链滴

某道 PHP 代码审计

作者：wizardforcel
原文链接：https://ld246.com/article/1476880169990
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

```php
<?php
if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
    {
        echo '<p>You password must be alphanumeric</p>';
    }
    else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
    {
        if (strpos ($_GET['password'], '*-*') !== FALSE)
        {
            die('Flag: ' . $flag);
        }
        else
        {
            echo('<p>*-* have not been found</p>');
        }
    }
    else
    {
        echo '<p>Invalid password</p>';
    }
}
?>
```

首先，ereg用00截断来绕过，之后输入长度小于 8，又得有*-*符号，那么留给我们的空间就只有三。这时候要想大于 9999999，只能用科学计数法，9e9，所以地址栏输入password=9e9%00*-*就拿到 Flag。

但是我说的重点不是这个，可以尝试在地址栏里面输入password[]=0，照样能过。不知道出题人是忽还是有意为之。。。

原文链接：某道 PHP 代码审计