

Apache 설정 문제점 (mod_mime Module)

Silverbug(Cho JooBong) <silverbug@apache-kr.org>
HSD(HackerS' Dream) Team
Apache/KR Security Team
<http://Ahnlab.com>(AhnLab, Inc)

1 일반적인 Apache 설치 시 문제점

가) 어떠한 문제가 생기는가?

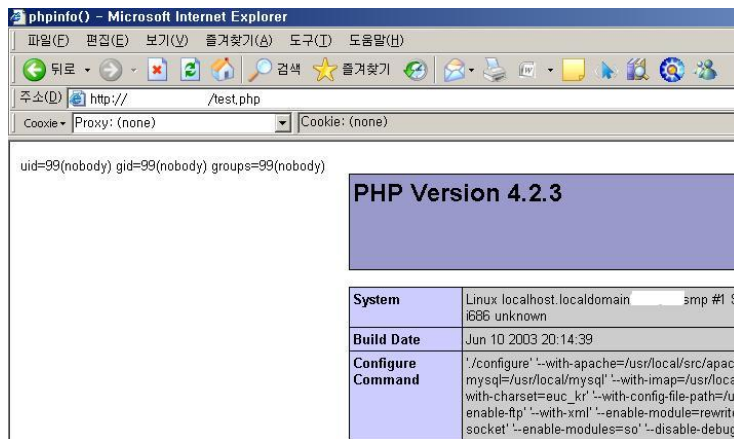
일반적으로 Apache를 설정할 때, 중요한 한가지를 빠뜨리는 경향이 있다. (아마 대부분 그럴 것이다.) 이 중요한 한가지를 제외하고 설정을 했을 때, 어떠한 문제가 일어나는지 살펴보자.

본론으로 넘어와서, 간단하게 테스트 해 보도록 하자. 자신의 서버나 게시판이 존재한다면, php 파일을 작성해 보도록 하자.

```
<?
    system("id");
    phpinfo();
?>
```

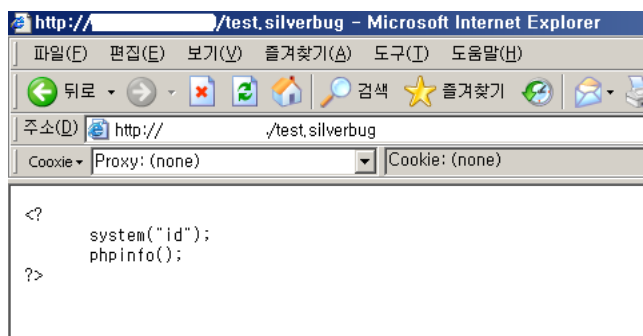
1. 위의 작성한 파일을 “test.php”로 저장해 보도록 하자.

결과는 다음과 같다. (정상적으로 “PHP“ 실행 됨.)



2. 다시 한번 위의 작성한 내용을 “test.silverbug” 파일이름으로 저장하고 실행해보자.

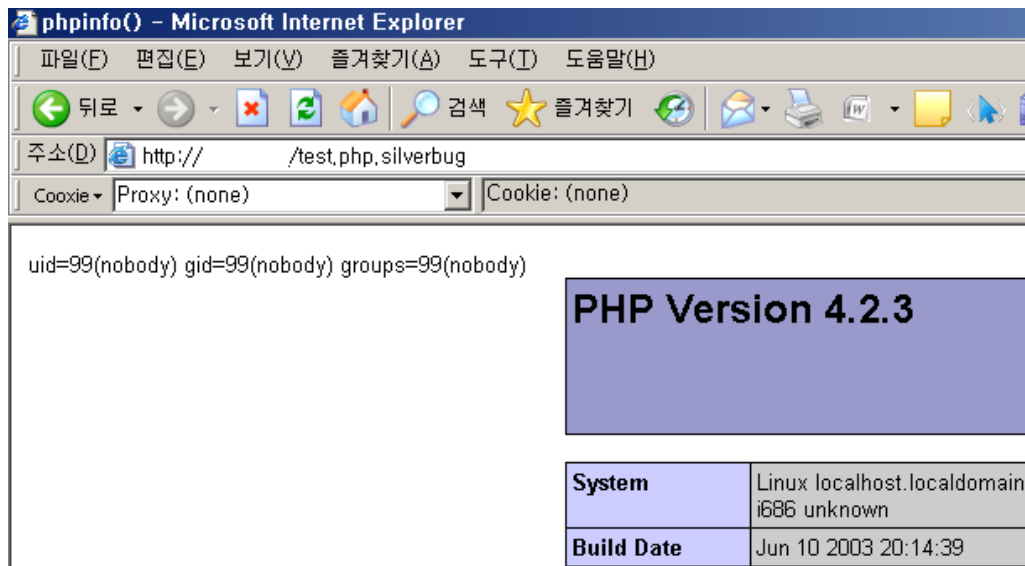
결과는 다음과 같다. (“PHP” 실행 불가)



3. 마지막으로 다시 한번 위에서 작성한 내용을 “test.php.silverbug” 파일이름으로 저장하고 실행해보자.

어떻게 예상하는가? 당신이 상상한 그 이상의 결과를 내뿜을 것이다.

결과는 다음과 같다.



황당하고 어이 없어 하는 사람들도 있을 것이다. 너무 황당하지 않는가? 처음 버그를 실수로 발견했는데, 필자는 “왜 이제까지 아무런 이슈가 없었을까?” 라는 생각을 했다.

또한 왜? 필자는 취약점이라고 하지 않고, 설정상의 문제라고 했을까? 필자 또한 취약점으로 무지 심각하게 오해하고, 거의 1년간 Apache Security Team에 신고를 하려고 했으나, 바쁜 일정과 아직 태어나지는 않았지만, 잘 자라고 있는 우리 아들을 돌보느라 최근에 Apache Security Team에 상황을 보고 했다.

2~3번 정도의 메일을 통한 대화 끝에, 취약점이 아니라 일부러 그렇게 만들어 놨다는 것이다. 왜? 효율성 때문에..... (사실 Apache Security Team에 보고하기 전에 소스를 확인하면서 취약점이 아닐 꺼 같다는 생각을 강하게 받았었다. 혹시나 했는데.. 역시나.....)

나) 왜 그러한 문제가 생기는 것일까?

왜 이러한 문제가 생기는지 간단하게 설명하면, Apache 웹 서버의 Mime 모듈은 다양하게, MIME을 받으려고 하는 부분에서 문제가 생긴다. 그럼 소스를 보고 간단하게 코드를 보면서 살펴보도록 하자.

```
Source File : mod_mime.c
Function Name : find_ct(request_rec *r)

fn = strrchr(r->filename, '/');
...
ext = ap_getword(r->pool, &fn, '.');
/* Parse filename extensions, which can be in any order */
while ((ext = ap_getword(r->pool, &fn, '.')) && *ext) {
int found = 0;
    if ((type = ap_table_get(conf->forced_types, ext))
        || (type = ap_table_get(hash_buckets[hash(*ext)], ext))) {
        r->content_type = type;
        found = 1;
    }
...
}
```

일단 간단하게 MIME Type만 체크하는 부분의 코드를 보도록 하자. 위 코드를 살펴보면 입력된 파일명을 받아서 “.”으로 끊으면서 반복하게 된다. 즉, “a.b.c” 파일이 존재할 경우 b와 c 둘 다 확장자로 인식한다는 뜻이다.
(유독 MIME 모듈에서만 이러한 형태를 취하고 있다. 다른 모듈 소스는 “strchr”을 통해 실제 마지막 확장자만을 확장자로 인식한다.)

여기서 ap_table_get 함수를 이용하여 확장자에 맞는 Content-Language, Content-Type, Special Handler, Content-Type을 결정하여, “r” 구조체 변수에 담게 된다.

만약 a.php.jpg 파일이 입력되면, 처음에 php 확장자의 각 Content 정보를 ‘r’ 구조체 변수에 담고, 다시 jpg 확장자의 각 Content 정보를 “r” 구조체에 담는다. 즉 마지막에는 jpg 확장자의 Content 정보만 “r” 구조체 변수에 들어간다는 것이다. 하지만 여기서 중요한 점이 있다. 코드를 살펴보면 ap_table_get 함수를 통해 입력된 확장자가 등록되지 않은 확장자라면??? “r” 구조체 변수는 기존 정보를 그대로 유지한다는 것이다.(사실 왜 이렇게 했는지 이해가 안될 뿐이다.)

즉 “test.php.silverbug”라면 “silverbug”라는 확장자는 아파치 설정에 포함되어 있지 않기 때문에, 기존에 입력된 “php” 확장자의 Content 정보를 가져간다는 것이다.

위의 문제점(?)이 어디에 적용될 것인가? 대부분의 Web Application은 실행 가능한 확장자를 업로드 하지 못하도록 필터 링하고 있다. 하지만 이러한 필터 링 방식을 살펴보면, 쉘 마지막 실제 확장자만을 체크하여 비교 체크를 한다. 이러한 경우 웹 서버 설정을 잘못해봤을 경우 php나 cgi 파일을 업로드 하여, 웹 서버의 사용자 권한을 획득할 수 있다.

2 문제점 해결 방법

가) Application 에서의 보안

- ① 파일 업로드 기능을 가지고 있는 웹 어플리케이션에서 확장자 체크를 끝부분만 하지 않고 임시적으로 전체 파일명에 대해 필터 링 기능을 가지고 있어야 한다
- ② 등록 불가능한 확장자를 체크하는 방식보다는 등록 가능한 확장자만을 체크하여 필터링 하여야 한다.
- ③ 파일을 업로드 할 때 실제 파일명은 데이터베이스에 기록하고, 실제로 파일이 저장될 때 파일명/확장자를 임의적으로 저장(File, DB)하도록 한다.

나) httpd.conf 파일 수정

FileMatch를 사용하여 확장자 끝부분(\$)만 비교하도록 설정한다.

다음과 같다.

CGI 파일 확장자

```
<FileMatch W.cgi$>
    SetHandler cgi-script
</FileMatch>
```

PHP 파일 확장자

```
<FileMatch W.php$>
    SetHandler application/x-httpd-php
</FileMatch>
```

또는

```
<FilesMatch "\\.ph(p[2-6]?|tml)$">
    SetHandler application/x-httpd-php
</FilesMatch>
```

그리고 소스는

```
<FilesMatch "\\.phps$">
    SetHandler application/x-httpd-php-source
</FilesMatch>
```

다) Source Code에서의 보안

mod_mime.c 파일의 find_ct 함수의 내용 중 ap_table_get에서 값을 얻어오지 못할 경우, else 처리를 하여 "r" 구조체 변수를 NULL 처리하도록 한다.

```
# php, etc... Patch
if ((type = ap_table_get(conf->forced_types, ext))
    || (type = ap_table_get(hash_buckets[hash(*ext)], ext))) {
    r->content_type = type;
    found = 1;
    fprintf(fp, "File Type Name :: %s\n", type);
} else {
    found = 0;
    r->content_type = NULL;
}

.....
# cgi, etc... Patch
/* Check for a special handler, but not for proxy request */
if ((type = ap_table_get(conf->handlers, ext)
    && r->proxyreq == NOT_PROXY) {
    r->handler = type;
    found = 1;
} else {
    found = 0;
    r->handler = NULL;
}
```

[참고 사이트]

<http://www.php.net/manual/en/install.unix.apache2.php>

http://httpd.apache.org/docs/2.2/en/mod/mod_mime.html#multipleext