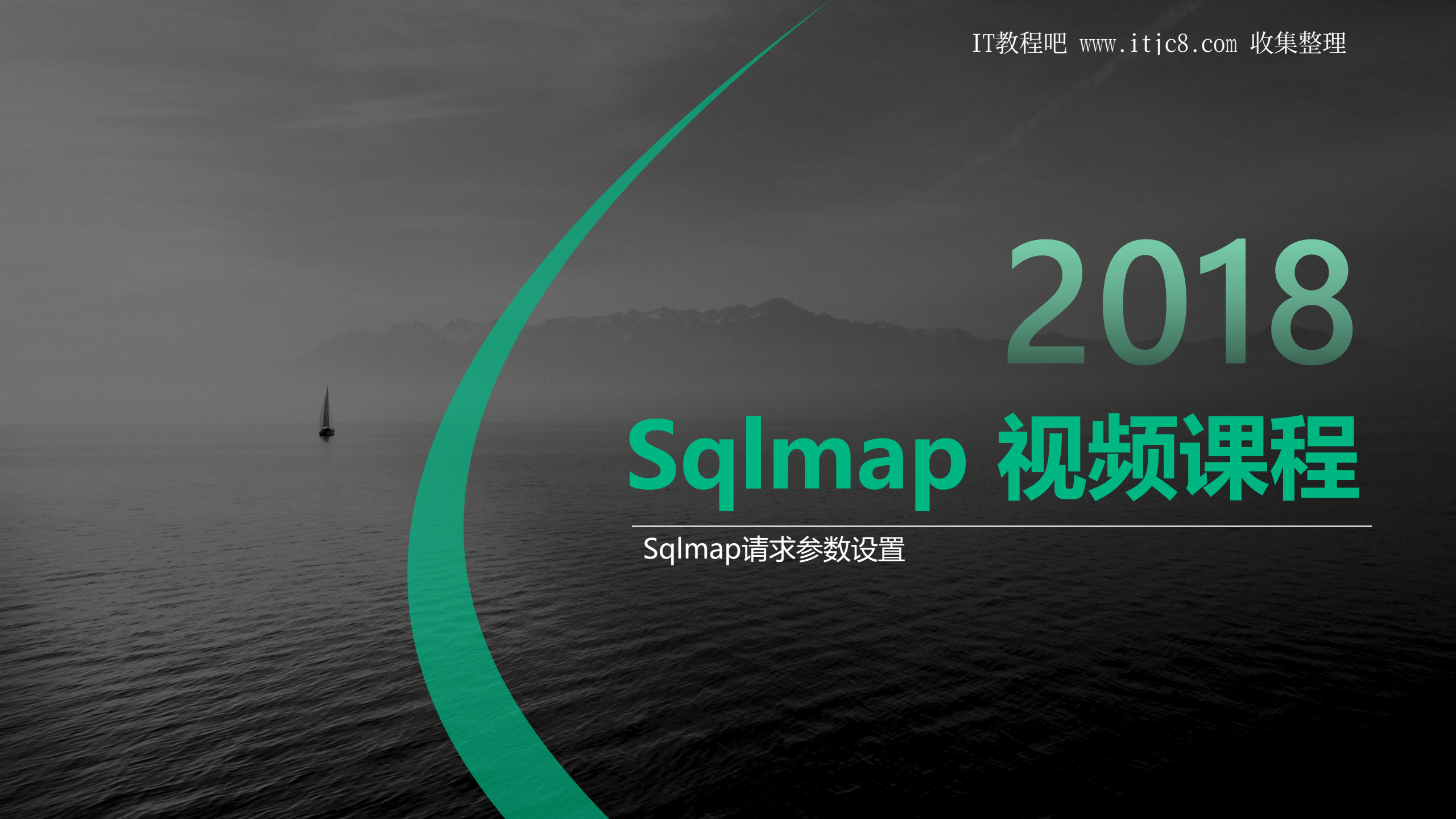


2018

Sqlmap 视频课程

Sqlmap请求参数设置

课程内容

1. Sqlmap设置User-Agent
2. Sqlmap设置Host头
3. Sqlmap设置Referer头
4. Sqlmap设置额外HTTP头

01

Sqlmap设置User-Agent

默认情况下，sqlmap使用以下用户代理头值执行HTTP请求: sqlmap/1.0-dev-xxxxxxx (http://sqlmap.org)

然而，通过提供自定义用户代理作为选项的参数，可以使用选项——user-agent来伪造它。

此外，通过 --random-agent, sqlmap将从./txt/user-agent中随机选择一个用于会话中的所有HTTP请求。
一些站点在服务端检测HTTP User-Agent值，如果不是一个合法的值，就会中断连接。同时Sqlmap也会曝出错误。

[hh:mm:20] [ERROR] the target URL responded with an unknown HTTP status code, try to force the HTTP User-Agent header with option --user-agent or --random-agent

注意针对User-Agent的值探测SQL注入，需要设置--level 值为3.

02

Sqlmap设置Host头

可以手动设置HTTP主机头值。默认情况下，从提供的目标URL解析HTTP主机头。

注意，如果 --level设置为5,将对HTTP主机头进行SQL注入检测。

03

Sqlmap设置Referer头

伪造HTTP Referer值是可能的。默认情况下，如果没有显式设置，HTTP请求中不会发送HTTP引用头。

请注意，如果--level设置为3或以上，将针对HTTP引用头 进行SQL注入测试。

04

Sqlmap设置额外HTTP头

通过设置选项--header，可以提供额外的HTTP标头。每个标头必须用换行符分隔，从配置INI文件中提供它们要容易得多。可以查看示例sqlmap.conf文件。

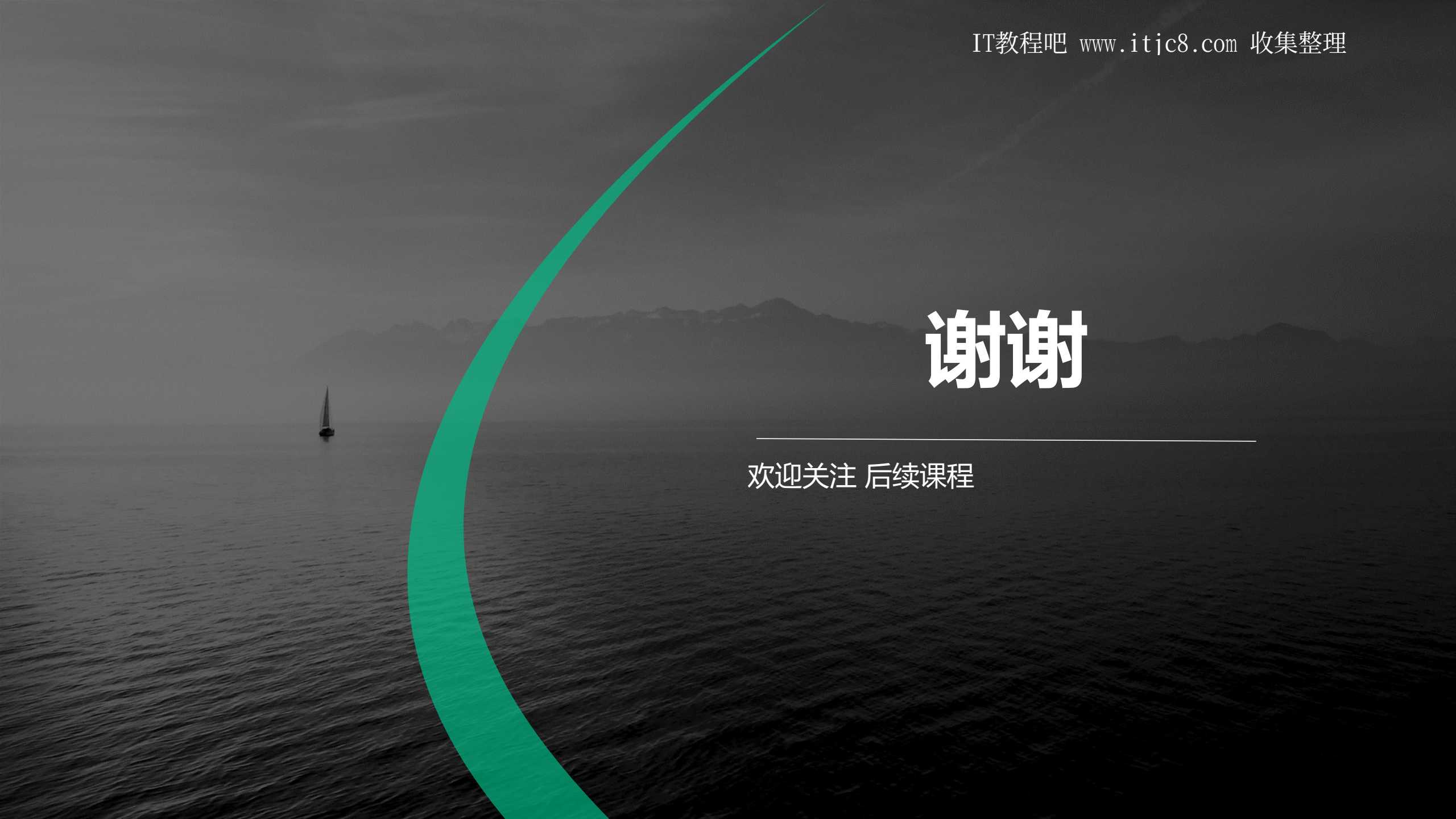
python sqlmap.py -u "http://192.168.21.128/sqlmap/mysql/get_int.php?id=1" --headers="Host:www.target.com\nUser-agent:Firefox 1.0" -v 5

sqlmap.conf

```
67  # sqlmap will also test for SQL injection on the HTTP User-Agent value.
68  agent =
69
70  # Use randomly selected HTTP User-Agent header value.
71  # Valid: True or False
72  randomAgent = False
73
74  # HTTP Host header value.
75  host =
76
77  # HTTP Referer header. Useful to fake the HTTP Referer header value at
78  # each HTTP request.
79  referer =
80
81  # Extra HTTP headers
82  headers = Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
83   Accept-Language: en-us,en;q=0.5
84   Accept-Charset: ISO-8859-15,utf-8;q=0.7,*;q=0.7
85
```

总结

1. Sqlmap设置User-Agent
2. Sqlmap设置Host头
3. Sqlmap设置Referer头
4. Sqlmap设置额外HTTP头



谢谢

欢迎关注 后续课程