

源码如下

```
1 <?php
2 show_source("21.php");
3 echo '<br>';
4 error_reporting(0);
5 require 'flag.php';
6 if ("POST" == $_SERVER['REQUEST_METHOD'])
7 {
8     $password = $_POST['password'];
9     if (0 >= preg_match('/^[[[:graph:]]{12,}$/', $password)) //preg_matc
h - 执行一个正则表达式匹配
10     {
11         echo 'Wrong Format';
12         exit;
13     }
14     while (TRUE)
15     {
16         $reg = '/([[:punct:]]+|[[:digit:]]+|[[:upper:]]+|[[:lower:]]+)/';
17         if (6 > preg_match_all($reg, $password, $arr))
18             break;
19         $c = 0;
20         $ps = array('punct', 'digit', 'upper', 'lower');
21         foreach ($ps as $pt)
22         {
23             if (preg_match("/[[:$pt:]]+/", $password))
24                 $c += 1;
25         }
26         if ($c < 3) break;
27         if ("42" == $password) echo $flag;
28         else echo 'Wrong password';
29         exit;
30     }
31 }
32 ?>
```

主要考察对正则表达式的理解

```
1 preg_match('/^[[[:graph:]]{12,}$/', $password)
```

意为匹配12个非空字符

```
1 $reg = '/([[:punct:]]+|[[:digit:]]+|[[:upper:]]+|[[:lower:]]+)/';
```

[:punct:] 任何标点符号 [:digit:] 任何数字 [:upper:] 任何大写字母 [:lower:] 任何小写字母

后面的正则也是同理

所以全文的要求就是一个等于42的数字字母和字符都有的数

所以payload不唯一

```
1 password=42.000000000000000000e+0
```