世安杯 类型 writeup

原创

风—— 于 2018-10-14 15:41:45 发布 470 收藏

分类专栏： Hacking 文章标签： CTF WEB

本文链接：https://blog.csdn.net/sss937146043/article/details/83047785

打开题目页面后先出现的代码

```php
<?php
show_source(__FILE__);
$a=0;
$b=0;
$c=0;
$d=0;
if (isset($_GET['x1']))
{
        $x1 = $_GET['x1'];
        $x1=="1"?die("ha?"):NULL;
        switch ($x1)
        {
        case 0:
        case 1:
                $a=1;
                break;
        }
}
$x2=(array)json_decode(@$_GET['x2']);
if(is_array($x2)){
    is_numeric(@$x2["x21"])?die("ha?"):NULL;
    if(@$x2["x21"]){
        ($x2["x21"]>2017)?$b=1:NULL;
    }
    if(is_array(@$x2["x22"])){
        if(count($x2["x22"])!==2 OR !is_array($x2["x22"][0])) die("ha?");
        $p = array_search("XIPU", $x2["x22"]);
        $p===false?die("ha?"):NULL;
        foreach($x2["x22"] as $key=>$val){
            $val==="XIPU"?die("ha?"):NULL;
        }
        $c=1;
}
}

$x3 = $_GET['x3'];
if ($x3 != '15562') {
    if (strstr($x3, 'XIPU')) {
        if (substr(md5($x3),8,16) == substr(md5('15562'),8,16)) {
            $d=1;
        }
    }
}
if($a && $b && $c && $d){
    include "flag.php";
    echo $flag;
}
?>
```

依据代码可得需要a,b,c,d都要为1的时候，才可以得到flag。

先来看第一段代码

```php
if (isset($_GET['x1']))
{
        $x1 = $_GET['x1'];
        $x1=="1"?die("ha?"):NULL;
        switch ($x1)
        {
        case 0:
        case 1:
                $a=1;
                break;
        }
}
```

die是php的一个函数，相当于exit（）就是是输出的作用，但是输出完 会退出本脚本，所以我们要避免输出die。 就可得x1需要等于0.

```php
$x2=(array)json_decode(@$_GET['x2']);
if(is_array($x2)){
    is_numeric(@$x2["x21"])?die("ha?"):NULL;
    if(@$x2["x21"]){
        ($x2["x21"]>2017)?$b=1:NULL;
    }
    if(is_array(@$x2["x22"])){
        if(count($x2["x22"])!==2 OR !is_array($x2["x22"][0])) die("ha?");
        $p = array_search("XIPU", $x2["x22"]);
        $p===false?die("ha?"):NULL;
        foreach($x2["x22"] as $key=>$val){
            $val==="XIPU"?die("ha?"):NULL;
        }
        $c=1;
}
}
```

首先是json_decode解码，详情请看 http://php.net/manual/en/function.json-decode.php
键x21的值不可为纯数字，但是需要大于2017，所以只要让键x21的值为2018a就可以。**因为php中大于小于是不会判断类型是否相同**，所以前面是数字就可以通过前面并且大于2017.

x22里面需要是一个数组，且有两个元素，第一个元素也需要是数组，利用array_search有如下特性：

```
[php > $a = array_search("XIPU", [[1],0]);
[php > var_dump($a);
int(1)
```

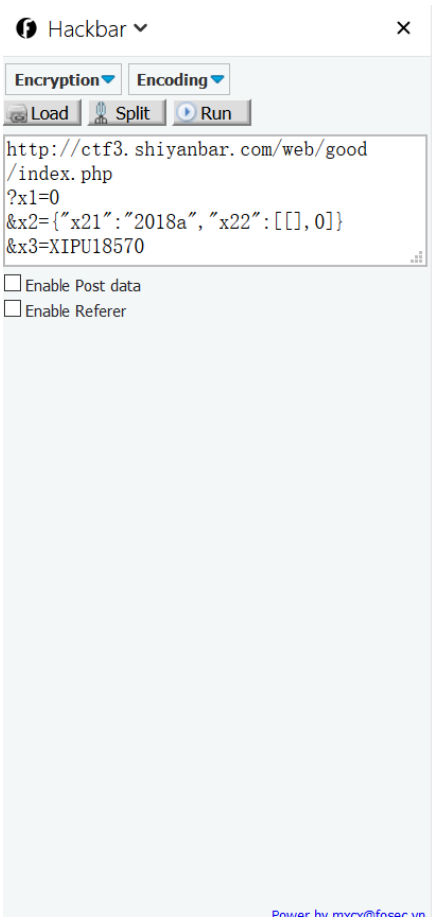


```php
$x3 = $_GET['x3'];
if ($x3 != '15562') {
    if (strstr($x3, 'XIPU')) {
        if (substr(md5($x3),8,16) == substr(md5('15562'),8,16)) {
            $d=1;
        }
    }
}
```

最后的x3是因为15562的MD5是0e开头，在弱比较的时候会判断为0。然后php的MD5是32位的，所以只需要找到前面XIPU加上后面是的数字经过MD5后也为0e开头即可。附上大神脚本。

```python
import hashlib

for i in xrange(1000000):
    s = 'XIPU' + str(i)
    mymd5 = hashlib.md5()
    mymd5.update(s)
    mymd5 = mymd5.hexdigest()
    flag = 1
    if mymd5[8:10] == '0e':
        for j in mymd5[10:24]:
            if j.isalpha():
                flag = 0
                break
        if flag == 1:
            print s
            break
```




```php
                switch ($x1)
                {
                case 0:
                case 1:
                        $a=1;
                        break;
                }
}
$x2=(array)json_decode(@$_GET['x2']);
if(is_array($x2)){
        is_numeric(@$x2["x21"])?die("ha?"):NULL;
        if(@$x2["x21"]){
                ($x2["x21"]>2017)?$b=1:NULL;
        }
        if(is_array(@$x2["x22"])){
                if(count($x2["x22"])!==2 OR !is_array($x2["x22"][0])) die("ha?");
                $p = array_search("XIPU", $x2["x22"]);
                $p===false?die("ha?"):NULL;
                foreach($x2["x22"] as $key=>$val){
                        $val==="XIPU"?die("ha?"):NULL;
                }
                $c=1;
}
}
$x3 = $_GET['x3'];
if ($x3 != '15562') {
        if (strstr($x3, 'XIPU')) {
                if (substr(md5($x3),8,16) == substr(md5('15562'),8,16)) {
                        $d=1;
                }
        }
}
if($a && $b && $c && $d){
        include "flag.php";
        echo $flag;
}
?> CTF{Php_1s_bstl4_1a}
```