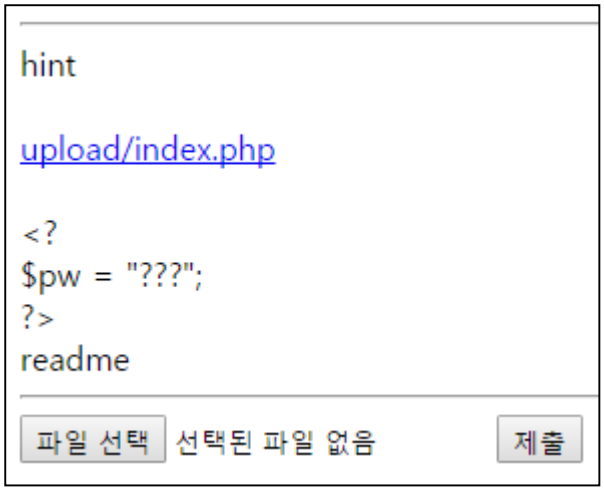
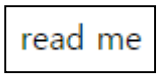
webhacking.kr 28번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-10
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

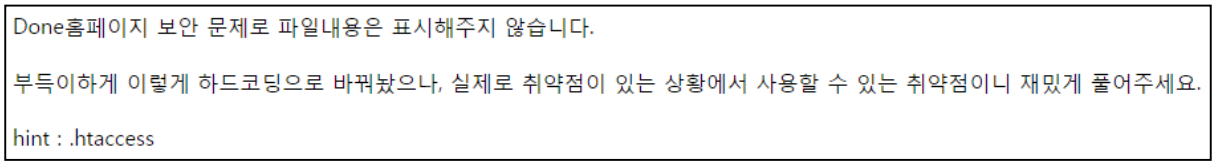
다음과 같이 hint가 주어지고 파일 제출이 가능하다.



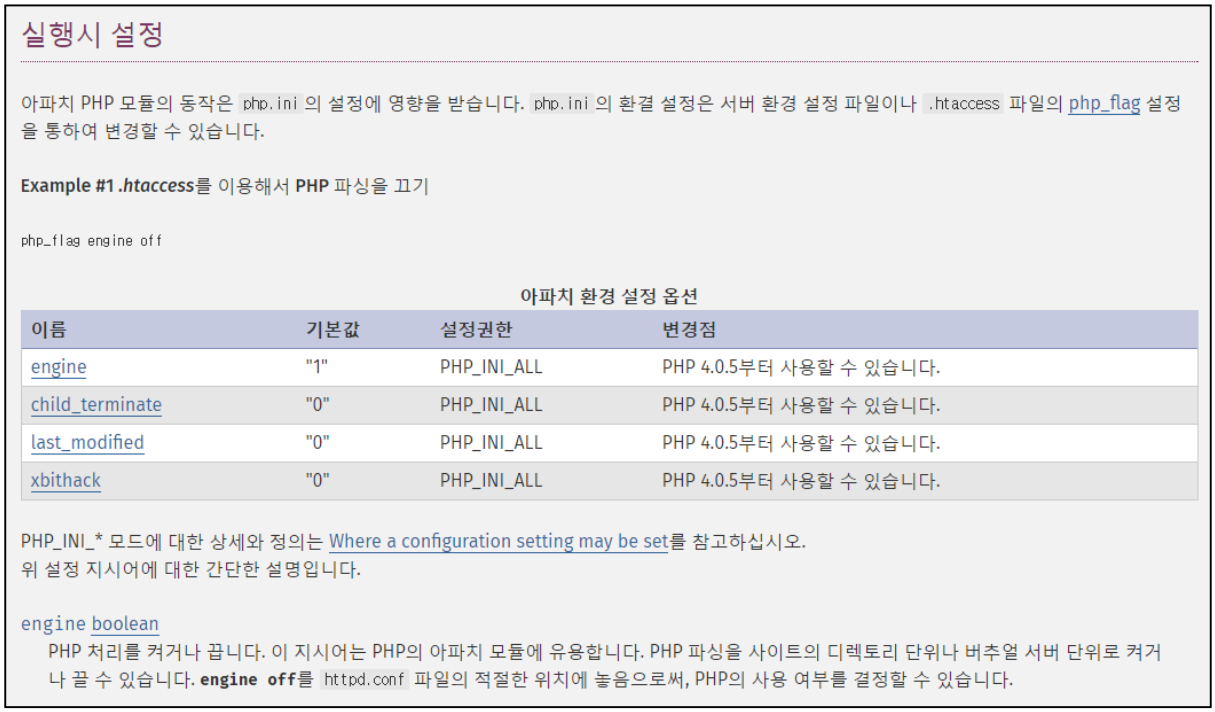
upload/index.php로 들어가니 다음과 같이 read me만 나온다.



아무 파일이나 제출해보니 다음과 같이 뜬다.



검색을 통해 php_flag engine off라는 것을 알게 되었다.



실행시 설정

아파치 PHP 모듈의 동작은 `php.ini` 의 설정에 영향을 받습니다. `php.ini` 의 환경 설정은 서버 환경 설정 파일이나 `.htaccess` 파일의 php_flag 설정을 통하여 변경할 수 있습니다.

Example #1 *.htaccess*를 이용해서 PHP 파싱을 끄기

```
php_flag engine off
```

아파치 환경 설정 옵션

이름	기본값	설정권한	변경점
engine	"1"	PHP_INI_ALL	PHP 4.0.5부터 사용할 수 있습니다.
child_terminate	"0"	PHP_INI_ALL	PHP 4.0.5부터 사용할 수 있습니다.
last_modified	"0"	PHP_INI_ALL	PHP 4.0.5부터 사용할 수 있습니다.
xbithack	"0"	PHP_INI_ALL	PHP 4.0.5부터 사용할 수 있습니다.

PHP_INI_* 모드에 대한 상세와 정의는 Where a configuration setting may be set를 참고하십시오.
위 설정 지시어에 대한 간단한 설명입니다.

engine boolean
PHP 처리를 켜거나 끕니다. 이 지시어는 PHP의 아파치 모듈에 유용합니다. PHP 파싱을 사이트의 디렉토리 단위나 버추얼 서버 단위로 켜거나 끌 수 있습니다. **engine off**를 `httpd.conf` 파일의 적절한 위치에 놓음으로써, PHP의 사용 여부를 결정할 수 있습니다.

.htaccess에 php_flag engine off라는 값을 넣어서 올리면 PHP 처리가 꺼져서 소스를 읽을 수 있을 것이다.
메모장으로 php_flag engine off를 쓰고 확장자를 없게 한 후 .htaccess라는 이름으로 만들어서 업로드하니 다음과 같이 클리어되었다.
원래는 업로드 한 후 페이지를 들어가서 클리어해야겠지만 보안상의 문제로 하드코딩 해둔 듯 하다.