

PHP 웹셸의 분석과 대응 방안

PHP 기반 웹셸의 동작 원리와
공개 웹셸의 기능 분석 및 대응 방안

작성자 : 동명대학교 THINK 정정홍 (zeratul621@naver.com)

1. 시작하면서	p. 2
2. 웹셸의 동작 원리	p. 3
3. r57shell	p. 5
4. kcWebTelnet	p. 9
5. phpRemoteView	p. 10
6. 웹셸 대응 방안	p. 12

1. 시작하면서

웹셸(WebShell)이란, 웹 기반에서 동작하는 셸 프로그램을 의미한다. 일반적으로 PHP, ASP, JSP 등과 같은 웹 스크립트 언어에서는 웹 서버에 콘솔 기반 명령어를 실행할 수 있는 함수나 문법을 지원하고 있는데, 이런 기능을 이용하여 마치 웹에서 SSH나 Telnet을 사용하는 것처럼 셸 프로그램을 만들어 사용할 수 있다.

하지만, 누구든지 접근이 용이한 웹 환경에서 셸을 사용할 수 있다는 점 때문에 최근 웹셸은 각종 침해사고에 악용되고 있다. 만약 어느 웹 사이트의 게시판에 파일을 업로드 할 수 있는 권한이 있고, 업로드 기능에 웹 스크립트 언어 확장자(*.php, *.asp, *.jsp, *.html 등)에 대한 필터링이 없다면 공격자는 웹셸을 업로드하여 해당 서버의 권한을 쉽게 획득할 수 있다. 웹셸을 사용할 수 있게 되면, 공격자는 웹 사이트내의 코드를 보거나, 개인정보를 유출 및 변조, 그리고 서버에 백도어를 심는 등 서버를 공격자 마음대로 제어할 수 있다.

또한, 웹셸은 그 특성상¹⁾ 바이러스 백신 프로그램에서 탐지를 잘 하지 않기 때문에²⁾ 서버 관리자가 웹셸을 탐지해내기 어렵다. 때문에 웹셸을 이용한 공격에 의해 침해사고를 당했을 경우, 그 피해 정도가 심각해질 수 있다.

본 문서에서는 PHP 기반 웹셸의 동작 원리와 인터넷상에 공개되어 있는 PHP 기반 웹셸들의 기능을 알아볼 것이다. 그리고 그에 대한 대응 방법과 웹셸을 탐지해내는 방법에 대해 알아보려고 한다.

1) 정상적인 웹 프로그램에도 시스템 명령을 실행하는 코드가 있을 수 있다.

2) 최신 버전의 V3나 카스퍼스키 등의 몇몇 백신 프로그램에서는 알려진 웹셸의 탐지가 가능하다.

2. 웹셸의 동작 원리

앞서 <시작하면서> 에서도 언급하였지만, 웹셸은 기본적으로 웹 스크립트 언어의 시스템 명령을 실행할 수 있는 함수나 문법을 활용하여 동작한다.

그렇다면, 시스템 명령을 실행하는 함수와 문법에는 어떤 것들이 있을까?

웹 서비스에 널리 쓰이는 언어인 PHP를 예로 들어보도록 하자. PHP에서는 다음과 같이 시스템 명령어를 실행할 수 있는 함수를 제공하고 있다.

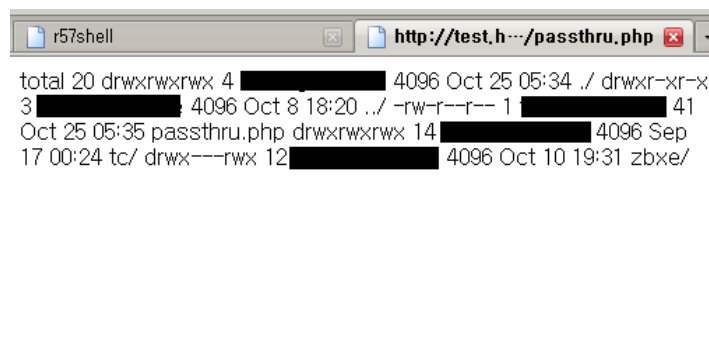
```
- passthru()
(참고 : http://www.php.net/manual/en/function.passthru.php)

- system()
(참고 : http://www.php.net/manual/en/function.system.php)
```

위 함수의 사용법은 간단하다.

다음과 같이 "ls -laF" 명령어를 실행하는 예제 소스 코드를 작성하여 간단한 테스트를 해보도록 하자.

```
<?php
    echo passthru("ls -laF", $v);
?>
```



[그림 1] 시스템 명령어를 실행한 화면

우리는 위 화면으로부터 웹 스크립트 언어를 이용하여 시스템 명령의 실행이 가능하다는 것을 알 수 있다.

그렇다면, 이러한 방식으로 시스템 명령어를 실행하면 어느 유저의 권한으로 실행될까? 결론부터 말하자면 실행중인 웹 서비스 데몬의 권한으로 실행된다. 일반적으로 Apache 웹서버 데몬은 nobody 유저의

권한으로 실행되며, 우분투 Apache 웹서버의 경우에는 www-data 유저의 권한으로 실행된다. 행어나 Apache 설치를 잘못하여 root 권한으로 Apache 데몬이 실행되고 있다면 매우 위험하다. 그 상태에서 만약 파일 업로드나 원격 실행에 취약한 프로그램을 사용하고 있다면 해당 서버의 미래는 불 보듯 뻔할 것이다.

하지만, nobody 권한으로 웹서버가 실행되고 있더라도 웹셸을 실행할 수만 있다면 공격자가 서버에 행할 수 있는 수단은 매우 많다.

이와 같은 방법을 이용하여 공격자의 명령어를 실행하고, 해당 결과를 일목요연하게 정리하여 보여주는 프로그램이 바로 웹셸(WebShell)이다. 웹셸은 공격자의 명령을 실행하여 결과만을 보여주는 단순한 것에서부터 서버 정보를 보여주고, 데이터베이스를 조작하거나 공격하는 것 등 다양한 종류의 웹셸이 있다. 이러한 웹셸들은 검색엔진에서 검색하면 손쉽게 구할 수 있다³⁾.



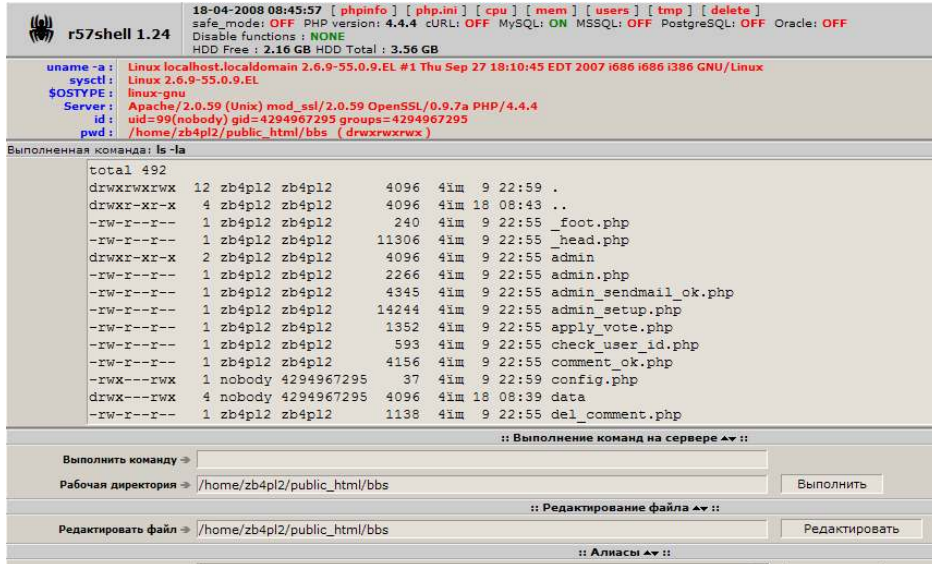
[그림 2] Google 검색엔진에서 "webshell" 이라는 키워드로 검색한 화면

다음 절부터는 해커들 사이에서 널리 사용되는 웹셸의 기능과 동작 원리, 그리고 대응 및 탐지 방안에 대해서 알아보도록 하겠다.

3) 2008년 10월 25일 기준으로 Google 검색엔진에서 "webshell" 을 검색하면 약 335,000 개의 결과가 검색된다.

3. r57shell

◎ 소개



[그림 3] r57shell의 실행 화면

PHP 환경에서 동작하는 웹셸이다. 단순히 터미널 환경을 웹에서 구현해주는 정도를 넘어 서버의 정보, 서버의 상태, 서버 사양 등 모든 정보를 한눈에 볼 수 있는 등 강력한 기능을 제공한다. 이외에 다양한 데이터베이스를 지원하며, DB 정보를 열람하거나 조작을 가할 수도 있다. 특히, 공격에 자주 쓰이는 기능들을 정리하여 편하게 명령어 또는 스크립트로 실행을 할 수 있다는 점이 매력이다.

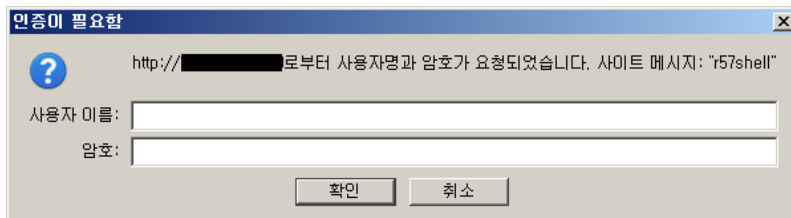
기본적으로 러시아어로 설정되어 있지만, 간단한 소스 코드 수정을 통해 영문으로 사용할 수 있는 기능도 지원한다.

◎ 사용 환경

- 실행 기반 : PHP
- 지원 데이터베이스 : cURL, MySQL, MSSQL, PostgreSQL, Oracle

◎ 주요 기능

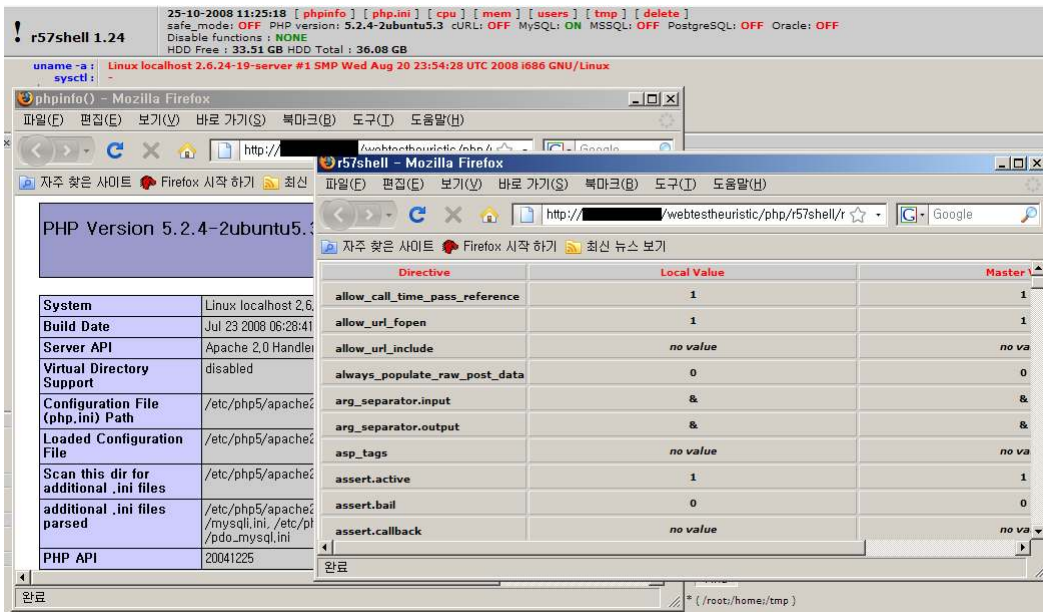
1) 로그인 기능



[그림 4] r57shell의 로그인 기능

r57shell은 사용자 인증 기능을 지원한다. 간단한 소스 코드 수정을 통해, r57shell에 인증 사용자 와 암호를 설정할 수 있다.

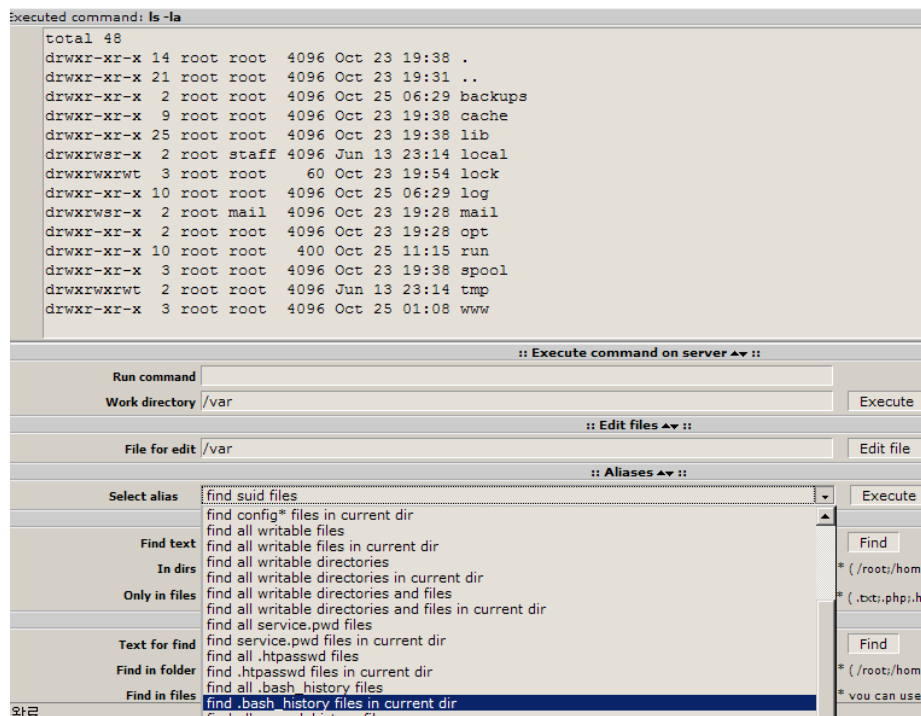
2) 서버 정보 열람 기능



[그림 5] r57shell로 서버 정보를 열람한 모습

r57shell은 서버내의 다양한 정보를 열람할 수 있는 기능을 지원한다. phpinfo()의 실행 결과, php.ini 설정파일 정보, 현재 서버에 존재하는 유저 리스트 등을 열람할 수 있다. 따라서 공격자는 웹 서버의 설정 환경과 사용자 정보 등을 한 눈에 볼 수 있다.

3) 터미널(Terminal) 기능

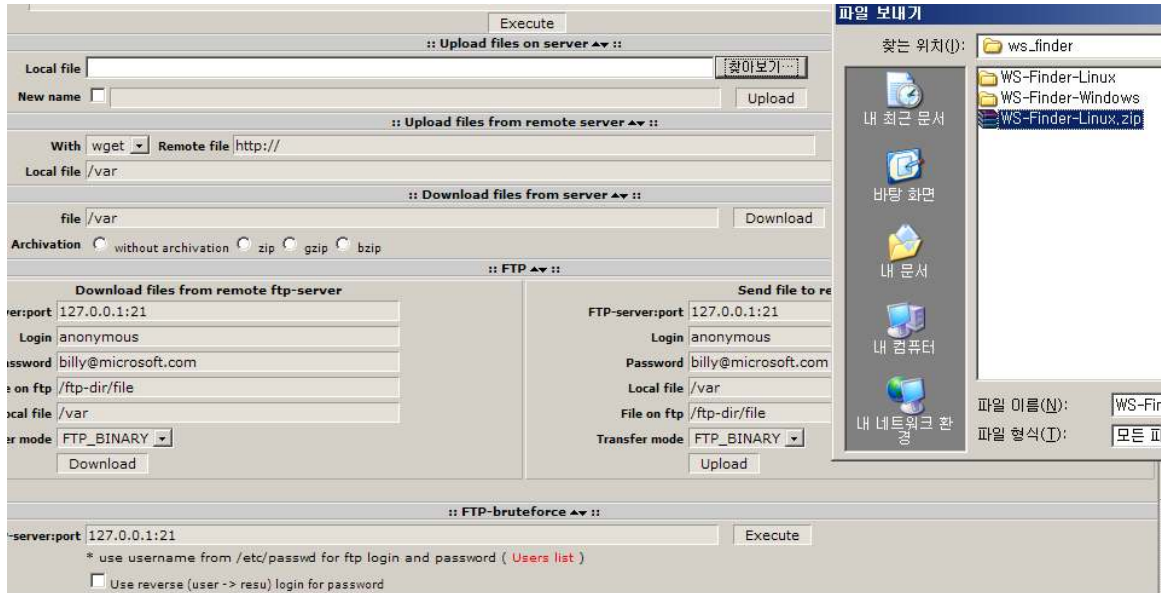


[그림 6] r57shell의 강력한 터미널 기능

r57shell은 보다 강력한 터미널 기능을 지원한다. 단순한 시스템 명령 실행/결과 출력 정도를 넘어

특정 파일을 편집하거나⁴⁾ 공격에 자주 쓰이는 명령어나 매크로를 쉽게 실행할 수 있도록 제공한다. 또한 공격자가 원하는 형태의 파일을 쉽게 찾을 수 있는 기능까지 제공한다.

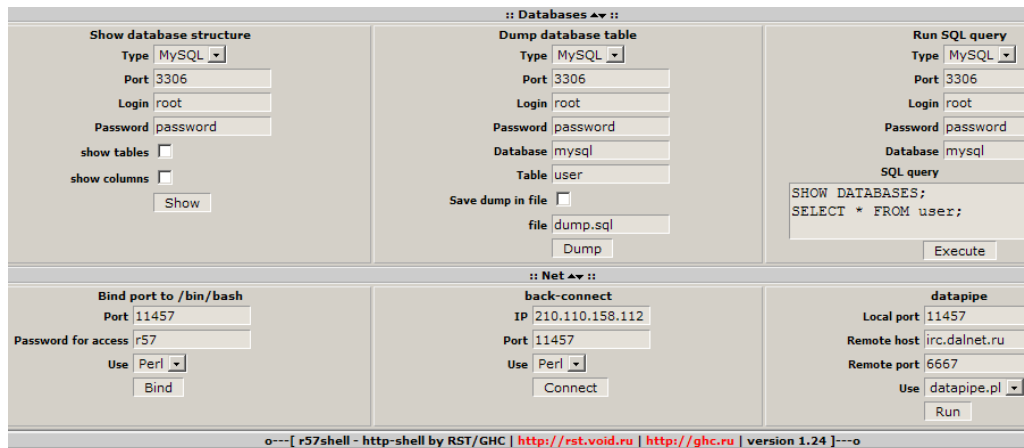
4) 파일 업로드/다운로드 기능



[그림 7] r57shell의 파일 업로드 / 다운로드 기능

r57shell은 해당 서버에 파일을 업로드/다운로드 할 수 있는 기능을 제공한다. 로컬 파일을 업로드 할 수 있는 기능에서부터 FTP 서버에서 업로드/다운로드하기, wget 명령어를 사용하기 등이 가능하다. 심지어 웹 서버에 FTP 서버가 있다면, FTP 서버에 무차별 대입 공격(bruteforce) 공격을 할 수 있는 기능까지 있다.

5) 데이터베이스 조작 기능



[그림 8] r57shell의 데이터베이스 조작 기능

r57shell의 가장 큰 특징으로는 데이터베이스를 조작할 수 있는 기능을 지원한다는 것이다. 기본적으로 PHP와 함께 널리 쓰이는 MySQL 뿐만 아니라, MSSQL, PostgreSQL, Oracle 등의 DB까지 조작

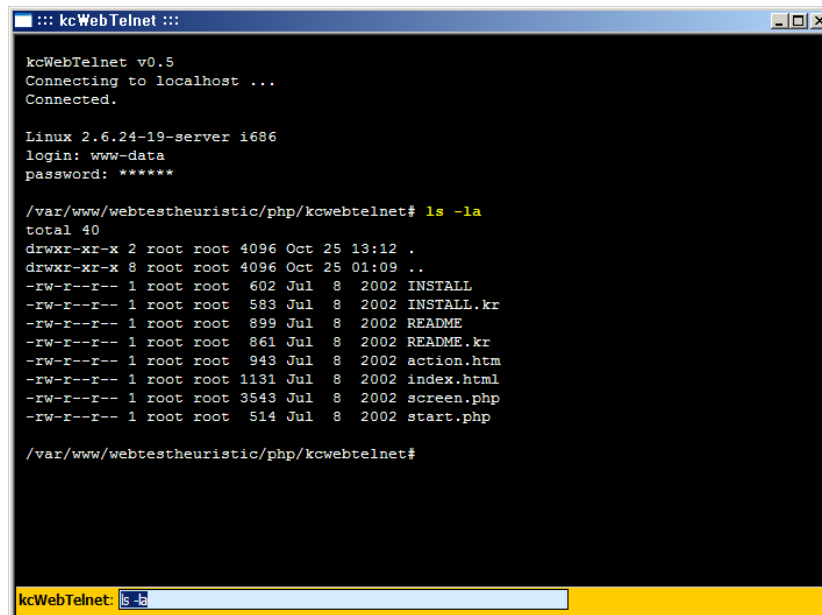
4) 물론 파일을 편집하고자 할 때에는 해당 파일이나 디렉토리의 권한(Permission)에 영향을 받는다.

할 수 있다. 공격자는 r57shell을 이용하여 DB에 임의의 쿼리문을 실행하거나, 공격자가 원하는 DB를 dump 받을 수 있다⁵⁾.

5) 단, 해당 데이터베이스의 로그인 가능한 계정명과 비밀번호를 알고 있어야 조작이 가능하다.

4. kcWebTelnet

◎ 소개



```
kcWebTelnet v0.5
Connecting to localhost ...
Connected.

Linux 2.6.24-19-server i686
login: www-data
password: *****

/var/www/webtestheuristic/php/kcwebtelnet# ls -la
total 40
drwxr-xr-x 2 root root 4096 Oct 25 13:12 .
drwxr-xr-x 8 root root 4096 Oct 25 01:09 ..
-rw-r--r-- 1 root root 602 Jul 8 2002 INSTALL
-rw-r--r-- 1 root root 583 Jul 8 2002 INSTALL.kr
-rw-r--r-- 1 root root 899 Jul 8 2002 README
-rw-r--r-- 1 root root 861 Jul 8 2002 README.kr
-rw-r--r-- 1 root root 943 Jul 8 2002 action.htm
-rw-r--r-- 1 root root 1131 Jul 8 2002 index.html
-rw-r--r-- 1 root root 3543 Jul 8 2002 screen.php
-rw-r--r-- 1 root root 514 Jul 8 2002 start.php

/var/www/webtestheuristic/php/kcwebtelnet#
```

[그림 9] kcWebTelnet의 실행 화면

kcWebTelnet은 한국인 개발자가 제작하여 배포한⁶⁾ 웹셸 프로그램이다. 명령어만을 실행하고 결과를 보여주는 단순한 기능만을 지원하지만, 인터페이스가 마치 유닉스 셸의 모습과 매우 흡사하고, 명령어를 실행하고 결과를 확인하기가 편리하다는 특징이 있다.

◎ 사용 환경

- 실행 기반 : PHP 4.x

◎ 주요 기능

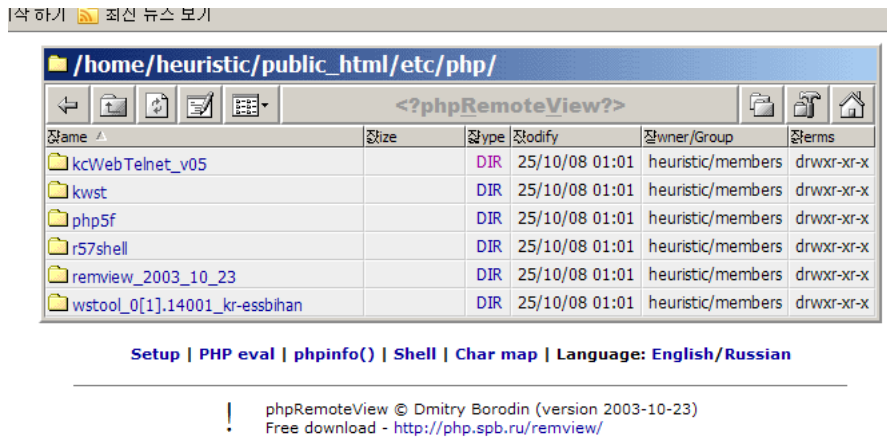
1) 터미널(Terminal) 기능

대부분의 웹셸 프로그램에서 지원하는 기능이다. 하지만, kcWebTelnet은 유닉스 셸과 흡사한 터미널을 제공해 주며, 명령어 실행 후에 실행하고자 하는 명령어를 입력하여 엔터키를 이용하여 실행할 수 있기 때문에 정적인 웹 환경에서도 마치 동적인 콘솔 환경처럼 웹셸을 다룰 수 있다.

6) kcWebTelnet의 소스 코드를 살펴보면 개발자 정보가 나와 있다.

5. phpRemoteView

◎ 소개



[그림 10] phpRemoteView의 실행 화면

phpRemoteView 웹shell은 윈도우즈 탐색기 형태의 인터페이스를 제공해 주는 것이 특징이다. Setup 메뉴를 통해 웹shell의 글꼴, 색상 등을 변경할 수 있고, phpinfo()의 실행 결과 모습, 공격자가 직접 서버에 명령어를 실행할 수 있는 기능 등을 지원한다.

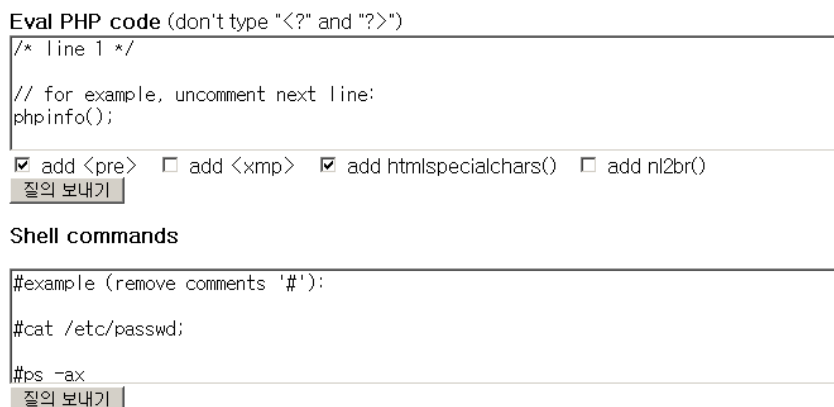
◎ 사용 환경

- 실행 기반 : PHP

◎ 주요 기능

1) PHP 코드 및 셸 명령 실행 기능

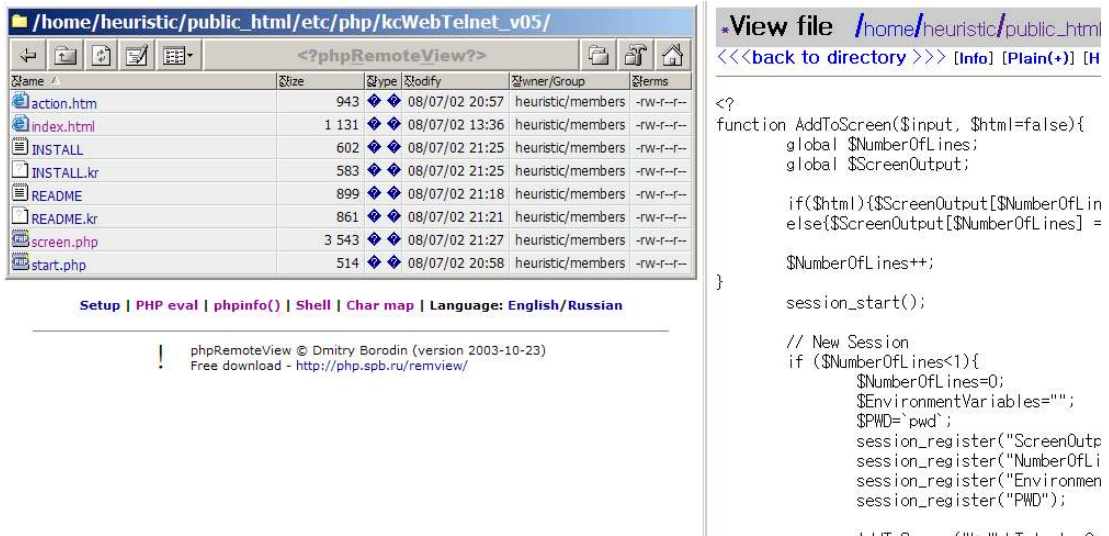
[START PAGE](#) | [Eval/Shell](#) | [Character map](#)



[그림 11] phpRemoteView의 PHP 코드 실행 및 명령 실행 기능

phpRemoteView는 입력 폼에 PHP 코드를 입력받아 실행하거나 시스템 명령을 실행할 수 있는 기능을 제공한다. 공격자는 공격용 소스 코드를 입력 필드에 입력하여 쉽게 서버를 공략할 수 있다.

2) 파일 탐색 및 소스 보기 기능

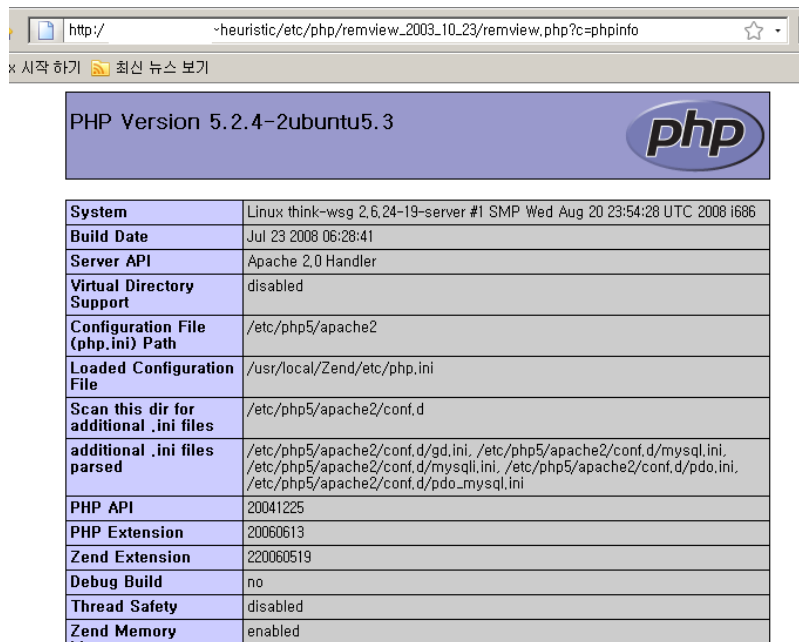


[그림 12] phpRemoteView의 파일 탐색 및 소스 보기 기능

phpRemoteView는 윈도우즈 탐색기 형태의 파일 탐색 및 소스 보기 기능을 지원한다. 공격자는 웹 서버의 디렉토리 구조를 쉽게 파악할 수 있고, 해당 파일에 해당하는 링크를 클릭하면 파일의 소스 코드를 보여준다.

또한, 소스 보기 페이지에서 해당 파일의 HexDump 정보를 보거나, 해당 파일을 편집 또는 다운로드 할 수 있는 기능까지 제공한다(물론 해당 파일에 대한 쓰기 권한이 있어야 한다).

3) 서버 정보 열람 기능



[그림 13] phpRemoteView의 서버 정보 열람 기능

`phpinfo()` 함수를 실행하여 해당 웹 서버의 서버 정보를 열람할 수 있다.

6. 웹쉘 대응 방안

우리는 지금까지 웹쉘의 동작 원리와 인터넷에 공개된 몇몇 웹쉘의 특징에 대하여 알아보았다. 이번 절 부터는 웹쉘의 패턴을 분석하여 웹쉘의 업로드를 차단하는 방법과 웹쉘을 탐지하는 방법 등에 대해 알아보도록 할 것이다.

◎ 웹쉘 차단하기

웹쉘이 공격자에 의해 업로드되는 경로는 다양하다. 웹쉘은 주로 웹 프로그램의 버그나 취약점을 통해 서버에 업로드되는 경우가 많다. 그 중 가장 많이 공격의 경로로 사용되는 것은 웹 사이트의 자료실 기능(파일 업로드가 가능한 페이지)이다.

만약 웹 사이트의 파일 업로드 기능을 이용하여 확장자가 *.php, *.html 인 파일을 업로드 할 수 있을 경우 공격자는 웹쉘을 업로드하여 웹 서버의 권한을 획득할 수 있다. 따라서, 웹 개발자는 파일 업로드 기능을 구현할 때, 웹 스크립트 언어를 실행할 수 있는 파일의 업로드는 필터링 하도록 한다.

파일 업로드 확장자 필터링 시에는 다음과 같이 정규 표현식을 이용하여 필터링하면 효과적이다.

```
//업로드 파일명 필터링
if (preg_match("/^.*\.(php|asp|htaccess|jsp|html|htm)$/i", $_FILES['file']['name'])) exit;
```

[예제 1] 정규 표현식을 이용한 파일 확장자 필터링 코드 예제

또한 passthru(), system() 함수 등을 사용하는 부분은 공격자가 \$_GET, \$_POST 변수의 조작을 통하여 시스템 명령어를 실행할 수 있는지의 여부를 살펴보도록 한다. ftp 관련 함수가 사용된 부분도 공격자가 이를 이용하여 공격자가 웹쉘을 원격의 FTP 서버에서 받아올 수 있으므로 주의깊게 살펴보도록 한다.

그리고 첨부 파일이 존재하는 디렉토리에 있는 파일들은 웹 스크립트 엔진이 해석하지 못하도록 제한한다면 좀 더 강력한 보안을 기대할 수 있을 것이다. 아파치 웹 서버의 경우 httpd.conf 파일을 열어 다음과 같은 Directory 지시자를 이용하여 파일 첨부 디렉토리의 웹 스크립트 언어 실행 권한을 제한할 수 있다.

```
<Directory "/home/homepage/www/bbs/data">
    RemoveType .html .php .htm
</Directory>
```

[예제 2] 아파치에서 특정 디렉토리의 PHP 실행 권한을 제한하는 코드 예제

◎ 웹쉘 탐지하기

웹쉘은 리눅스의 find 명령 등을 이용하여 시스템 명령을 실행하는 코드가 있는지의 여부를 검사하여 웹쉘을 탐지할 수 있다. 하지만, 최근에 등장하는 웹쉘들은 소스 코드를 암호화하여 제대로 탐지를 하지

못하도록 하기도 한다.

윈도우즈 서버의 경우에는 최신 버전의 카스퍼스키 백신이나 V3 백신 등을 이용하여 웹쉘을 탐지할 수 있다. 하지만, 리눅스의 경우에는 암호화된 웹쉘을 검사하기가 까다로울 수 있는데, 이럴 경우에는 한국정보보호진흥원에서 제공하는 휘슬(Whisl: Web Hacking Inspection Security Tool)⁷⁾을 이용하면 쉽게 탐지할 수 있다.

휘슬은 인터넷침해사고대응센터(<http://www.krcert.or.kr>) 웹 사이트에서 휘슬 사용 신청서를 다운로드 받아 작성하여 제출하면 제공받을 수 있다.

다음은 휘슬을 이용하여 웹쉘을 검사한 화면이다.

```
Checking the configuration
  [Config] Checking directory : /home
  [Config] Inspection Center directory : /root
Response Fail(H=[HTTP/1.0 400 text/html
] B=[<html><head><title>Error</title></head><body>
<h2>ERROR: 400</h2>
Incorrect hostname<br>
</body></html>
])

Checking /hone directory
  [1 Found] /hone/zb4p12/public_html/kcueb/screen.php
  [2 Found] /hone/zb4p12/public_html/review.php
  [20 Found] /hone/zb4p12/public_html/r57shell.php
Check Result
  [INFO] 1291 Files checked
  [INFO] 3 Suspected WebShell
  [INFO] Time cost : 00:02:55
  [INFO] Finish sending the checking result
[Press <ENTER> to continue]
```

[그림 14] 휘슬을 이용하여 웹쉘을 탐지하는 장면

7) 한국정보보호진흥원(KISA)에서 제공하는 웹쉘 전문 탐지 프로그램이다.