PHP特性&缺陷对比函数&CTF考点

原创 大飞先生 于 2022-09-13 11:27:09 发布 阅读量2k 收藏 11 点赞数 2 版权
分类专栏： 基础的渗透测试 文章标签： php 开发语言

#详细点：

==与===

md5

intval

strpos

in_array

preg_match

str_replace

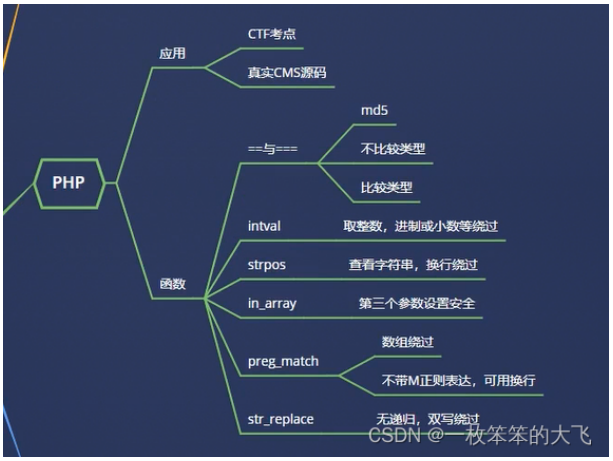
PHP比对规则

== 和 ===

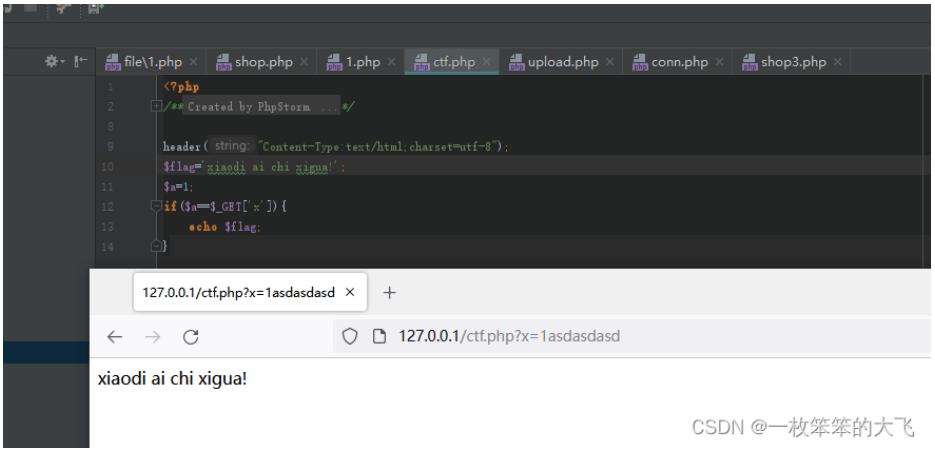
=：赋值

==：对比，但是不会对比数据类型

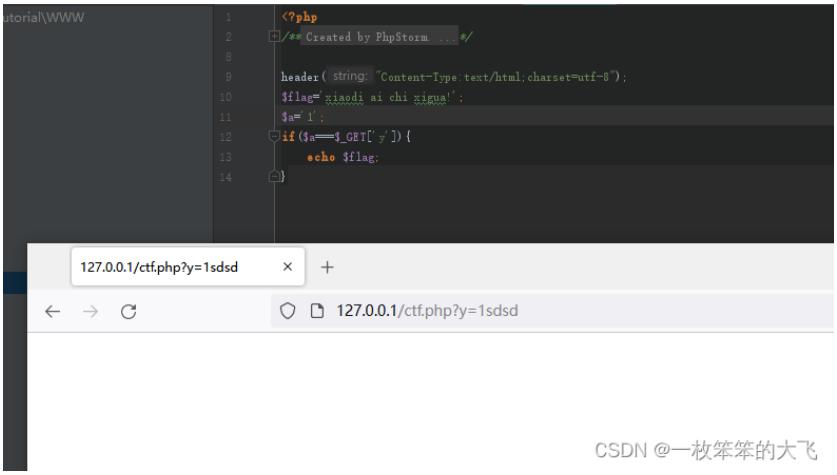
===：对比，同时对比数据类型

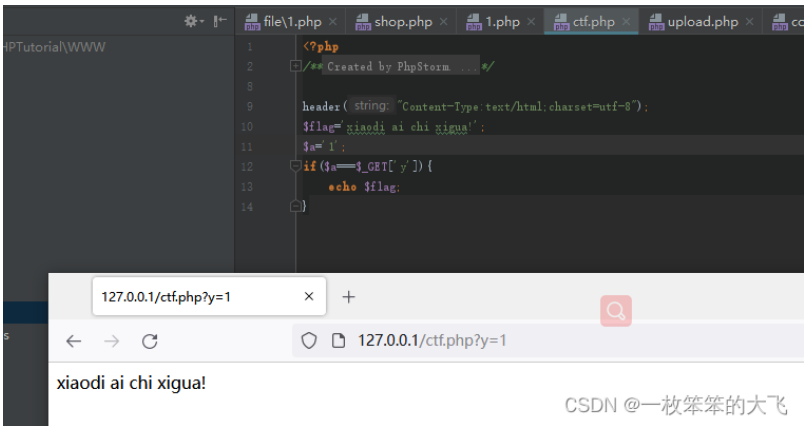


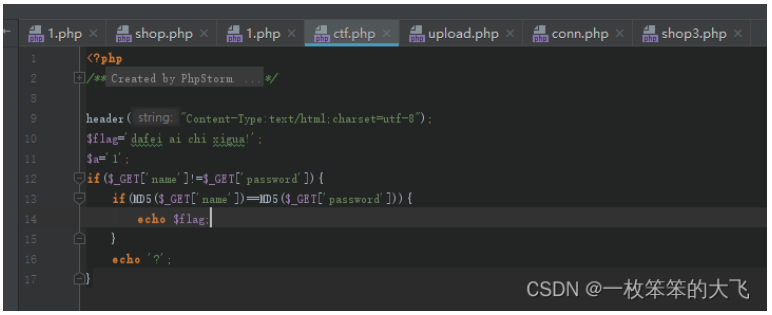
1.== 只要赋值变量是1开头，都可以正常访问



2.===

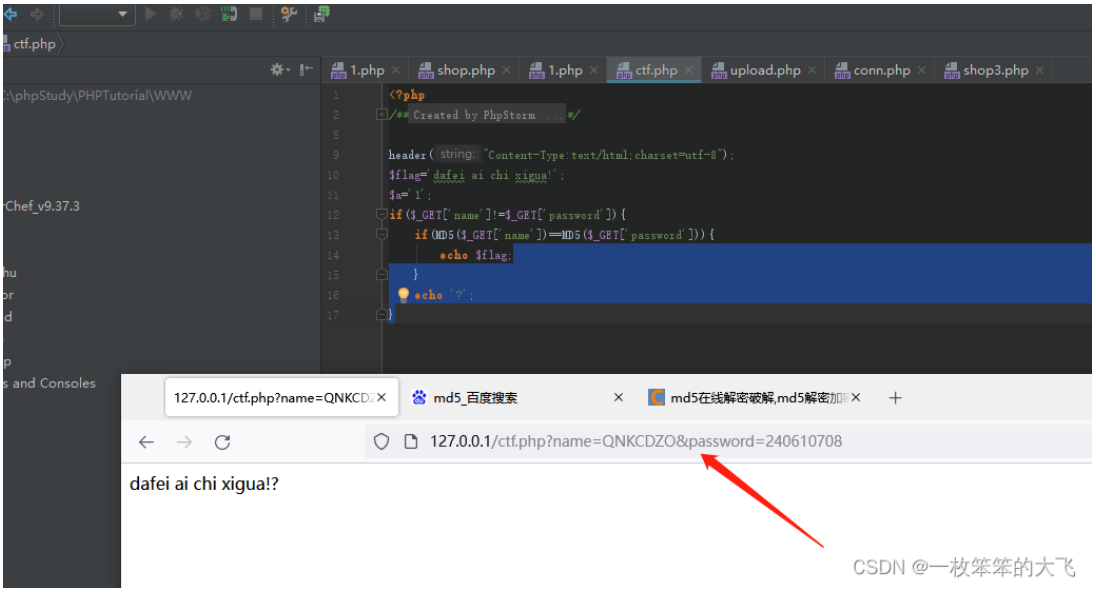




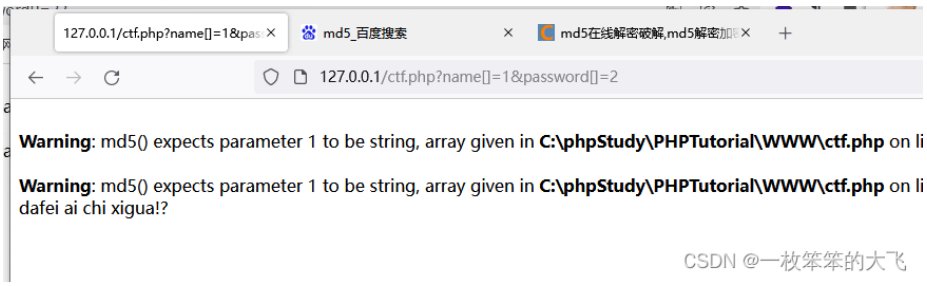


可以看到这两个MD5值都是0开头，而==符号存在的

http://127.0.0.1/ctf .php?name=QNKCDZO&password=240610708



当遇到===的PHP验证代码时



2.intval

intval() 函数用于获取变量的整数值。

intval() 函数通过使用指定的进制 base 转换（默认是十进制），返回变量 var 的 integer 数值。 intval() 不能用于 object，否则会产生 E_NOTICE 错误并返回 1。

语法

int intval (mixed $var [, int $base = 10])

参数说明：

- $var：要转换成 integer 的数量值。
- $base：转化所使用的进制。

如果 base 是 0，通过检测 var 的格式来决定使用的进制：

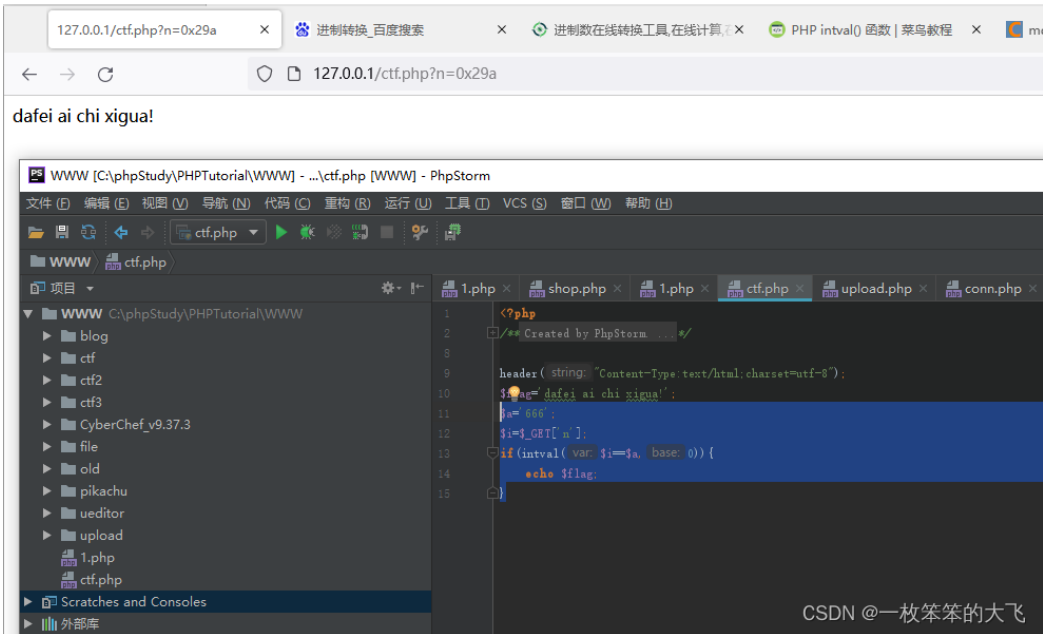
- 如果字符串包括了 "0x" (或 "0X") 的前缀，使用 16 进制 (hex)；否则，
- 如果字符串以 "0" 开始，使用 8 进制(octal)；否则，
- 将使用 10 进制 (decimal)。

1. 绕过方式1.0 +1.0

```
<?php
header("Content-Type:text/html;charset=utf-8");
$flag='dafei ai chi xigua!';
$a='1';
$i=$_GET['n'];
if(intval($i==$a)){
    echo $flag;
}
```

2.绕过方式 666　0x29a（16进制）

```
$a='666';

$i=$_GET['n'];

if(intval($i==$a,0)){

    echo $flag;

}
```



PHP strpos() 函数

查找 "php" 在字符串中第一次出现的位置：

定义和用法

strpos() 函数查找字符串在另一字符串中第一次出现的位置。

注释：strpos() 函数对大小写敏感。

注释：该函数是二进制安全的。

相关函数：

- stripos() - 查找字符串在另一字符串中第一次出现的位置（不区分大小写）
- strripos() - 查找字符串在另一字符串中最后一次出现的位置（不区分大小写）
- strrpos() - 查找字符串在另一字符串中最后一次出现的位置（区分大小写）

语法

```
strpos(string,find,start)
```

string	必需。规定要搜

find	必需。规定要查找的字符串。
start	可选。规定在何处开始搜索。

1. 对于strpos()函数，利用换行绕过（%0a）

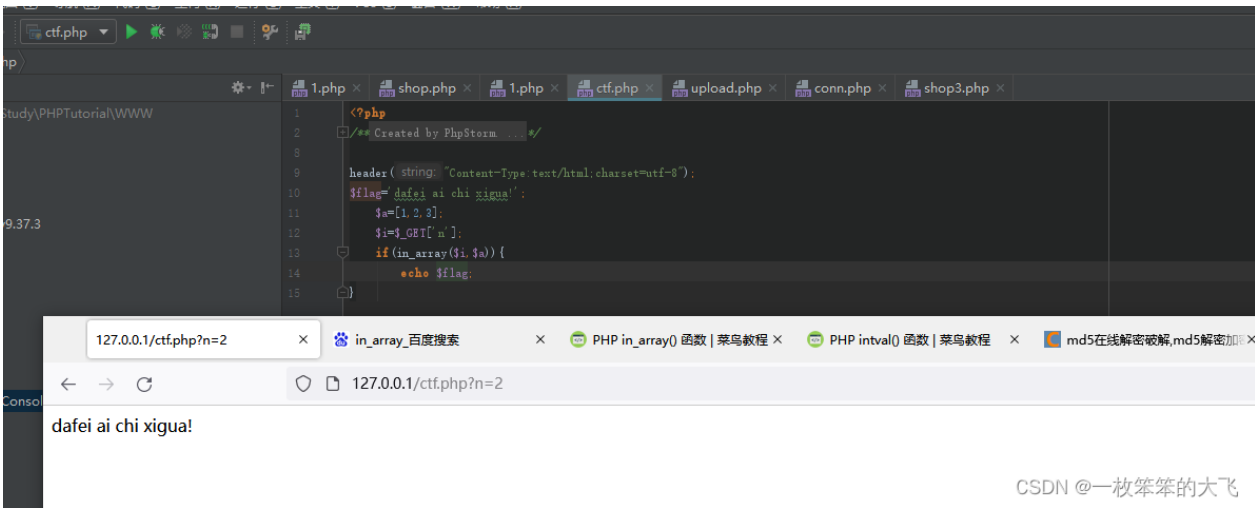
`0a`：换行

PHP in_array() 函数

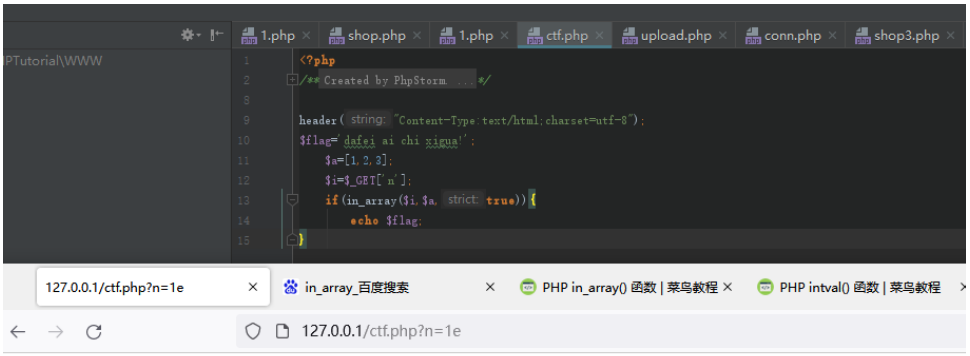
in_array() 函数搜索数组中是否存在指定的值。

```
bool in_array ( mixed $needle , array $haystack [, bool $strict = FALSE ] )
```

needle	必需。规定要在数组搜索的值。
haystack	必需。规定要搜索的数组。
strict	可选。如果该参数设置为 TRUE，则 in_array() 函数检查搜索的数据与数组的值的类型是否相同。



设置true属性时



PHP preg_match() 函数

preg_match 函数用于执行一个正则表达式匹配。

语法

```
int preg_match ( string $pattern , string $subject [, array &$matches [, int $flags = 0 [, int $offset = 0 ]]] )
```

搜索 subject 与 pattern 给定的正则表达式的一个匹配。

参数说明：

- $pattern: 要搜索的模式，字符串形式。
- $subject: 输入字符串。
- $matches: 如果提供了参数matches，它将被填充为搜索结果。 $matches[0]将包含完整模式匹配到的文本， $matches[1] 将包含第一个捕获子组匹配到的文本，以此类推。
- $flags：flags 可以被设置为以下标记值：
    1. PREG_OFFSET_CAPTURE: 如果传递了这个标记，对于每一个出现的匹配返回时会附加字符串偏移量(相对于目标字符串的)。 注意：这会改变填充到matches参数的数组，使其每个元素成为一个由 第0个元素是匹配到的字符串，第1个元素是该匹配字符串 在目标字符串subject中的偏移量。
- offset: 通常，搜索从目标字符串的开始位置开始。可选参数 offset 用于 指定从目标字符串的某个未知开始搜索(单位是字节)。
- isset（）函数用于检测变量是否已设置并且非NULL。如果已经使用unset（）释放了一个变量之后，再通过isset（）判断将返回FALSE。
- 如果使用isset（）测试一个被设置成NULL的变量，将返回FALSE。同时要注意的是null字符（“\0”）并不相等于PHP的NULL常量。

```
//模式分隔符后的"i"标记这是一个大小写不敏感的搜索
preg_match('/^php$/im')
```

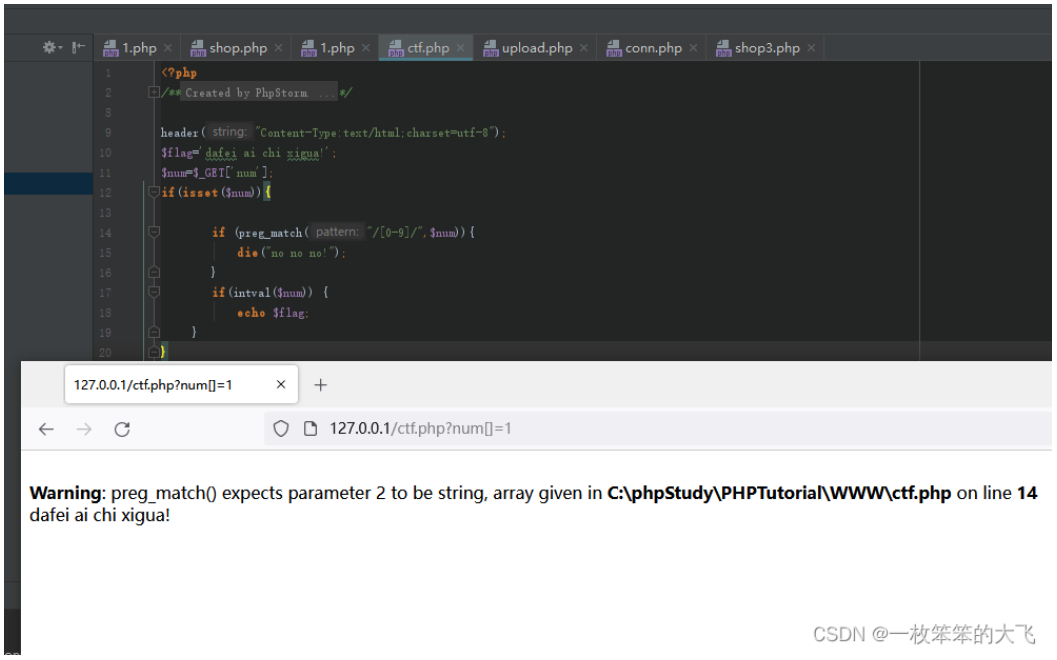
^:前边随意

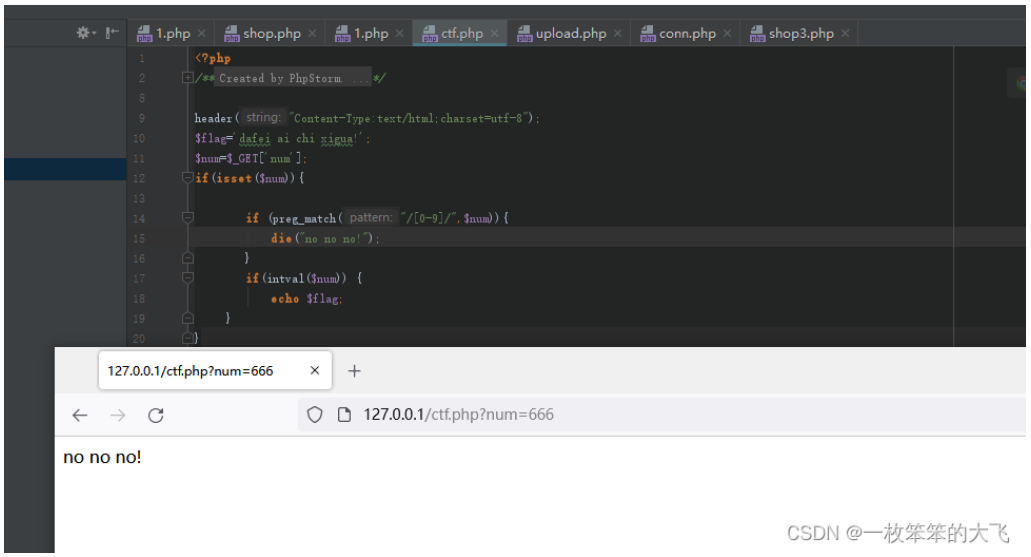
$：结尾随意

/i：不区分大小写

/m：换行匹配

绕过函数方法：利用数组，pre_match处理不了数组数据





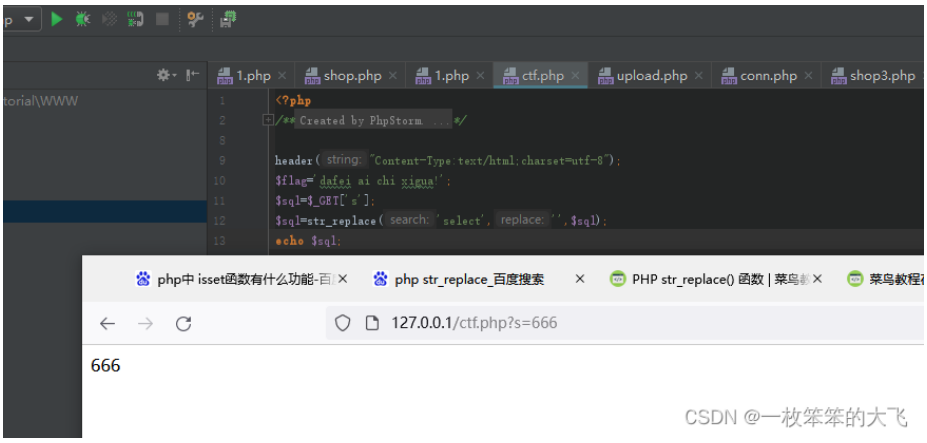
PHP str_replace() 函数

实例

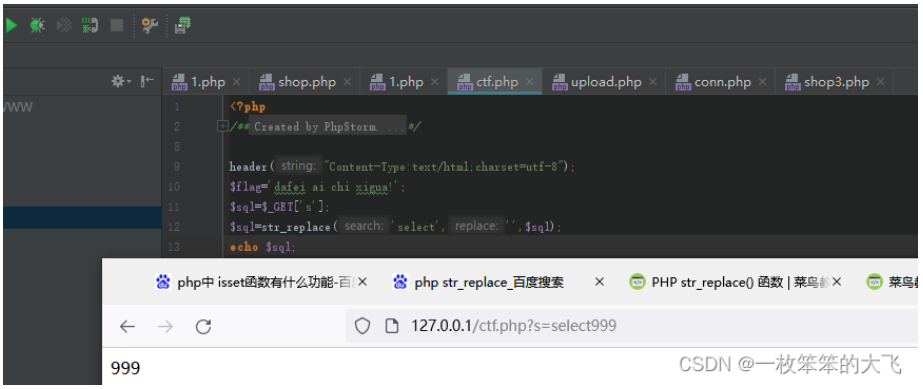
把字符串 "Hello world!" 中的字符 "world" 替换成 "Peter":

```
<?php
echostr_replace("world","Peter","Helloworld!");
?>
```

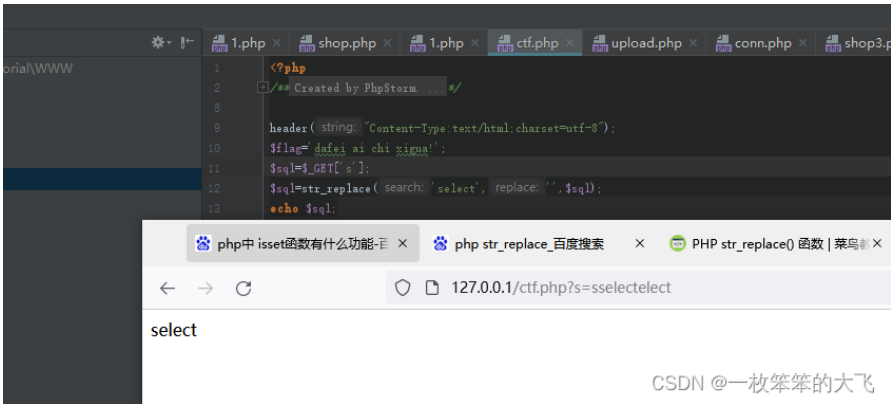
正常情况



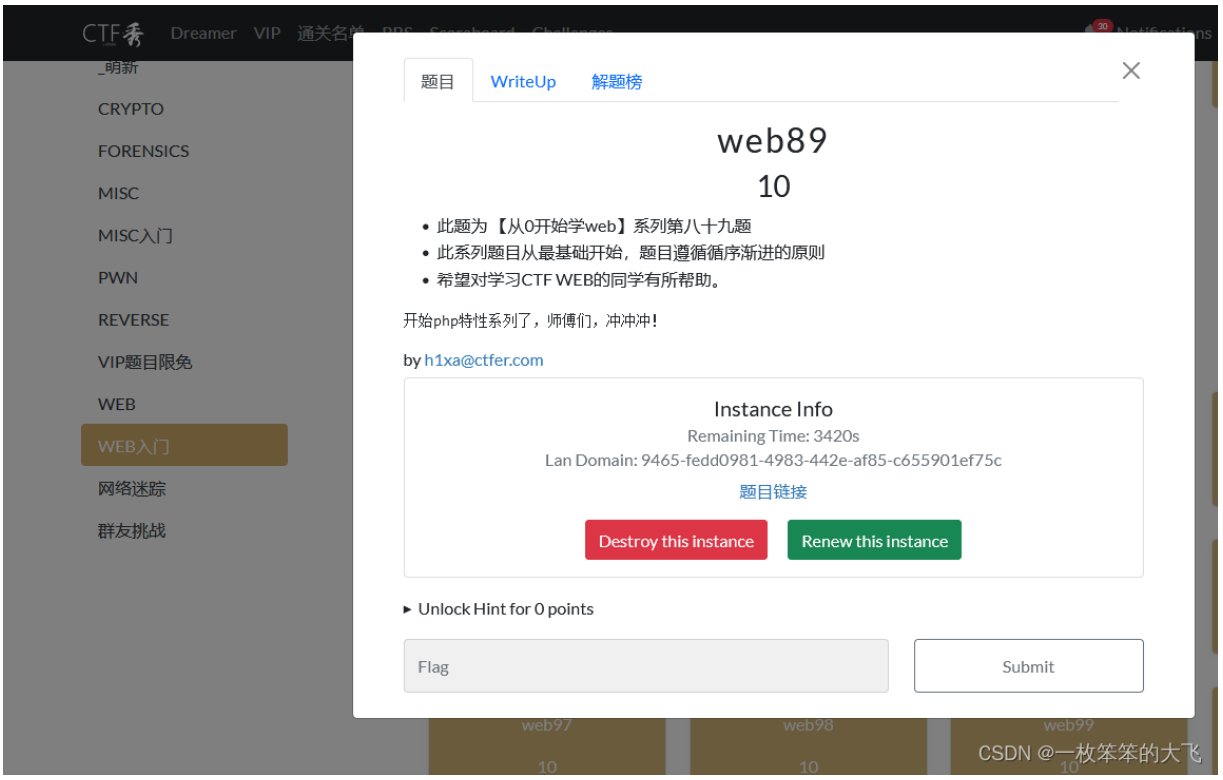
过滤掉select时

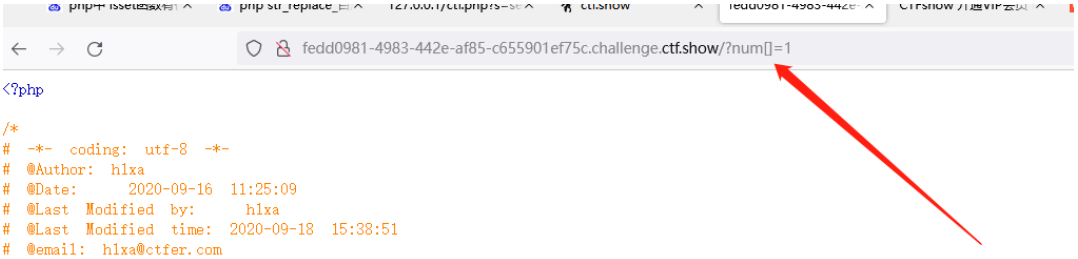


过滤方法，只能过滤一次select



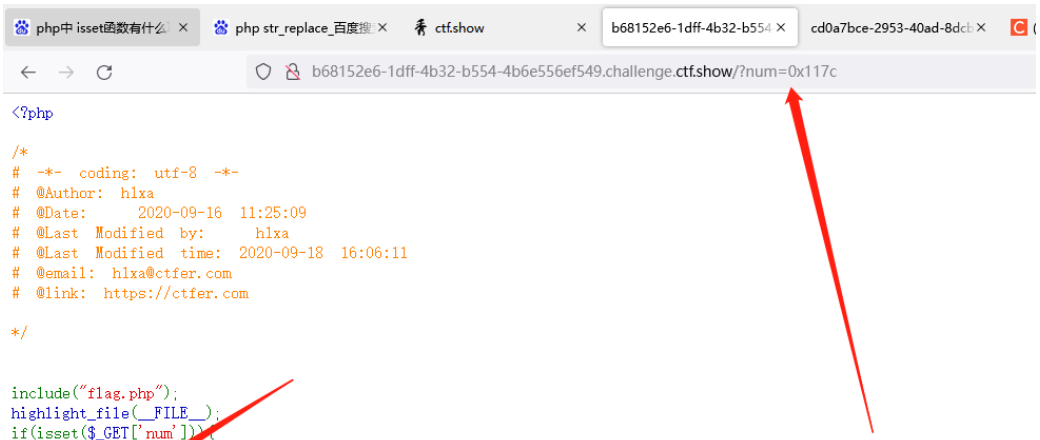
CTFshow实战演练






```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date: 2020-09-16 11:25:09
# @Last Modified by: h1xa
# @Last Modified time: 2020-09-18 15:38:51
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/


include("flag.php");
highlight_file(__FILE__);

if(isset($_GET['num'])){
        $num = $_GET['num'];
        if(preg_match("/[0-9]/", $num)){
                die("no no no!");
        }
        if(intval($num)){
                echo $flag;
        }
}
```

Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/index.php** on line **20**
ctfshow{1981b8a7-86bd-4084-9342-3cfae040e73d}




```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date: 2020-09-16 11:25:09
# @Last Modified by: h1xa
# @Last Modified time: 2020-09-18 16:06:11
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/


include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
        $num = $_GET['num'];
        if($num==="4476"){
                die("no no no!");
        }
        if(intval($num,0)===4476){
                echo $flag;
        }else{
                echo intval($num,0);
        }
}
```

ctfshow{5ea9f4fc-3f35-4f06-bc83-96bab0a293eb}

82bc263c-cd14-409e-855a-f8845f7ed7bd.challenge.ctf.show/?num=010574

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: Firebasky
# @Date: 2020-09-16 11:25:09
# @Last Modified by: hlxa
# @Last Modified time: 2020-09-18 16:32:58
# @link: https://ctfer.com

*/

include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
        $num = $_GET['num'];
        if($num==4476){
                die("no no no!");
        }
        if(preg_match("/[a-z]/i", $num)){
                die("no no no!");
        }
        if(intval($num,0)==4476){
                echo $flag;
        }else{
                echo intval($num,0);
        }
}
```

ctfshow{7ee6faaa-f5c2-4af0-b1e4-f0ddaab0926e}

== 不限制数据类型

pre_match限制了a-z的输入，所以使用不了0x开头的16进制，只可以用0开头的8进制进行绕过

intval base=0 代表可以使用8、16进制绕过

//模式分隔符后的"i"标记这是一个大小写不敏感的搜索

e6105e33-0310-4950-acf7-030fa0326862.challenge.ctf.show/?cmd=%0Aphp

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: Firebasky
# @Date: 2020-09-16 11:25:09
# @Last Modified by: hlxa
# @Last Modified time: 2020-09-18 16:16:09
# @link: https://ctfer.com

*/

show_source(__FILE__);
include('flag.php');
$a=$_GET['cmd'];
if(preg_match('/^php$/im', $a)){
        if(preg_match('/^php$/i', $a)){
                echo 'hacker';
        }
        else{
                echo $flag;
        }
}
else{
        echo 'nononononо';
}
```

ctfshow{21d53cec-98ab-43b4-bcea-7a2e8620a005}

/i 不区分大小写 /m 匹配换行

%0A 换行符

eb89e13e-c90d-4d0c-9dff-f1d84c693a38.challenge.ctf.show/?num=%0A010574

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: hlxa
# @Date: 2020-09-16 11:25:09
# @Last Modified by: hlxa
# @Last Modified time: 2020-09-18 16:46:19
# @link: https://ctfer.com

*/

include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
        $num = $_GET['num'];
        if($num==="4476"){
                die("no no no!");
        }
        if(preg_match("/[a-z]/i", $num)){
                die("no no no!");
        }
        if(!strpos($num, "0")){
                die("no no no!");
        }
        if(intval($num,0)===4476){
                echo $flag;
        }
}
```

ctfshow{792f479e-7182-46d1-8933-7e81984a0dc6}

过滤0 使用换行符%0a进行绕过

bd117850-a318-4f50-ae23-eff812177eee.challenge.ctf.show/?num=%0A010574

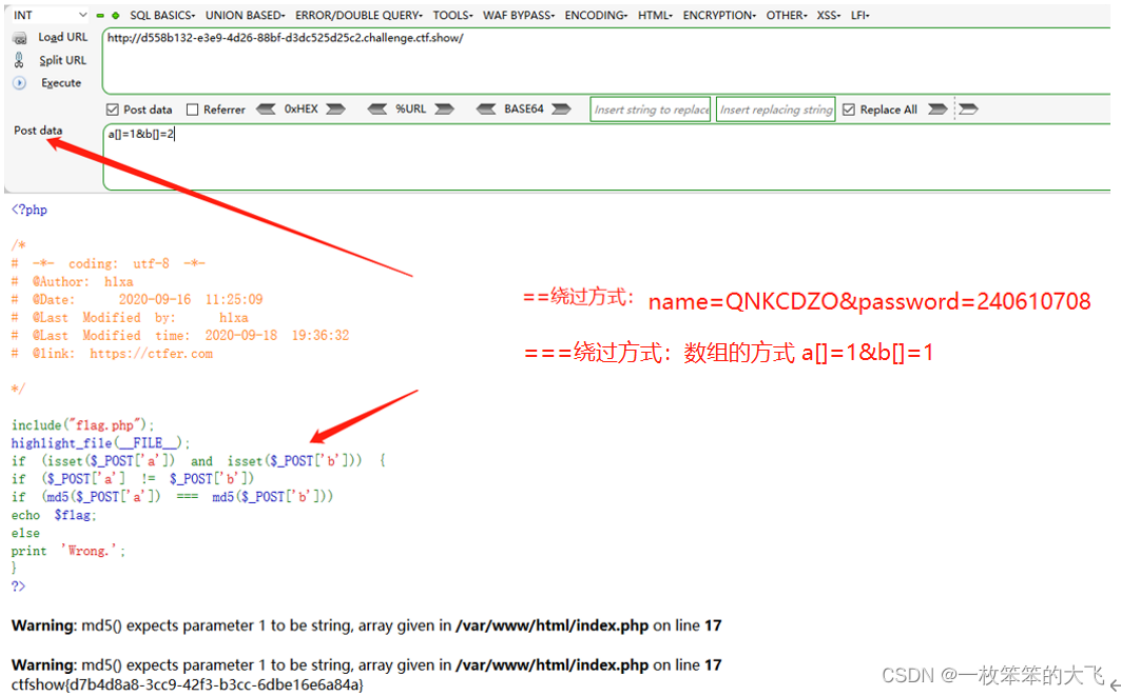
```php
<?php

/*
#  -*-  coding:  utf-8  -*-
#  @Author:  hlxa
#  @Date:      2020-09-16  11:25:09
#  @Last  Modified  by:      hlxa
#  @Last  Modified  time:  2020-09-18  16:53:59
#  @link:  https://ctfer.com

*/

include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
        $num  =  $_GET['num'];
        if($num==4476){
                die("no  no  no!");
        }
        if(preg_match("/[a-z]|\./i",  $num)){
                die("no  no  no!!");
        }
        if(!strpos($num,  "0")){
                die("no  no  no!!!");
        }
        if(intval($num,0)===4476){
                echo  $flag;
        }
}
```

ctfshow{10d6225c-ab8a-47af-9464-285c3796503b}

572ceee6-2d5c-42e2-8918-71967f52fe70.challenge.ctf.show/?u=./flag.php

```php
<?php

/*
#  -*-  coding:  utf-8  -*-
#  @Author:  hlxa
#  @Date:      2020-09-16  11:25:09
#  @Last  Modified  by:      hlxa
#  @Last  Modified  time:  2020-09-18  19:21:24
#  @link:  https://ctfer.com

*/


highlight_file(__FILE__);

if(isset($_GET['u'])){
        if($_GET['u']=='flag.php'){
                die("no  no  no");
        }else{
                highlight_file($_GET['u']);
        }


}

<?php

/*
#  -*-  coding:  utf-8  -*-
#  @Author:  hlxa
#  @Date:      2020-09-16  11:24:37
#  @Last  Modified  by:      hlxa
#  @Last  Modified  time:  2020-09-16  11:25:00
#  @email:  hlxa@ctfer.com
#  @link:  https://ctfer.com

*/


$flag="ctfshow{29823bd9-52e9-4039-afb9-c1e4cbebdc79}";
```

绕过方式：利用文件目录的格式./flag.php ！ = flag.php



name=QNKCDZO&password=240610708

成功的拿到了flag

CTF 离线C PHP python 汇编函数查询 chm电子书合集 离线比赛时使用 学习

strpos() 函数判断字符串中是否包含某字符串的方法 12-20
用php的strpos() 函数判断字符串中是否包含某字符串的方法判断某字符串中是否包含某字符串的方法 if(strpos('www.idc-gz.com','idc-gz') !== false){ echo '包含'; }else{ echo '不包含'; } …

CTF PHP离线chm文档 08-09
CTF PHP离线chm文档

CTF Attack & Defense线下攻防赛比赛技巧.pdf 01-15
不错的资源哦！

CTF-Web-Challenge:使用PHP在Web中进行CTF挑战 03-25
CTF-网络挑战使用PHP在Web中进行CTF挑战链接： ：

php弱类型比较及绕过 weixin_45349299的博客 2602
字符串和数字比较使用==时,字符串会先转换为数字类型再比较，若字符串以数字开头，则取开头数字作为转换结果，不能转换为数字的字符串（例如"aaa"是不能转换为数字的字符串，而"123"或"123aa"…

刷题学习记录（封神台） qq_73861475的博客 151
PHP 过滤器用于对来自非安全来源的数据（比如用户输入）进行验证和过滤。

php一些特性函数（ctfshow） qq_62046696的博客 1825
preg_match()返回 pattern 的匹配次数。 它的值将是0次（不匹配）或1次，因为preg_match()在第一次匹配后 将会停止搜索。preg_match_all()不同于此，它会一直搜索subject 直到到达结尾。 如果发生…

eval函数读取文件 ctf 09-02
引用中提到了一种通过使用file()函数将文件内容存入数组，然后通过var_dump()和eval()函数将数组内容输出到页面的方法。eval()函数的参数是一个字符串，该字符串末尾必须有分号，并且在最后还要…

“相关推荐”对你有帮助么？

非常没帮助 没帮助 一般 有帮助 非常有帮助

大飞先生
码龄3年 暂无认证

38	39万+	27万+	3万+	
原创	周排名	总排名	访问	等级

438	38	22	16	69
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

Ubuntu搭建ARL资产灯塔系统（适用所有版本，5分钟迅速搭建成功） 2058
PHP特性&缺陷对比函数&CTF考点 2031
Python-shellcode免杀分离 1913
CDN绕过篇&漏洞回链&接口探针&全网扫描&反向邮件 1775
PHP-nginx-ctfShow文件上传漏洞 1715

分类专栏

基础的渗透测试 26篇
渗透测试 2篇
http 1篇

最新评论

gophish平台搭建
常微笑: 请问下，大佬，那个邮件报告是收集的哪方面的信息呢?

Python-shellcode免杀分离
Young洋475: 为啥我换成32位了，还是报错呀

PHP特性&缺陷对比函数&CTF考点
wlopghost: 好家伙，正好在上小迪的课就能刷到你这文章
XSS学习笔记（一）、CTFSHOW-316到...
shdkfbbv: 331 借助修改密码重置管理员权限 POST 发送ajax数据包时不用加127.0 ...
PHP-nginx-ctfShow文件上传漏洞
zhuo21hahaha: 咋跟小迪课程的文档内容那么像呢🥰

最新文章

内网安全-隧道技术&SSH实现通信&DNS上线与通信&CS上线Linux主机
Python-shellcode免杀分离
vulnhub-RAVEN:2(MYSQL-UDF提权，手工提权/工具自动提权)

2023年 14篇 2022年 24篇

目录