2018

Sqlmap 视频课程

SqImap注入 注入位置介绍

课程内容

1. Sqlmap注入介绍
2. Sqlmap设置指定注入参数
3. Sqlmap设置URI注入位置
4. Sqlmap设置任意注入位置

01

Sqlmap注入介绍

Sqlmap注入介绍

所谓SQL注入，就是通过把SQL命令插入到Web表单提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。具体来说，它是利用现有应用程序，将（恶意的）SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。

由此可见：SQL注入发生位置 HTTP数据包中任意位置

上节课：1、-o 可以开启所有性能优化参数
2、--thread 默认线程数为1
3、--null-connectin:为了检索没有body响应的内容。

02

Sqlmap设置指定注入参数

Sqlmap测试参数

-p, --skip --param-exclude --skip-static

-p ：指定具体探测的参数。例如：-p “id,user-agent”

--skip：忽略探测具体的参数。 例如：--level --skip “user-agent,referer”

--param-exclude：忽略包含具体内容的参数。例如：--param-exclude="token|session" 不对包含token或session的参数进行探测。

--skip-static：忽略非动态参数

03

Sqlmap设置URI注入位置

当注入点位于URI本身内部时，会出现一些特殊情况。除非手动指向URI路径，否则sqlmap不会对URI路径执行任何自动测试。必须在命令行中添加星号(*)来指定这些注入点。

例如，当使用Apache web服务器的mod_rewrite模块或其他类似的技术时，这就显得特别有用了

python sqlmap.py -u "http://targeturl/param1/value1*/param2/value2/"

04

Sqlmap设置任意注入位置

与URI注入点类似，星号(*)(注意:这里也支持Havij样式%INJECT %)也可以用来指向GET、POST或HTTP头中的任意注入点。注入点可以通过在带有选项-u的GET参数值、带有选项-数据的POST参数值、带有选项-H的HTTP头值、带有选项-头、用户代理、引用和/或cookie的HTTP头值中指定，或者在带有选项-r的文件中加载的HTTP请求的通用位置指定。

python sqlmap.py -u "http://targeturl" --cookie="param1=value1*;param2=value2"

总结

1. Sqlmap注入介绍
2. Sqlmap设置指定注入参数
3. Sqlmap设置URI注入位置
4. Sqlmap设置任意注入位置

谢谢

欢迎关注