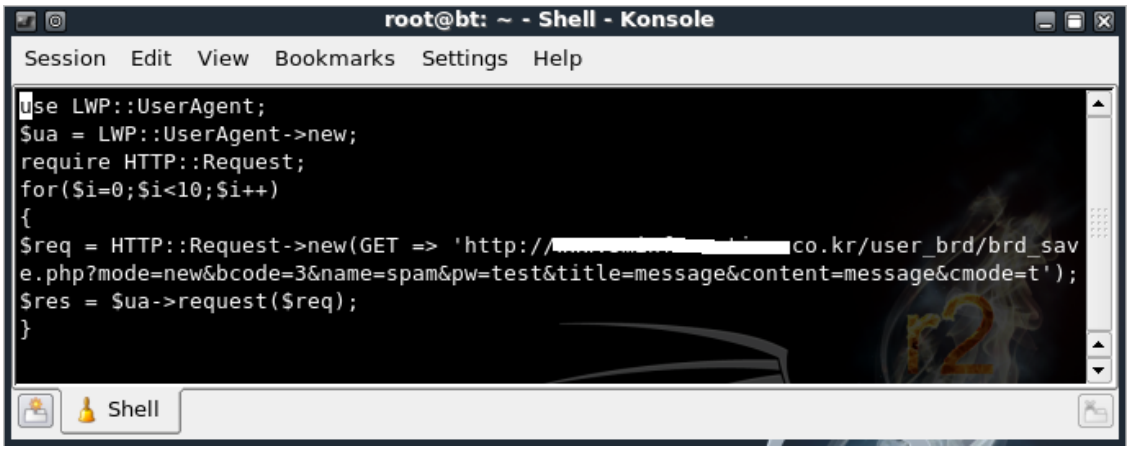
■ **HOME > 커뮤니티 > 게시판(공지사항/QA/자료실)**

- xxxx.co.kr/user_brd/brd_save.php

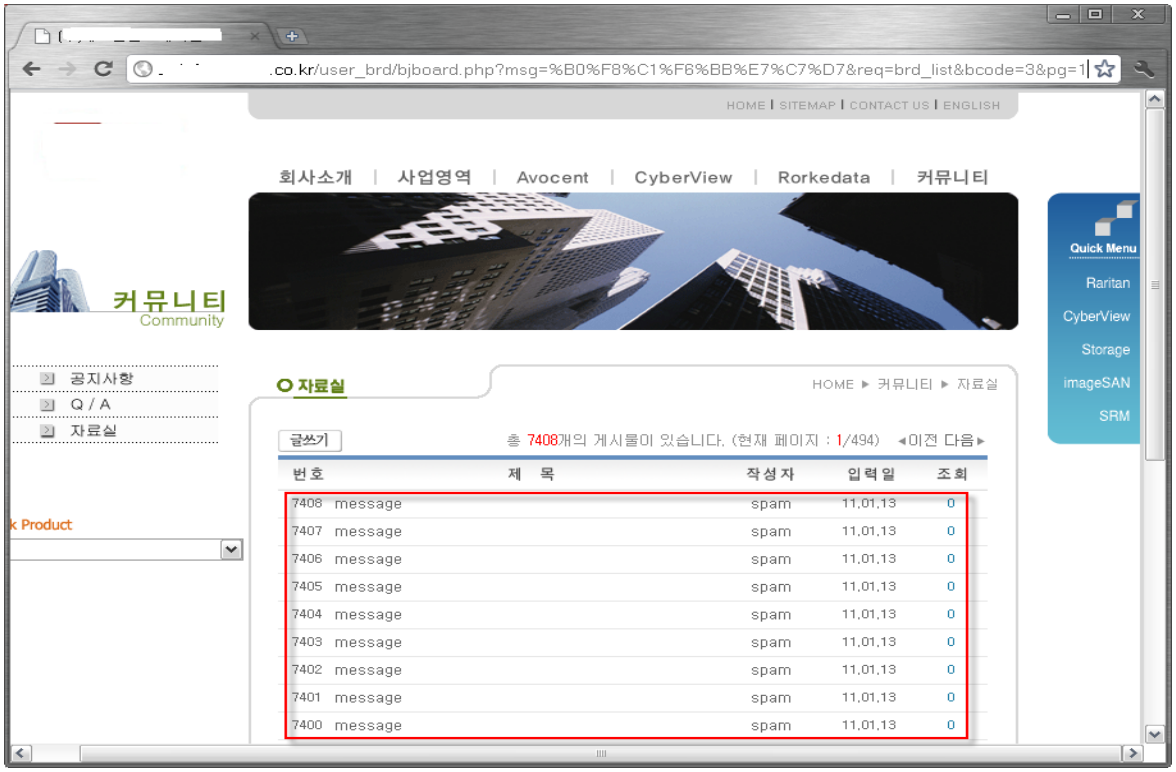
쿼리문의 직접전송을 통해 올바른 경로를 통하지 않고도 컨텐츠의 업로드가 가능하다.

- 취약점 상세화면

아래와 같은 쿼리를 자동으로 전송하는 스크립트를 작성하여 실행



악성 컨텐츠가 대량으로 등록된 모습



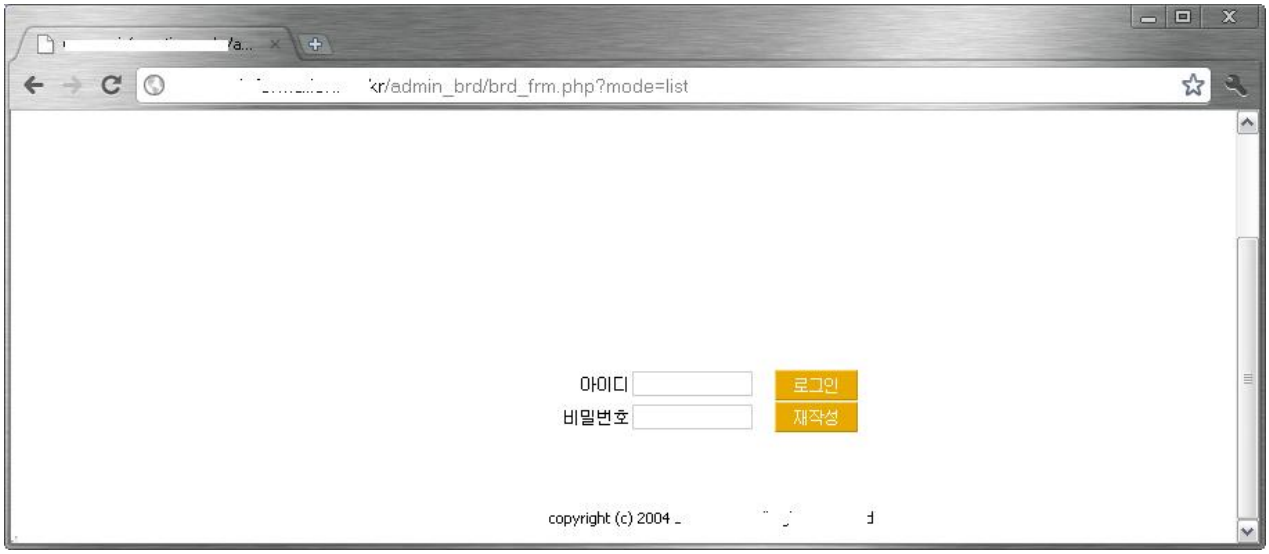
➢ **해결방안**

정상적인 경로를 통해서만 컨텐츠의 등록이 가능하도록 2단계 이상의 검증절차를 수행하거나 authenticity token을 사용한다.

■ **관리자 페이지 노출**

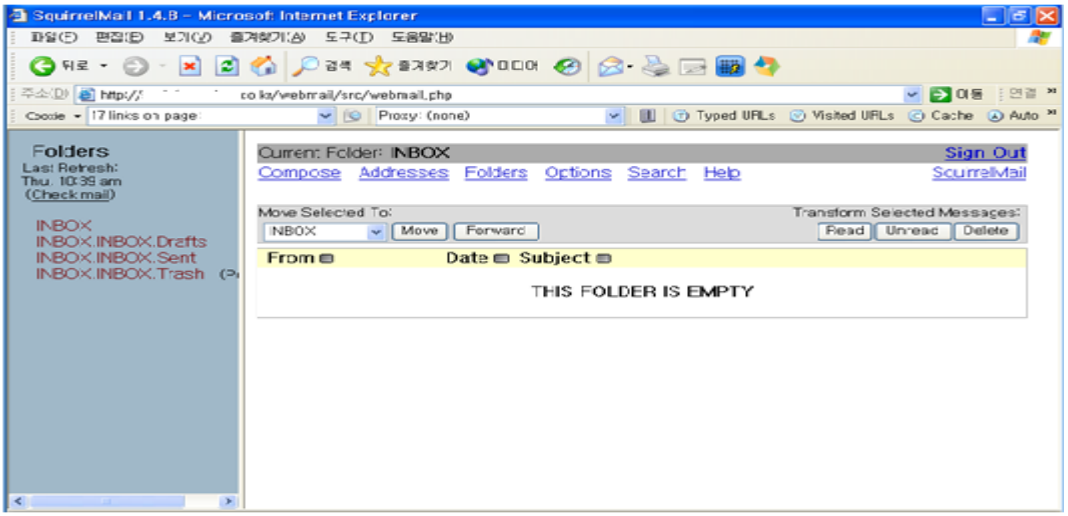
- xxxx.co.kr/admin_brd/brd_frm.php?mode=list

예측가능한 웹 관리자 페이지의 경로가 존재하며 해당 페이지로의 접근이 허용된다.



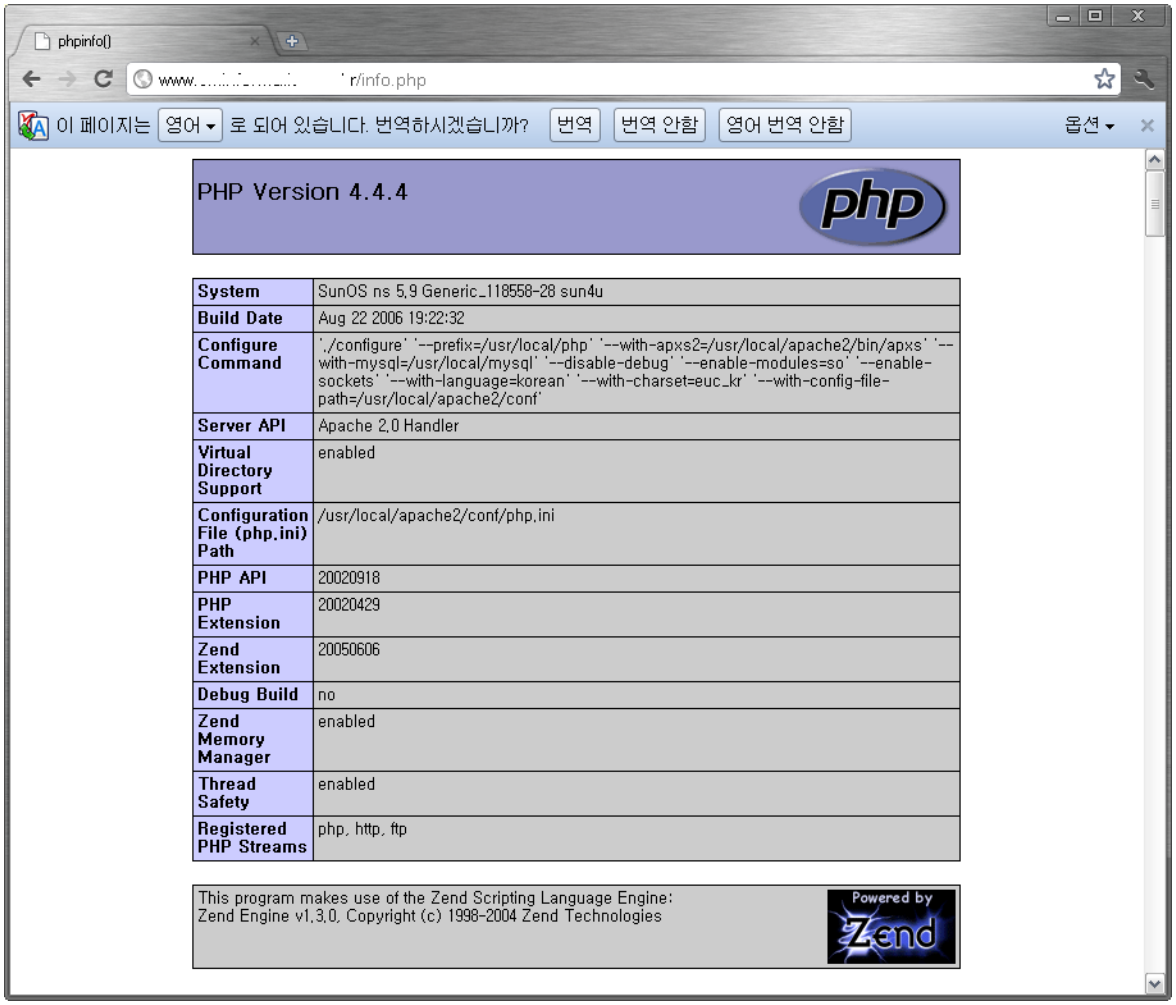
- **xxxx.co.kr/webmail/src/login.php**

메일관리자 페이지의 경로가 존재하며 예측가능한 관리자 계정정보를 사용하여 로그인이 가능하다.



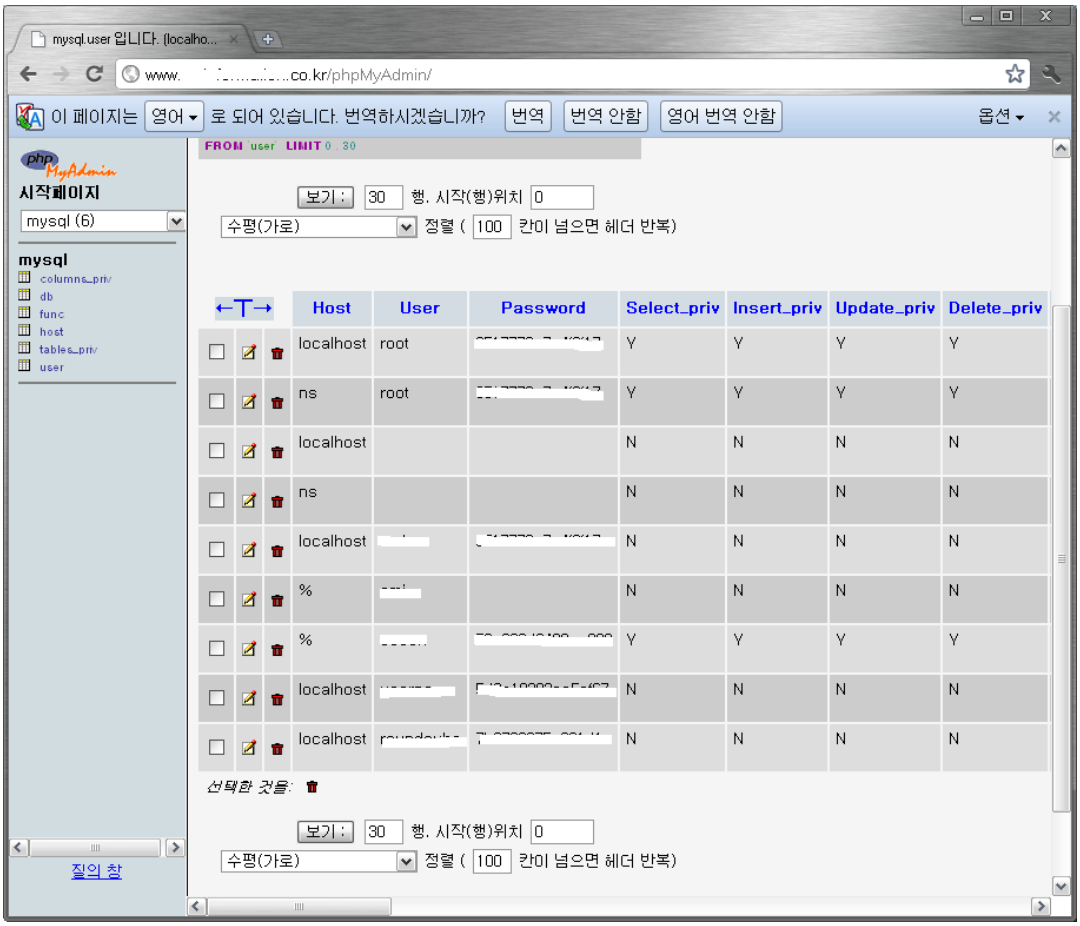
- **xxx.co.kr/info.php**

phpinfo함수를 사용하는 PHP파일명이 존재하며 해당 파일을 요청하여 PHP웹서버 정보를 확인할 수 있다.



- xxxx.co.kr/phpMyAdmin/

phpMyAdmin프로그램의 사용을 확인하였으며 관리자의 계정 인증 없이 Mysql root계정으로 접근이 가능하다.



➢ **해결방안**

관리자 인증 페이지에 대한 원격 접근을 차단하며 , 원격 접근이 필요할 경우 임의의 IP에만 접근을 허용하도록 한다. 또한 모든 관리자 페이지는 관리자 인증 여부 검사를 수행한다.

PHP환경의 예

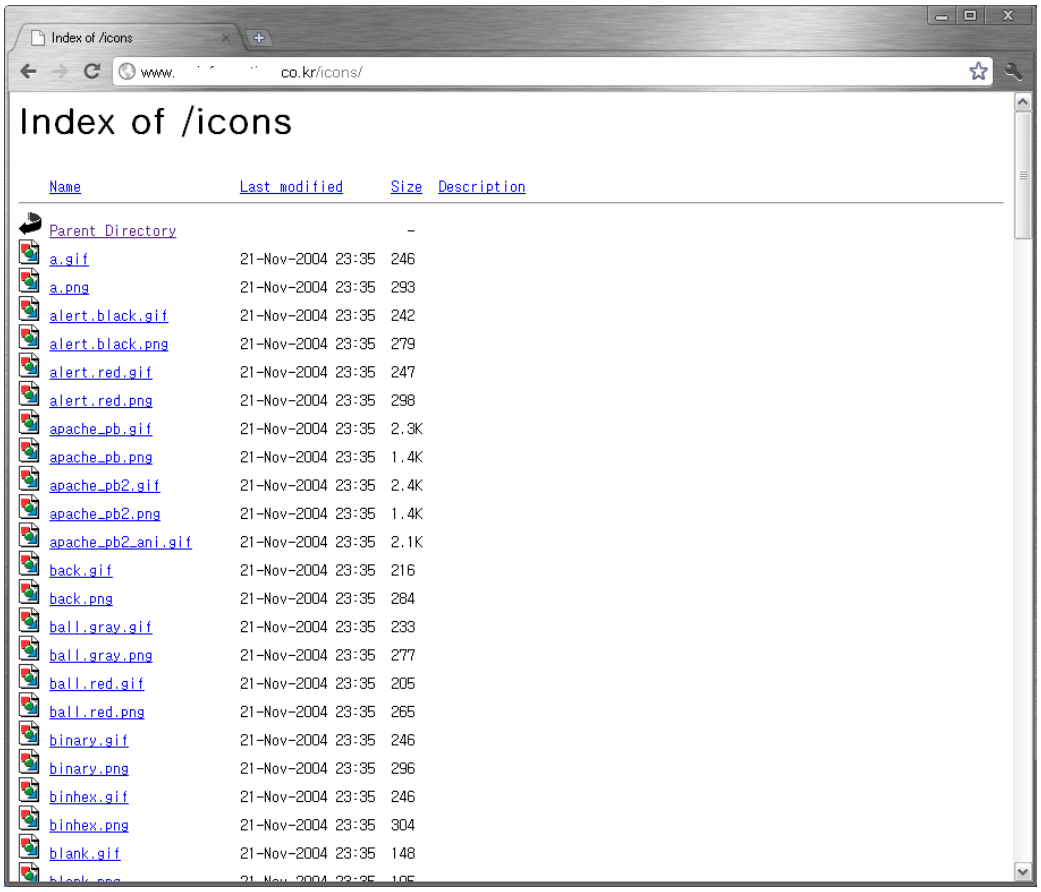
```
@session_start();
If(!myfunc_userauth($userid, $userpw) || $_SERVER[“REMOTE_ADDR”]!=”10.10.1.1”
Print “인증실패”;
LogSave(userid, user_ip, 0)
If(!session_is_registered(“logged_in”))
$logged_in = 1;
$user_ip = $_SERVER[“REMOTE_ADDR”];
Session_register(“logged_in”);
Session_register(“userid”);
Session_register(“user_ip”);
```

4.1.4 Directory Listing 취약점

■ **icons디렉터리 노출**

- xxxx.co.kr/icons/

디렉터리에 직접 접근하여 내부 파일의 열람이 가능하다.



➢ **해결방안**

Apache환경의 예

Httpd.conf 환경설정 파일에서 Options 항목 뒤의 Indexs라는 단어를 지우고 파일을 저장한다. 이때 Options는 디렉터리 별로 설정할 수 있게 되어 있으므로 모든 디렉터리에 대해서 Options항목 뒤에 Indexs를 삭제한다.

삭제 후 Apache데몬을 재 시작한다.

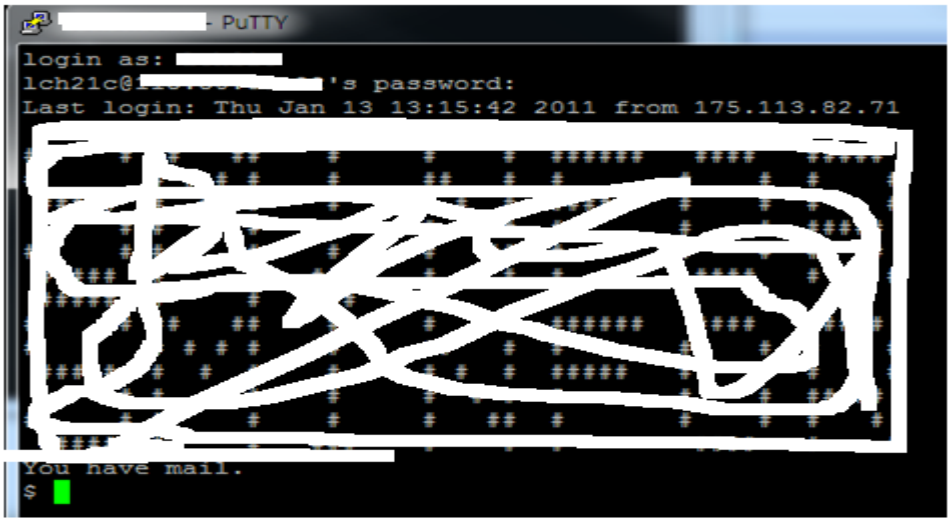
```
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "C:/APM Setup/htdocs">
    Options Indexes FollowSymLinks MultiViews ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#
# UserDir: The name of the directory which is appended onto a user's home
# directory if a ~user request is received.
#
```

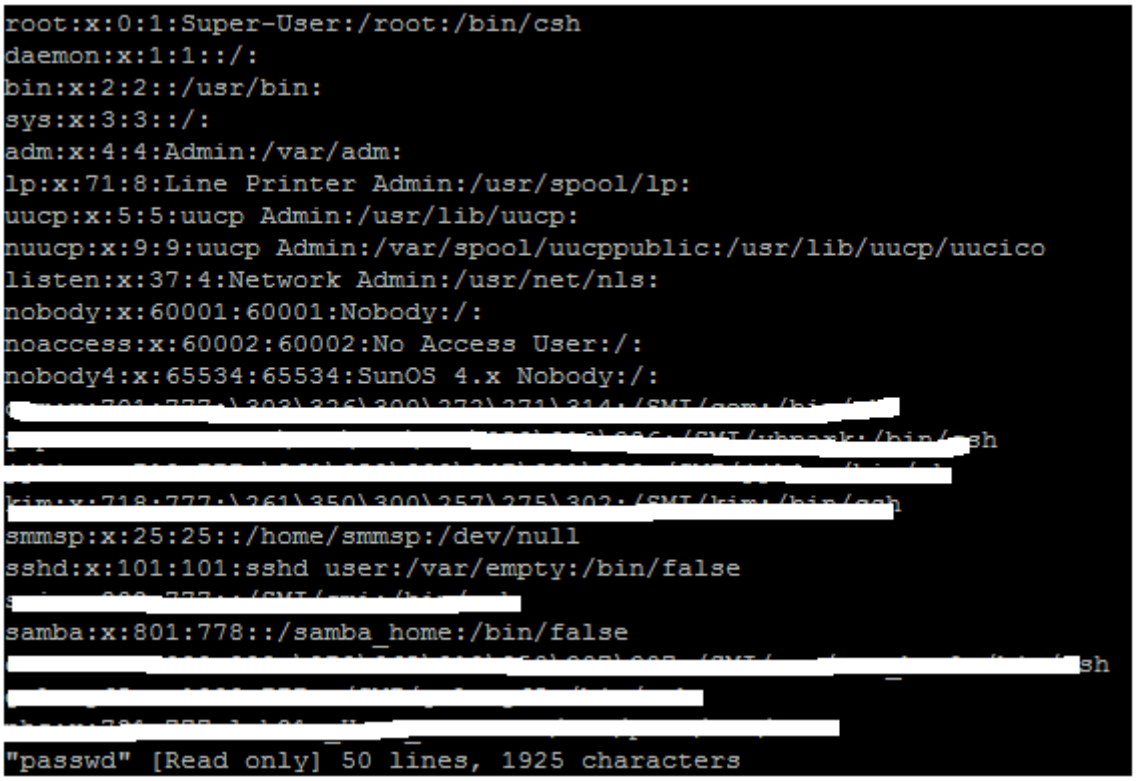
4.1.5 원격 서비스 접속 가능

■ **SSH 서비스 접속 가능**

- xxx.xxx.xxx.xxx

SSH클라이언트를 통하여 예측 가능한 관리자 계정으로 로그인이 가능하다. 접속 이후 서버상의 민감한 파일을 열람하거나 탈취할 수 있다.





➢ **해결방안**

서버 관리자의 계정정보를 공격자가 쉽게 예측할 수 없도록 수정한다.
관리자의 IP에 한하여 접속이 가능하도록 ACL등의 보안정책을 수립한다.