目录

一、题目

1、源码

```php
$sanitized = [];

foreach ($_GET as $key => $value) {
    $sanitized[$key] = intval($value);
}

$queryParts = array_map(function ($key, $value) {
    return $key . '=' . $value;
}, array_keys($sanitized), array_values($sanitized));

$query = implode('&', $queryParts);

echo "<a href='/images/size.php?" .
    htmlentities($query) . "'>link</a>";
```

2、知识点

知识点	说明
array_map()	将用户自定义函数作用到数组中的每个值上，并返回用户自定义函数作用后的带有新的值的数组
array_keys()	返回包含数组中所有键名的一个新数组
array_values()	返回包含数组中所有值的一个新数组

3、解读

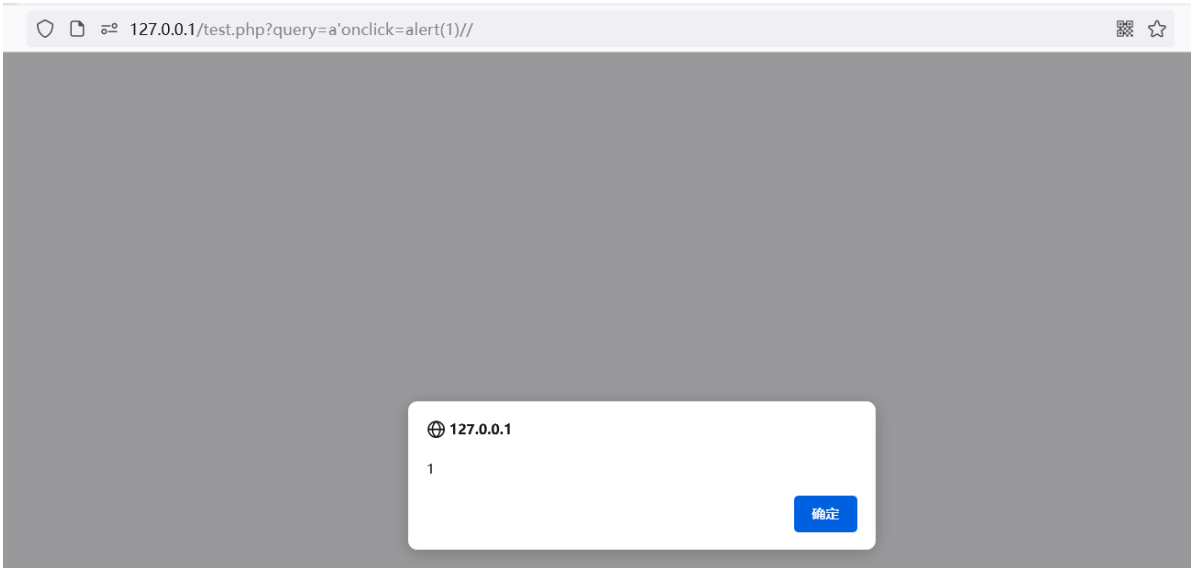
1）第1行，定义数组变量$sanitized。
2）第3行，foreach循环遍历GET方法传入的数据，将参数和值分别赋值给$key和$value，然后将$value转换成整数型作为$sanitized数组中$key的值。
3）第7行，使用函数array_map()处理$sanitized数组，用=分割键值，赋值给$queryParts。
4）第11行，使用&对$queryParts中的键值进行分割，赋值给$query。
5）第13行，使用函数htmlentities()对$query进行过滤，并拼接到HTML代码中输出。

4、分析

1）$query参数可控。
2）函数htmlentities()中可以逃逸单引号。
3）最后拼接在<a>标签。

5、利用

```
?query=a'onclick=alert(1)//
```



二、CMS

1、源码-DM企业建站系统 v201710

```
admindm-youramemod_common/login.php
```

```php
if($act=='login'){

$user= @htmlentitiesdm(trim($_POST['user']));
$ps= @htmlentitiesdm(trim($_POST['password']));


if(strlen($user)<2 or strlen($ps)<2){
    alert('字符不够 sorry,user need more long');    jump($jumpv);
}

require_once WEB_ROOT.'component/dm-config/mysql.php';
     // $salt = '00';is in config.php
  $pscrypt= crypt($ps, $salt);
     //echo $pscrypt;
 $ss_P="select * from ".TABLE_USER."  where  email='$user' and
 ps='$pscrypt'  order by id desc limit 1";
    // echo $ss_P;exit;
        if(getnum($ss_P)>0){
                    $row=getrow($ss_P);
                    $userid=$row['id'];
```

component/dm-config/global.common.php

```php
function htmlentitiesdm($v){
   return htmlentities(trim($v),ENT_NOQUOTES,"utf-8");
}
```

2、知识点

知识点	说明
crypt()	返回使用DES、Blowfish或MD5算法加密的字符串
ENT_NOQUOTES	对单引号和双引号都不转换

3、解读

1）图1，第15行，将变量$user到SQL查询语句中。第3行，变量$user是通过POST方法传递进来的参数user，并经过函数htmlentitiesdm()进行过滤。

2）图2，跟进到函数htmlentitiesdm()，可以看到这里第二个参数值指定的规则是ENT_NOQUOTES，也就是不对单引号和双引号进行转换。

4、分析

通过POST传递user参数，用单引号闭合前面的SQL语句，拼接需要执行SQL命令。

5、利用

```
    user=admin'and sleep(5)--+
```

6、修复方案

```
    针对函数htmlentities()，使用的使用加上可选参数，并选择ENT_QUOTES。
```

7、参考链接

```
    https://github.com/hongriSec/PHP-Audit-
Labs/blob/master/Part1/Day12/files/README.md
```