

php writeup,writeup---你真的会PHP吗?

转载

我在这里等着看 于 2021-03-29 05:50:17 发布 38 收藏

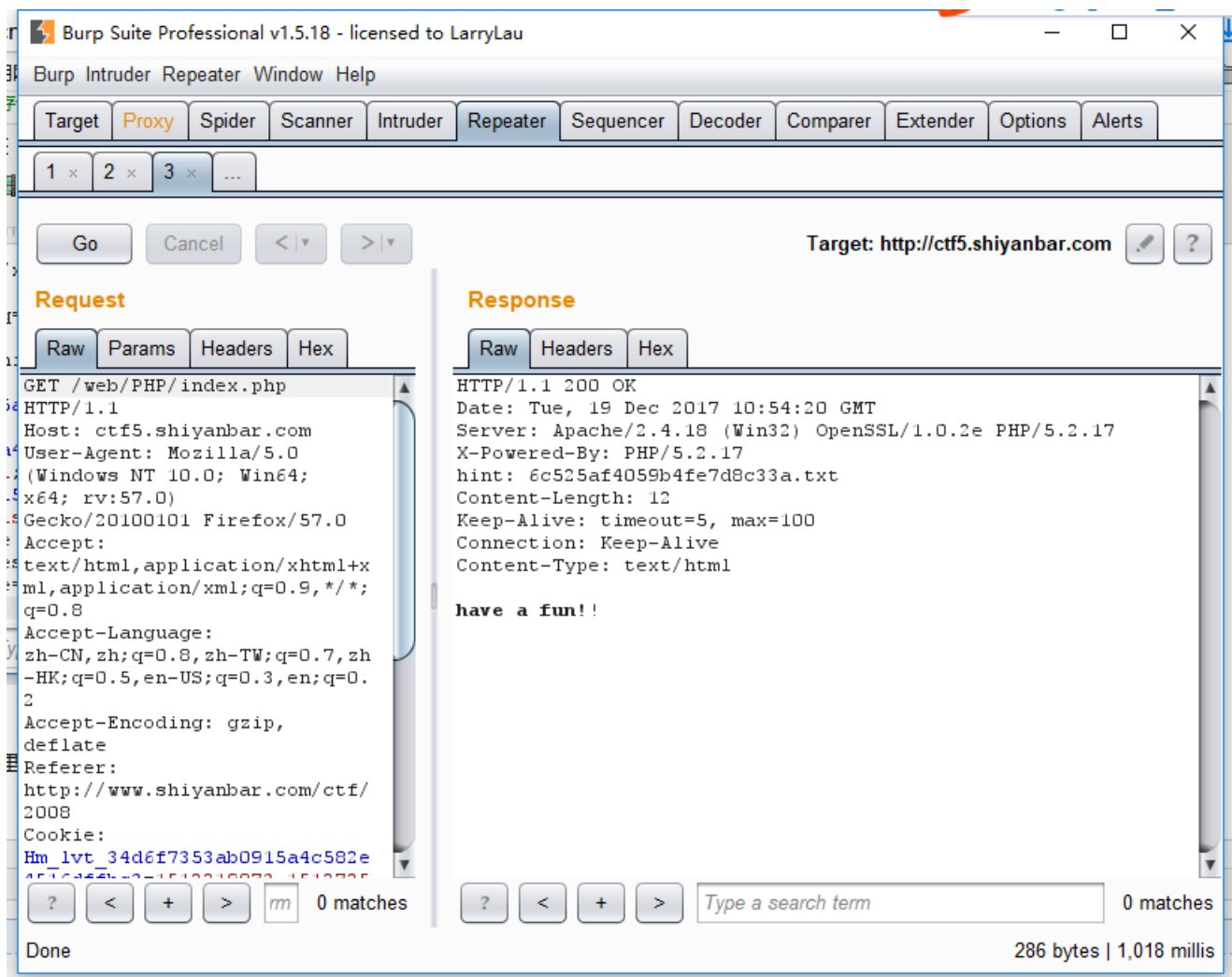
文章标签: [php writeup](#)

实验吧的一道题php审计题.

<http://ctf5.shiyanbar.com/web/PHP/index.php>



抓包发现: hint:.....txt



是这样的, 根据response反馈的信息, 我们可以看见 hint(提示)

那就打开它看看吧

```
ctf5.shiyanbar.com/web/PHP/6c525af4059b4fe7d8c33a.txt
火狐官方网站 火狐官方网站 火狐官方网站 常用网址 JD 京东商城 常用网址 JD 京东商城 火狐官

<?php

$info = "";
$req = [];
$flag="xxxxxxxxx";

ini_set("display_error", false);
error_reporting(0);

if(!isset($_POST['number'])){
    header("hint:6c525af4059b4fe7d8c33a.txt");

    die("have a fun!!");
}

foreach($_POST as $global_var) {
    foreach($global_var as $key => $value) {
        $value = trim($value);
        is_string($value) && $req[$key] = addslashes($value);
    }
}

function is_palindrome_number($number) {
    $number = strval($number);
```

代码审计

//条件1: 判断是否为数值型

```
if(is_numeric($_REQUEST['number'])){
```

```
$info="sorry, you can't input a number!";
```

```
}elseif($req['number']!=strval(intval($req['number']))){ //条件二: 判断intval(number)是否等于原来number的值
```

```
$info = "number must be equal to it's integer!! ";
```

```
}else{
```

```
$value1 = intval($req["number"]);
```

```
$value2 = intval(strrev($req["number"]));
```

```
if($value1!=$value2){ //条件三: 判断翻转后number的值是否相等
```

```
$info="no, this is not a palindrome number!";
```

```
}else{
```

```
if(is_palindrome_number($req["number"])){ //条件四, 判断number是否为回文字符串
```

```
$info = "nice! {$value1} is a palindrome number!";
```

```
}else{
```

```
$info=$flag;
```

```
}
```

```
}
```

```
}
```

```
echo $info;
```

分析:

number 不能是数字

```
number2 = trim(number)
```

```
intval(number2) = number2
```

```
intval(number2) = intval(strrev(number2))
```

trim(number) 不是回文

解:

第一个条件(1): 很好解决, 末尾加一个空白字符

第二个条件(3): 只要是一个在表示范围内的数字字符串都行

第三, 第四个条件(4,5): 正常思维下, 是相互矛盾, 不能共存的,

但是我们可以利用intval(string)函数特点-----当string太大, 或者格式错误(不是数字串)时返回 0

+ 数字 有正数负数, 正数翻转后还是数, 负数(-12)翻转后(12-)就不是一个数了, + intval(-0) = 0

所以 构造字符串 '-0 ' 就可以满足所有条件了

The image shows a browser's developer tools interface with two panels: 'Request' and 'Response'.
The 'Request' panel shows a POST request to /web/PHP/index.php. The raw request body is 'number=-0%00'.
The 'Response' panel shows an HTTP 200 OK response. The raw response body is 'FLAG{2dd8711082fe24c19ae8}'.