2018

Sqlmap 视频课程

Sqlmap注入参数介绍

课程内容

1. Sqlmap强制设置DBMS
2. Sqlmap强制设置OS系统
3. Sqlmap关闭负载转换机制
4. Sqlmap关闭字符转义机制

01

Sqlmap强制设置DBMS

Sqlmap DBMS指定

默认情况下Sqlmap会自动识别探测目标Web应用程序的后端数据库管理系统（DBMS），以下列出Sqlmap完全支持的DBMS种类。

Mysql、Oracle、Microsoft SQL Server、IBM DB2、SQLite、Firebird、Sybase、SAP MaxDB、HSQLDB、Informix

--dbms 数据库管理系统名称 [版本号]

例如：--dbms mysql 5.0 、--dbms microsoft sql server 05

02

Sqlmap强制设置OS系统

Sqlmap OS指定

默认情况下Sqlmap会自动识别探测目标Web应用程序的后端操作系统（OS），以下列出Sqlmap完全支持的OS种类。

Linux 、Windows

例如：--os windows 或 --os linux

请注意，此选项不是强制性的，强烈建议只在完全确定底层操作系统的后端数据库管理系统时才使用它。如果不知道它，让sqlmap自动为您识别它。

03

Sqlmap关闭负载转换机制

在检索结果时，sqlmap使用一种机制，在这种机制中，所有条目都被转换为字符串类型，并在NULL值的情况下用空格字符替换。这样做是为了防止出现任何错误状态(例如，将空值与字符串值连接起来)，并简化数据检索过程本身。尽管如此，还是有报告的案例(例如MySQL DBMS的旧版本)由于数据检索本身的问题(例如没有返回值)需要关闭这种机制(使用此开关)。

--no-cast

04

Sqlmap关闭字符转义机制

在sqlmap需要在有效负载中使用(单引号分隔)字符串值(例如，选择'foobar')时，这些值将自动转义(例如，选择CHAR(102)+CHAR(111)+CHAR(111)+CHAR(98)+CHAR(97)+CHAR(114))。这样做的原因有两个:混淆有效负载内容和防止后端服务器上查询转义机制(例如magic_quotes和/或mysql_real_escape_string)的潜在问题。用户可以使用这个开关关闭它(例如减少有效负载大小)。

--no-escape

总结

1. Sqlmap强制设置DBMS
2. Sqlmap强制设置OS系统
3. Sqlmap关闭负载转换机制
4. Sqlmap关闭字符转义机制

谢谢

欢迎关注