i春秋-百度杯十月场-fuzzing

原创

S1lenc3 于 2018-11-01 22:55:00 发布 12 收藏

1. 打开链接，提示 show me key，抓包，传值key=1，GET请求没有用，而POST请求有返回。

2.将md5值直接拿去解密，得到key=ichunqiu105　OK,进入下一步。

3.得到提示，

拿到x0.txt的源代码：发现正好是解密函数。

4.本地搭建环境，进行解密，代码如下：

```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, $ckey_length) :
substr(md5(microtime()), -$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));
    }

}

echo authcode($string =
'46e3F1JIRmzRCyC2nNdtyJesBjT2mVhU7mccXVdvxa6Ta5FpUzdjBZclk48wbnSrnzjQaU5scNsvmCfxawCiDE0aDNzFevY',
$operation = 'DECODE', $key = 'ichunqiu105');
?>
```

5.本地运行，拿到flag