

다음과 같은 폼이 있다.

메일 :

쿼리 전송

우선 메일을 넣고 쿼리를 전송해보자.

메일 : blackzer0@blackwar.kr

쿼리 전송

Done이라는 경고창이 뜬다.



소스보기를 통해 소스를 보자.



다음이 소스이다.

```
<html>
<head>
<title>Challenge 47</title>
</head>
<body>

<pre>
<form method=post action=index.php>
<font size=2>메일</font> : <input type=text name=email size=50 style=border:0
maxlength=50><input type=submit>


</form>

</pre>

<!-- index.phps -->

</body>
</html>
```

주석으로 index.phps를 가리켰으니 들어가서 실제 소스를 보자.

 <http://webhacking.kr/challenge/bonus/bonus-11/index.phps>

이것이 실제 소스이다.

mail()함수를 이용해 메일을 보내는 것이다.

mail header injection 이다.

```
<html>
<head>
<title>Challenge 47</title>
</head>
<body>

<pre>
<form method=post action=index.php>
<font size=2>메일</font> : <input type=text name=email size=50 style=border:0
maxlength=50><input type=submit>

</form>

<?
```

```

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>");
}
?>

</pre>

<!-- index.phps -->

</body>
</html>

```

mail header injection을 위해 우선 파로스로 잡아보았다.

8	GET	http://webhacking.kr/
46	POST	http://webhacking.kr/challenge/bonus/bonus-11/index.php
51	POST	http://ts.naver.com/t
53	GET	http://webhacking.kr/challenge/bonus/bonus-11/index.php

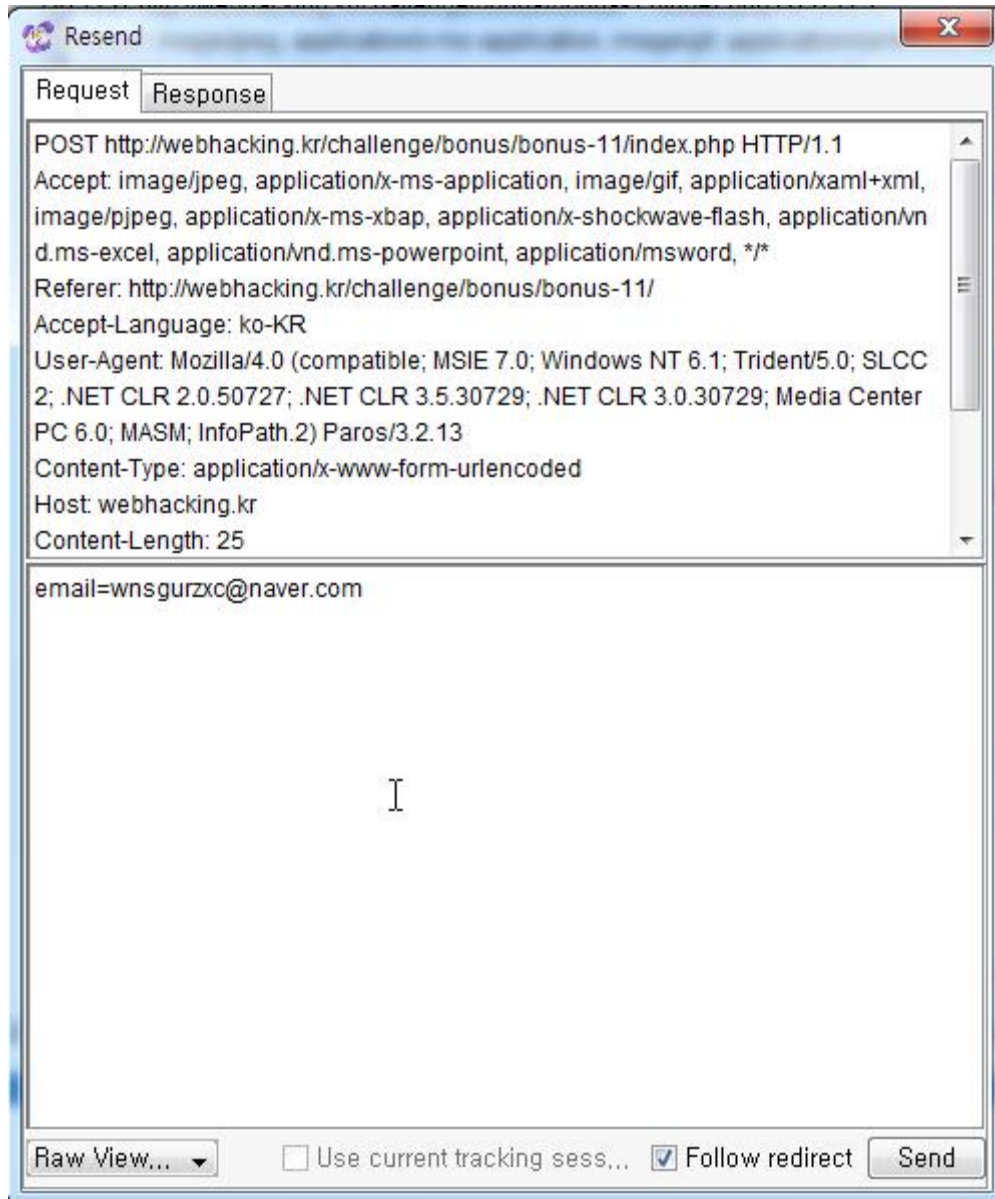
Resend로 Request를 수정하자.

8	GET	http://webhacking.kr/
46	POST	http://webhacking.kr/challenge/bonus/bonus-11/index.php
51	POST	http://ts.naver.com/t
53	GET	http://webhacking.kr/challenge/bonus/bonus-11/index.php

Resend...

Tag...

email=wmsgurzxc@naver.com 으로 되어있다.



cc: (참조)를 이용해서 admin@webhacking.kr 으로 가는 메일을 자기 메일로 보내보자.
<http://impactlife.springnote.com/pages/5164661> (mail header 관련 글이므로 참조하자)



다음과 같이 메일이 성공적으로 도착했다.



readme라는 제목의 메일이 도착하였다.



비밀번호를 얻었고, 인증에 성공했다.

★ readme

보낸 사람 : <wnsgurzxc@naver.com>주소록에 추가 | 수신차단하기
받는 사람 : <admin@webhacking.kr>
참조 : <wnsgurzxc@naver.com>

password is 5277d703a0d977760272ca5b4f74d8f3