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

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';
?>
```

观察可知要构造cookie:lScer=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）