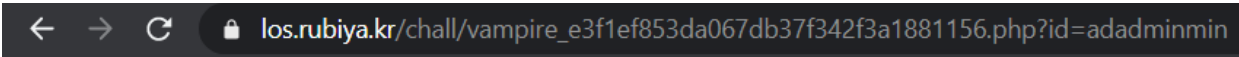

query : select id from prob_vampire where id=""

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/\.'/i', $_GET[id])) exit("No Hack ~_~");
$_GET[id] = strtolower($_GET[id]);
$_GET[id] = str_replace("admin", "", $_GET[id]);
$query = "select id from prob_vampire where id='{$_GET[id]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id'] == 'admin') solve("vampire");
highlight_file(__FILE__);
?>
```

Challenge lần này cần nhập vào admin nhưng nếu nhập trực tiếp sẽ bị filter. Filter cũng chuyển tất cả kí tự thành thường để tránh bypass bằng kí tự hoa.



query : select id from prob_vampire where id='admin'

VAMPIRE Clear!

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/\.'/i', $_GET[id])) exit("No Hack ~_~");
$_GET[id] = strtolower($_GET[id]);
$_GET[id] = str_replace("admin", "", $_GET[id]);
$query = "select id from prob_vampire where id='{$_GET[id]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id'] == 'admin') solve("vampire");
highlight_file(__FILE__);
?>
```

Kiểm tra ta thấy filter sẽ thay 'admin' thành ''. Lỗ hổng ở đây là nếu filter chỉ áp dụng 1 lần ta có thể tạo input sao cho khi đi qua filter sẽ tạo thành 'admin'.

Input ở đây sẽ là **adadminmin**. Filter sẽ xóa chữ 'admin' ở giữa và còn lại chữ 'admin'.