08
/
04
2017
33
期

本期议题：1000种姿势 绕过软WAF

Python Fuzz脚本编写　　难度系数 ★★★☆☆

本期大咖

V@1n3R | 科拉实验室

怀揣干货分享精神的非娱乐圈无名小黑。web渗透爱好者，热衷于讨论分享，刻苦钻研。擅于使用Python编写脚本。

内容框架

- 01:速览基础知识
- 02:Fuzz脚本思路及实现
- 03:Fuzz特殊字符串
- 04:Fuzz寻找bypass规律
- 彩蛋1:tamper脚本编写
- 彩蛋2:sqlmap外部ip代理池拓展

KNOW IT THEN HACK IT

大咖面对面

该信息安全技术公益讲座由漏洞银行方主办

每周五晚20:00，业内大咖与你零距离分享

答疑解惑 | 资源交换 | 剖析动态 | 认知升级

众多专家与你我共同扬帆，畅游知识海洋

BUGBANK

漏洞银行 | BUGBANK

33期

“1000种姿势”绕过软WAF --Python Fuzz脚本编写

主讲： V@1n3R.

团队：科拉实验室

所需技能（一）Python基础入门

变量与输出字符串

```
counter = 100 # 赋值整型变量
miles = 1000.0 # 浮点型
name = "John" # 字符串
print (counter)
print (miles)
print (name)
print(“Hello world!”)
print(“Hello”+”world”)
a = 'hello'
b = 'world'
print(a+b)
```

所需技能（一）Python基础入门

条件判断（if）：

```
age = 3
if age >= 18:
    print('your age is', age)
    print('adult')
else:
    print('your age is', age)
    print('teenager')
```

所需技能（一）Python基础入门

List（列表）

```
list = [] #声明list是一个列表,大前提！
list = ['a','b','c']
print(list)


a = ['a']
b = ['b']
c = ['c']
list =  a+b+c      #多个列表组合成一个列表
print(list)
```

所需技能（一）Python基础入门

迭代（遍历列表）：

```
list = [1,2,3,'a','b','c']
for i in list:                    #循环遍历列表
        print(i)
```

所需技能（二）requests库安装以及简单使用

requests安装

Python3 -m pip install requests OR pip3 install requests OR pip install requests

requests简介

import requests #导入requests库

requests.get(‘https://github.com/timeline.json’) #GET请求，本次所需要用到的method

requests.post(“http://httpbin.org/post”) #POST请求

requests.put(“http://httpbin.org/put”) #PUT请求

requests.delete(“http://httpbin.org/delete”) #DELETE请求

requests.head(“http://httpbin.org/get”) #HEAD请求

requests.options(“http://httpbin.org/get”) #OPTIONS请求

所需技能（三）phpstudy下载安装

phpstudy安装

http://www.phpstudy.net/phpstudy/phpStudy20161103.zip

fuzz测试所需要的php文件

http://www.lz1y.cn/fuzz.zip

安装phpstudy的操作不在本次课程范围内，具体百度，也可以使用别的组件集成工具

Fuzz脚本思路

Waf(web应用防火墙)

Web应用防护系统（也称：网站应用级入侵防御系统。英文：Web Application Firewall，简称： WAF）。利用国际上公认的一种说法：Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一款产品。

检测sql注入

所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。SQL防护功能主要包括3点，分别是检测URL长度功能，检测URL非法功能和注入的防护规则。

而诸如狗狗此类防护产品都是正则匹配客户端发出的HTTP请求，然后拦截含有危险字符的请求已达到防护效果。

Bypass思路

本地搭建测试环境(mysql+apache)后,编写fuzz脚本利用环境特性爆破payload利用requests库发送请求，

打开web防护软件,过滤掉无效请求，根据response的content,来判断请求是否成功执行了注入。

sqlmap请求 抓包

使用sqlmap的--proxy代理参数,即可使用burp查看sqlmap的注入请求。

举个栗子:

某狗敏感点（Mysql数据库）

union select

含有information_schema等关键字的注入payload

一些mysql内置函数

等等..

更多的需要自己去fuzz测试,这里就不说了

Fuzz脚本实现

Fuzz

所谓fuzz也就是匹配模糊测试，这里我们就需要使用脚本来实现了

例如　很早之前 内联注入即可过狗(/*!union*/ /*!select*/ 1,2,3 --+)，现在狗狗的正则库也强大起来了。

不过还是有空可以钻。所以本次就使用内联注释来进行Fuzz。

Bypass实现

接下来就看我演示吧。

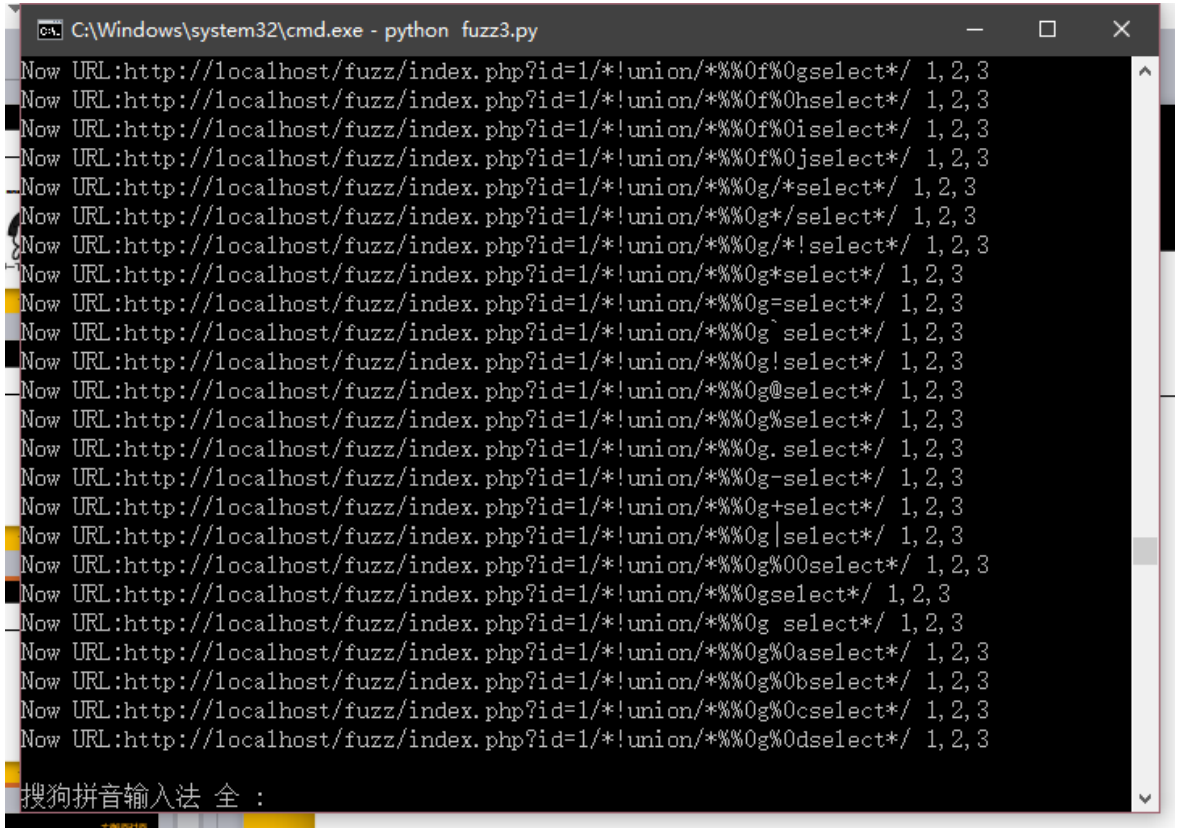
Fuzz脚本实现

Fuzz脚本

http://www.lz1y.cn/?p=659

密码:Fuzz

Fuzz脚本实现



本地Fuzz截图

Fuzz特殊字符

小部分

```
fuzz_zs = ['/*','*/','/*!','?','*','=','`','~','!','@','%','.','-','+','|','%00'.'%20' ,'%09', '%0a', '%0b', '%0c', '%0d' ,
'%a0' ,'/**/']
fuzz_sz = ['0','1','2','3','4','5','6','7','8','9']
fuzz_ch = ["%0a","%0b","%0c","%0d","%0e","%0f","%0g","%0h","%0i","%0j","%0k","%0l","%0m","%0n",
"%0o","%0p","%0q","%0r","%0s","%0t","%0u","%0v","%0w","%0x","%0y","%0z"]
```

以上仅仅为本人使用的,更多的需要自己发现...

彩蛋--自动化注入:Tamper脚本实现

Tamper脚本

神器sqlmap中的tamper提供了不少有意思的且有用的脚本，用以绕过各种waf，奈何现在waf也摸透了神器的自带脚本。

使用方法 sqlmap.py -u url --tamper=tampername.py

Tamper脚本实现

tamper库中有不少优秀的脚本，我们可以仿照现成的脚本

，修改成我们所需要的效果

脚本所在文件夹 ： ./sqlmap/tamper

注意TAMPER脚本满足条件:

*Mysql数据库

*Apache or IIS特定防护产品

彩蛋--自动化注入:Tamper脚本实现

apostrophemask	用UTF-8全角字符替换单引号字符
apostrophenullencode	用非法双字节unicode字符替换单引号字符
appendnullbyte	在payload末尾添加空字符编码
...	...
versionedmorekeywords	用MySQL注释包围每个关键字
versionedkeywords	用MySQL注释包围每个非函数关键字
...	...

完整介绍：

http://www.lz1y.cn/wordpress/?p=652

漏洞银行 | BUGBANK
www.bugbank.cn