

[weixin_30333885](#) 于 2018-06-28 19:37:00 发布 39 收藏

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/LOW-ctfer/p/9240356.html>

版权

后台登录

1、看源码

有这样一段php代码

```
<!-- $password=$_POST['password'];
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
$result=mysqli_query($link,$sql);
if(mysqli_num_rows($result)>0){
    echo 'flag is :'.$flag;
}
else{
    echo '密码错误!';
} -->
```

其中关键是

```
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
```

考察md5的这个函数

md5(string, raw)

raw 可选, 默认为false

true:返回16字符2进制格式

false:返回32字符16进制格式

简单来说就是 true将16进制的md5转化为字符了,

那么如果某一字符串的md5恰好能够产生如'or'之类的注入语句, 就可以进行注入了.

难点就在如何寻找这样的字符串, 我上网查函数的时候碰巧找到的

字符串: ffifyop

md5后, 276f722736c95d99e921722cf9ed621c

再转成字符串: 'or'6<trash>

就可以了

FALSE

函数isset(): 检测变量是否设置

只能用于变量, 传递任何其它参数都将造成解析错误. 若想检测常量是否已设置, 可使用 defined() 函数

格式: `isset (mixed var [, mixed var [, ...]])`

若变量不存在或存在但其值为NULL则返回 FALSE

若变量存在且值不为NULL, 则返回 TURE

同时检查多个变量时, 每个单项都符合上一条要求时才返回 TRUE, 否则结果为 FALSE

== : 比较运算符 忽略类型, 只要值相同就可以, 类型不同时也可以
===: 恒等运算符, 同时检查表达式的值与类型。

die()函数 : 停止程序运行, 输出内容

sha1()函数: 计算字符串的 SHA-1 散列。默认的传入参数类型是字符串型

语法: sha1(string,raw)

string 必需。规定要计算的字符串。

raw 可选。规定十六进制或二进制输出格式:

TRUE - 原始 20 字符二进制格式

FALSE - 默认。40 字符十六进制数

阅读代码可知

登录成功条件: (1) 传入name,password的值 (2) name和password的值不能相等 (3) name和password的 sha1加密散列值相等

然后不会了。。搜的

?name[]=a&password[]=b

Form

PIN码(PIN1), 全称Personal Identification Number.就是SIM卡的个人识别密码。

不知道这句话在这里什么意思

查看源码, 发现有一行type 是hidden 就很有意思, name="showsource" value="0"

尝试把0改成1, 就出现了php

这个比较好理解

Once More

题目提示很有用

hint: ereg()函数有漏洞哩; 从小老师就说要用科学的方法来算数。

提示我们要用ereg()函数的漏洞, 并留意科学计数法

看源码

```
ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE
```

语法

```
int ereg(string pattern, string originalstring, [array regs]);
```

定义和用途

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。

Return Value

如果匹配成功返回true,否则,则返回false

这里表示输入的password必须是大小写字母和数字

```
strpos($_GET['password'], '*-') !== FALSE
```

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)

ereg函数漏洞

ereg()函数存在NULL截断漏洞,导致正则过滤被绕过,所以可以用%00来截断正则匹配

用科学记数法构造: 1e8%00*-*

注意URL编码问题

PHP大法

语法

```
int eregi(string pattern, string string, [array regs]);
```

定义和用法

eregi()函数在一个字符串搜索指定的模式的字符串。搜索不区分大小写。Eregi()可以特别有用的检查有效性字符串,如密码。

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。

返回值

如果匹配成功返回true,否则,则返回false

注意输入url后会自动进行一次编码

转载于:<https://www.cnblogs.com/LOW-ctfer/p/9240356.html>