mysql 多字节编码漏洞_[三个白帽子]is_numeric的理解和PHP脚本多字节字符解析模式带来的安全隐患writeup...

原创

胖葫芦 于 2021-02-01 21:31:39 发布 53 收藏
文章标签： mysql 多字节编码漏洞

本文链接：https://blog.csdn.net/weixin_28713299/article/details/113596065

0x01 is_numeric理解

简单翻看is_numeric实现代码，is_numeric对输入的参数，先做了样式判断如果是整型、浮点型就直接返回true，如果是字符串则进入is_numeric_string函数进行判断

```
switch (Z_TYPE_P(arg)) {

case IS_LONG:

case IS_DOUBLE:

RETURN_TRUE;

break;

case IS_STRING:

if (is_numeric_string(Z_STRVAL_P(arg), Z_STRLEN_P(arg), NULL, NULL, 0)) {

RETURN_TRUE;

} else {

RETURN_FALSE;

}

break;

default:

RETURN_FALSE;

break;
```

经过查找，找到真正的处理函数_is_numeric_string_ex,省略一些代码，我们只用知道哪些字符能够出现在is_numeric的参数中，很明显可以看出，

空格、\t、\n、\r、\v、\f、+、-能够出现在参数开头，“点”能够在参数任何位置，E、e只能出现在参数中间。

```
ZEND_API zend_uchar ZEND_FASTCALL _is_numeric_string_ex(.....) /* {{{ */

{

.....

/* Skip any whitespace
```

```
* This is much faster than the isspace() function */
while (*str == ' ' || *str == '\t' || *str == '\n' || *str == '\r' || *str == '\v' || *str == '\f') {
str++;
length--;
}
ptr = str;
if (*ptr == '-') {
neg = 1;
ptr++;
} else if (*ptr == '+') {
ptr++;
}
if (ZEND_IS_DIGIT(*ptr)) {
/* Skip any leading 0s */
while (*ptr == '0') {
ptr++;
}
....
for (type = IS_LONG; !(digits >= MAX_LENGTH_OF_LONG && (dval || allow_errors == 1)); digits++, ptr++) {
check_digits:
if (ZEND_IS_DIGIT(*ptr)) {
tmp_lval = tmp_lval * 10 + (*ptr) - '0';
continue;
} else if (*ptr == '.' && dp_or_e < 1) {
goto process_double;
} else if ((*ptr == 'e' || *ptr == 'E') && dp_or_e < 2) {
const char *e = ptr + 1;
if (*e == '-' || *e == '+') {
ptr = e++;
}
if (ZEND_IS_DIGIT(*e)) {
```

goto process_double;

}

}

break;

}

.....

}

}

再看下我们的题目中第一个需要bypass的地方：

if(is_numeric($num)&&!in_array($num[0],$filter)&&strtolower(urlencode($num[0]))!='%0b'&&!preg_match('/[\s]{1,}/',$num[0]) && !intval($num))

1.is_numeric($num)检测

2.!in_array($num[0],$filter)过滤array('0',' ','\n','\t','\r','\v','\f','+','-');

3.strtolower(urlencode($num[0]))!='%0b'过滤%0b

4.!preg_match('/[\s]{1,}/',$num[0]) 过滤\t\n\r\f\v

5.!intval($num) 必须intval检测返回false

综合看下来”.0“似乎是唯一选择。