2018

Sqlmap 视频课程

Sqlmap请求参数设置

课程内容

1. Sqlmap设置超时

2. Sqlmap设置重试次数

3. Sqlmap设置随机化参数

4. Sqlmap设置日志过滤目标

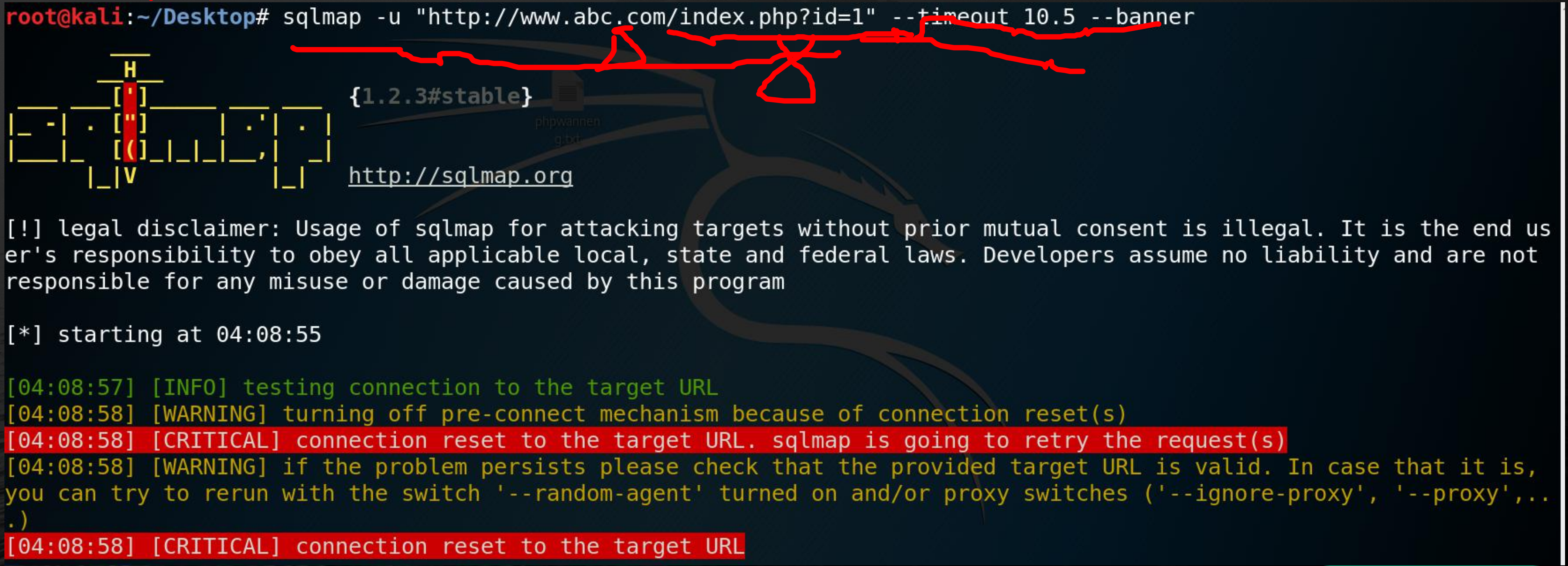
01

Sqlmap设置超时

Sqlmap中设置超时

在考虑超时HTTP(S)请求之前，可以指定等待的秒数。有效值是一个浮点数，例如10.5表示10秒半。默认设置为30秒。

例如：--timeout 10.5



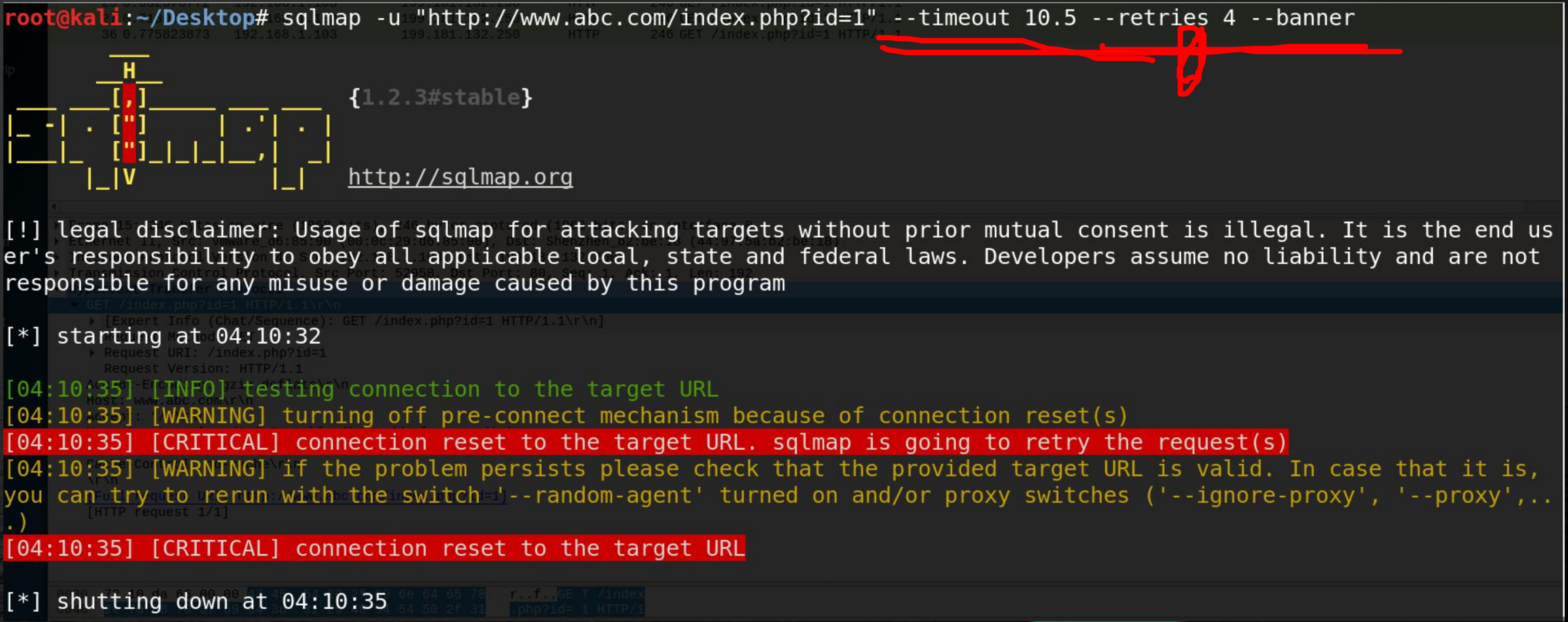
```
root@kali:~/Desktop# sqlmap -u "http://www.abc.com/index.php?id=1" --timeout 10.5 --banner
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.3#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 at 04:08:55

[04:08:57] [INFO] testing connection to the target URL
[04:08:58] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[04:08:58] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[04:08:58] [WARNING] if the problem persists please check that the provided target URL is valid. In case that it is,
you can try to rerun with the switch '--random-agent' turned on and/or proxy switches ('--ignore-proxy', '--proxy',..
.)
[04:08:58] [CRITICAL] connection reset to the target URL
```

02

Sqlmap设置重试次数

Sqlmap中设置重试次数

--retries count 设置对应重试次数，默认情况下重试3次。



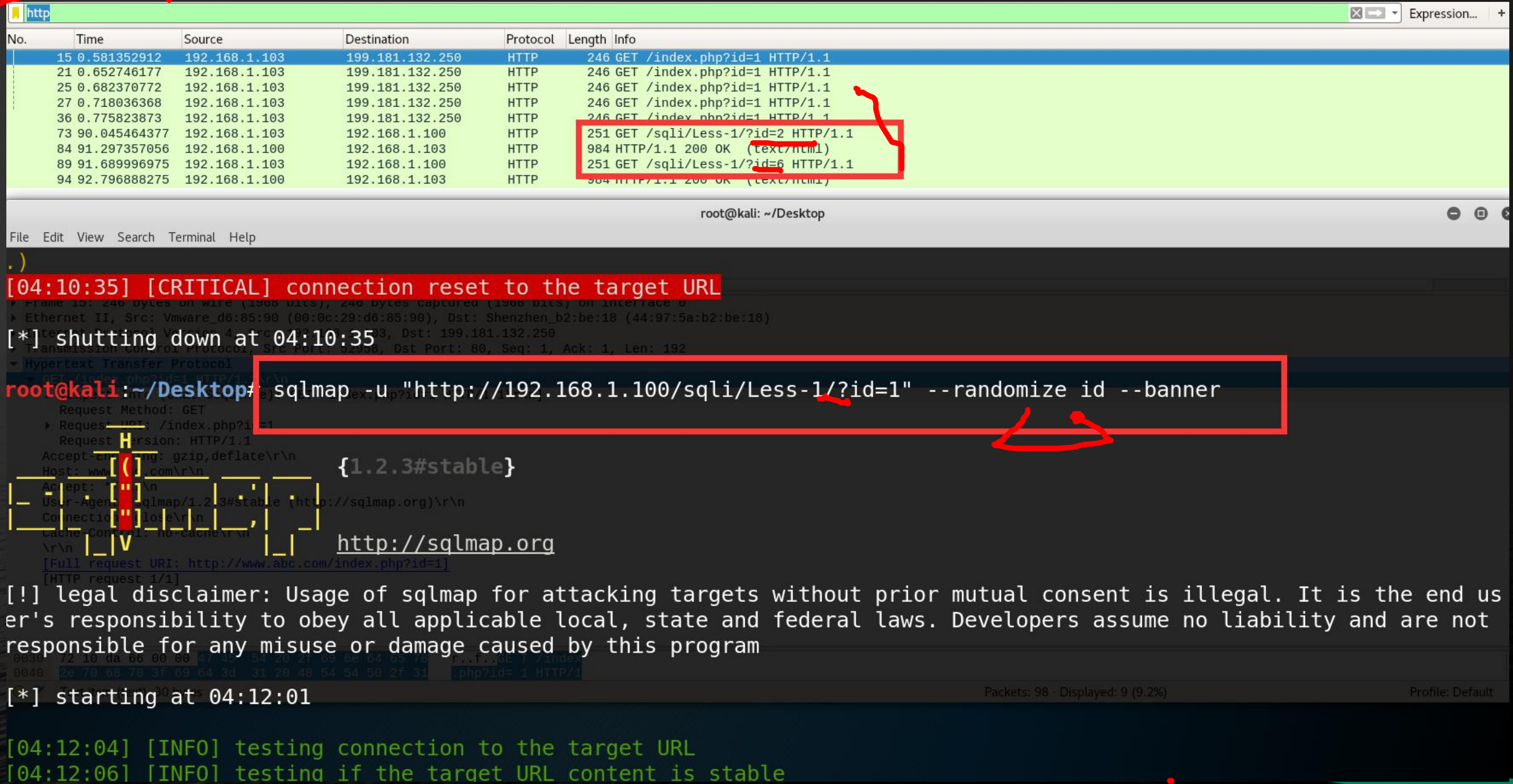
```
root@kali:~/Desktop# sqlmap -u "http://www.abc.com/index.php?id=1" --timeout 10.5 --retries 4 --banner
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.2.3#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 at 04:10:32

[04:10:35] [INFO] testing connection to the target URL
[04:10:35] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[04:10:35] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[04:10:35] [WARNING] if the problem persists please check that the provided target URL is valid. In case that it is,
you can try to rerun with the switch '--random-agent' turned on and/or proxy switches ('--ignore-proxy', '--proxy',..
.)
[04:10:35] [CRITICAL] connection reset to the target URL

[*] shutting down at 04:10:35
```

03

Sqlmap设置随机化参数

Sqlmap可以指定要在每次请求期间随机更改其值的参数名称。长度和类型根据提供的原始值保持一直。

--randomize 参数名称



```
No.  Time          Source         Destination     Protocol Length Info
  15 0.581352912   192.168.1.103  199.181.132.250 HTTP     246 GET /index.php?id=1 HTTP/1.1
  21 0.652746177   192.168.1.103  199.181.132.250 HTTP     246 GET /index.php?id=1 HTTP/1.1
  25 0.682370772   192.168.1.103  199.181.132.250 HTTP     246 GET /index.php?id=1 HTTP/1.1
  27 0.718036368   192.168.1.103  199.181.132.250 HTTP     246 GET /index.php?id=1 HTTP/1.1
  36 0.775823873   192.168.1.103  199.181.132.250 HTTP     246 GET /index.php?id=1 HTTP/1.1
  73 90.045464377  192.168.1.103  192.168.1.100   HTTP     251 GET /sqli/Less-1/?id=2 HTTP/1.1
  84 91.297357056  192.168.1.100  192.168.1.103   HTTP     984 HTTP/1.1 200 OK  (text/html)
  89 91.689996975  192.168.1.103  192.168.1.100   HTTP     251 GET /sqli/Less-1/?id=6 HTTP/1.1
  94 92.796888275  192.168.1.100  192.168.1.103   HTTP     984 HTTP/1.1 200 OK  (text/html)
```

```
.)
[04:10:35] [CRITICAL] connection reset to the target URL

[*] shutting down at 04:10:35

root@kali:~/Desktop# sqlmap -u "http://192.168.1.100/sqli/Less-1/?id=1" --randomize id --banner
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.3#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   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 at 04:12:01

[04:12:04] [INFO] testing connection to the target URL
[04:12:06] [INFO] testing if the target URL content is stable
```

04

Sqlmap设置日志过滤目标

与使用选项-l使用从提供的日志解析的所有主机不同，您可以指定有效的Python正则表达式，用于过滤所需的日志。

```
python sqlmap.py -l burp.log --scope="(www)?\.target\.(com|net|org)"
```

--skip-urlencode 不进行URL加密。

总结

1. Sqlmap设置超时
2. Sqlmap设置重试次数
3. Sqlmap设置随机化参数
4. Sqlmap设置日志过滤目标

sdpez

谢谢

欢迎关注 后续课程