

Penetration Testing on Websites Using jSQL Injection

Vineeth M V

PG Scholar

Department of Master of Computer Applications
Amal Jyothi College of Engineering
Kottayam, Kerala, India
vineeth@mca.ajce.in

Paulin Paul

Assistant Professor

Department of Master of computer applications
Amal Jyothi College of Engineering
Kottayam, Kerala, India
paulinepaul@amaljyothi.ac.in

Abstract— jSQL Injection is a Java-based SQL injection tool for retrieving database information from a remote server. Provides a standardised way to access a database using SQL from within Java. It is open source, free, and cross-platform (Windows, Linux, Mac OS X, Solaris). jSQL uses JSON Objects to extract data from databases (s) .The GNU General Public License (GNU GPL or GPL) is a commonly used free software licence that allows users to run, study, exchange, and change software. Creating a database connection with a JDBC (Java DB Connectivity) Driver, SQL-like syntax, and SQL feature implementation: Where, Group By, Having, Aggregate functions, Order By [Desc], Join, Left Join, Select [Distinct] [Top], Delete and update, Data in a table can be graphically sorted and filtered.; table records can be added, edited, and deleted immediately on the table data grid; they can also be exported as insert sql commands, textual content, or an Excel record structure (XLS)

I. INTRODUCTION

Kali Linux is a Debian GNU/Linux-based enterprise-ready security auditing Linux distribution. Kali is designed at security professionals and IT directors, and it allows them to perform improved penetration testing, forensic analysis, and security audits. On March 13th, 2013, Kali Linux was born and released. It's a security-focused variant of Linux that comes with a slew of tools for finding flaws and securing your network. Kali includes hundreds of tools for diverse information security activities, including penetration testing, security research, computer forensics, and reverse engineering. It was created by Offensive Security's Manti Aharoni and Devon Kearns as a rebuild of Backtrack, their prior information security testing Linux distribution

A. Features and other information of Kali Linux

- Kali includes over 600 penetration testing tools.
- Always has been (and always will be) free (as in beer)
- Created in a safe environment
- Support for multiple languages
- Completely customizable etc.
- OS Family - Unix like
- Working State – Active
- Kernel Type - Monolithic kernel (Linux)
- Default UI - GNOME3
- Release. Kernel 5.2.9, GNOME 3.30.2

B. History of Kali Linux

- Knoppix, the forerunner of Kali Linux, was the first bootable live Linux operating system, and it is still in use today.
- Knoppix project was then forked into Whoppix and then re-forked into WHAX.
- Backtrack had an extended reign of almost seven years as the penetration testers and hacker's desire.
- Backtrack is a custom designed native environment devoted to hacking. As of 2011 it turned into used by more than four million newbie and professional security researchers.

C. Penetration Testing

It's also known as penetration testing, and it's the process of evaluating a computer system, network, or internet app to find weaknesses that an attacker could exploit. A penetration test may attempt to exploit those flaws in the same way that a hostile hacker would, reducing the actual list of device flaws to a handful of security flaws.

Following are the different Strategies of penetration testing

• Targeted testing

It's completed by way of a collaboration between the agency's IT and penetration testing teams. Because everyone can see the test being performed, it's commonly referred to as a "lights-on" technique.

• External testing

This sort of audit focuses on a company's outwardly visible servers and devices, such as DNS, e-mail servers, Web servers, and firewalls. The goal is to see if an outside attacker can get in and if so, how they can get in after they have gained access.

• Internal testing

This test simulates an inside attack behind the firewall with the aid of a licenced user with elevated entry credentials. This type of check is useful for evaluating how much damage an unhappy employee would want to do.

- Blind testing

By severely limiting the facts revealed to the character or crew executing the test ahead, a blind test methodology simulates the manoeuvres and approaches of a real attacker. Normally, they should be given the employer's phone number. This type of examination may be costly because it necessitates a significant amount of time for reconnaissance.

D. Benefits of Penetration Testing

- Intelligently control vulnerabilities
- keep away from the charge of community downtime
- Meet regulatory requirements and avoid fines

II. JSQL-JavaScript Query Language

JSQL Injection is a Java-based SQL injection tool for retrieving database information from a remote server. Provides a standardised way to access a database using SQL from within Java. It is open source, free, and cross-platform (Windows, Linux, Mac OS X, Solaris). JSQL uses JSON Objects to extract data from databases (s). I normally use sqlmap to identify and exploit SQL injections. It is a command-line utility that can do a variety of tasks, including using all conceivable SQL injection methods, attempting to defeat server protection, and creating shells. It's also cross-platform, dependable, and efficient. Because sqlmap is so powerful and adaptable, it provides a plethora of options for the command-line programme. For newcomers, this may appear to be excessively difficult. The graphical interface of JSQL Injection is fantastic. The application is written in Java, and it is cross-platform and resource-light. The executable file is only 2.14 MB in size.

A. Installation

Install Java 8 or higher, then download the most recent release and double-click the jsqI-injection-v0.83.jar file to start the software. To launch the software, execute java -jar jsqI-injection-v0.83.jar in your terminal. If you're using Kali Linux, you may acquire the current version by typing sudo apt-get -f instal jsqI or by running apt update then apt full-upgrade.

B. Find a Vulnerable URL

You can find out via Google's dork list. OR, look for a URL that ends in php?id=xx, where 'xx' is a number value. Example: <http://www.website.com/user.php?id=3>

Add a single quote (') to the end of the URL, for example, <http://www.website.com/user.php?id=xx'>.

And don't be surprised if you get a SQL Syntax Error! Keep your cool because this is a vulnerable site.

C. Features Provided by the JSQI

- Admin Page - Aids in the discovery of website admin pages
- Read File - Assists in reading a file's content
- Web shell - A web shell is a script that can be posted to a web server to enable remote administration of the computer
- SQL shell - The MySQL Shell can be used to perform data queries and changes as well as numerous administration tasks.
- Upload - Assists in the upload of a file to a directory.
- Brute force - Assists in the decryption of the Hash ID

- Encoding – Assists in encrypting a string into a Hash of any type.

D. Limitations

Only if the site is not secured will the jsqI injection function. Even though dorks are provided, finding the vulnerability on the site is tough. Large databases are difficult to retrieve since they take a long time. Brute-Force injection in jsqI takes a long time.

III. jSQL GUI AND ITS WORKING

It extracts data from the database in the form of JSON Values as a first step. The JSON Value is then subjected to a variety of JSQI injection instructions. The database is checked for vulnerabilities using JSQI. You don't have to use any commands, which makes JSQI the most user-friendly tool for SQL Injection.

Figure 1: jsqI interface



Figure 2: Database list fetched using jsqI injection tool

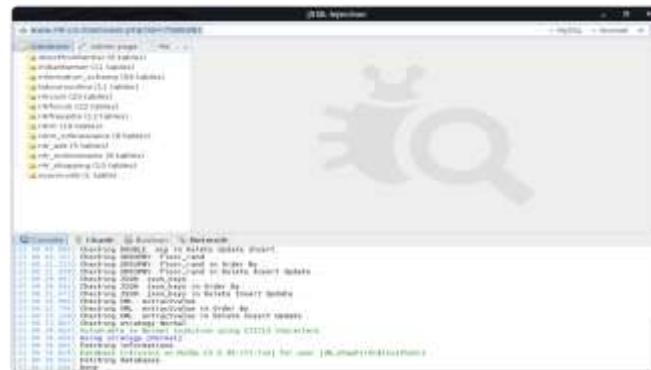


Figure 3: Table list fetched from selected database using jsqI injection tool

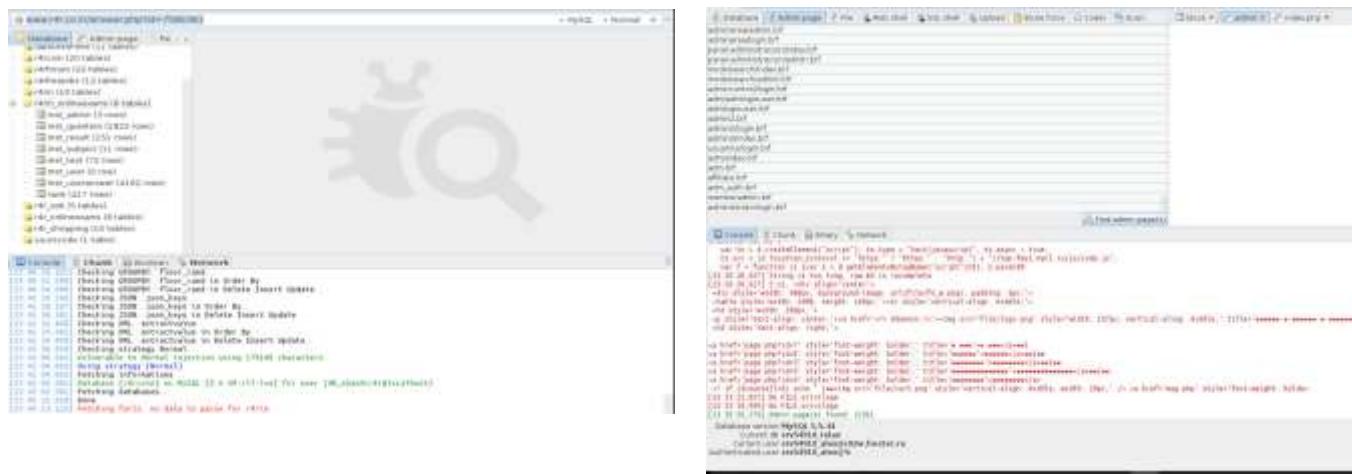
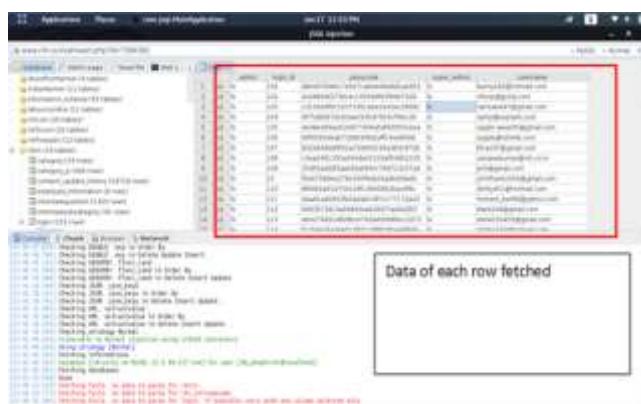


Figure 4: Rows list fetched from selected table using jSQL injection tool



Figure 5: Data from selected rows fetched using jSQL injection tool



A. Search for Admins with jSQL Injection

Go to the next tab to do so. We have a list of potential addresses here. You have the option of checking one or more pages:

B. Operations with files after detection of SQL injections

In addition to database activities such as reading and editing, in the event of SQL injection detection, the following file operations are possible:

- reading files stored on the server
- uploading and unloading fresh files to the server
- bringing Shelves to the server for unloading

And all this is implemented in JSQl Injection!

There are several restrictions, such as the SQL server's need for file permissions. They are disabled in reasonable system administrators, and access to the file System Get will fail. It is sufficient to verify for the presence of file privileges. Go to one of the tabs (reading files, shell creation, new file download) and try to perform one of the tasks listed.

C. Mass checking sites on SQL injection

This feature, too, is JSQl injection. Everything is really simple: simply download the list of sites (which you may import from a file), select the ones you want to verify, and press the appropriate button to begin the process.

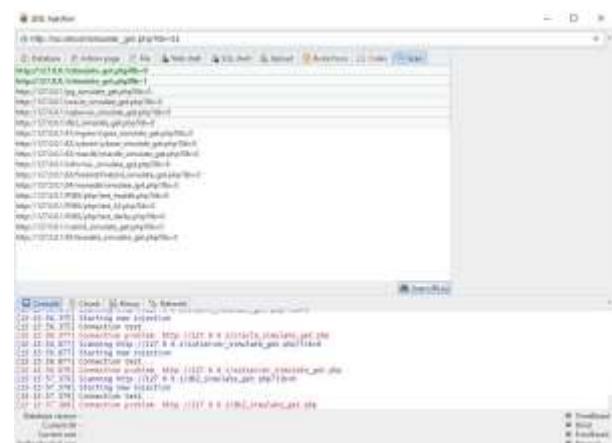


Figure 6: Admin page tab in jSQL injection

IV. BBQSQL INJECTION AND JSQL INJECTION ARE COMPARED IN THIS STUDY.

BBQSQL Injection:

BBQSQL, often known as the 'Blind SQL' injection framework, assists you in resolving challenges when the available exploitation tools are ineffective. It's a semi-automatic programme written in Python that enables for some customisation for any complex SQL injection findings. BBQSQL uses a menu-driven technique to ask various questions and then constructs the injection/attack based on the user's response. It's a versatile tool with a built-in user interface to make it easy to use. It's also quick because to the use of Python Gevent. Cookies, Files, HTTP Auth, Proxies, URL, HTTP Method, Headers, Encoding techniques, Redirects behaviour, and so on are all covered. Setting up parameters and choices, as well as configuring the attack as needed, are all part of the pre-use prerequisites.

It is possible to adjust the tool's setup to employ either a frequency or a binary search strategy. It can also tell if the SQL injection was successful by scanning for specified values in the application's HTTP responses. If the attacker successfully leverages SQL Injection, the database will produce an Error message complaining about the wrong syntax of the SQL Query. The way data is retrieved from the database is the only difference between Blind SQL and regular SQL injection.

jSQL Injection:

jSQL is a java-based SQL Injection tool that is free, open-source, and cross-platform compatible. It's put together with the help of libraries like Hibernate, Spock, and Spring. Access, MySQL, SQL Server, Oracle, PostgreSQL, SQLite, Teradata, Firebird, Ingris, and many other databases are supported by jSQL Injection. The source code for jSQL Injection is hosted on GitHub, and Travis CI is used for

continuous integration. It looks for a variety of injection tactics, including Normal, Error, Blind, and Time. Other functions include searching for administration pages, brute-force password hashing, Web shell and SQL shell development and visualisation, and so on. jSQL Injection can read and write data. jSQL injection is supported by Kali, Parrot OS, Pentest Box, BlackArch Linux, and other pen-testing distributions.

V. CONCLUSION

jSQL Injection is a good, powerful tool for finding and exploiting web sites that are vulnerable to SQL injection. Its undeniable benefits include ease of use and built-in related functions. When it comes to website analysis, jSQL Injection can be a novice's best friend.

It, like any graphical interface tools, cannot be automated with scripts. However, thanks to the built-in feature of mass web site scanning, some automation is available in this application as well.

The sqlmap programme is substantially more difficult to use than the jSQL Injection application. However, sqlmap allows for more sorts of SQL injection, as well as dealing with file-based firewalls and other features.

As a result, jSQL Injection is a beginner hacker's best friend.

VI. REFERENCES

- [1] David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni "Metasploit The Penetration Tester's Guide", pp. 2-12, July 2011.
- [2] <https://jsql.codeplex.com/>
- [3] [http://cyborg.ztrela.com/jsql.php/](http://cyborg.ztrela.com/jsql.php)
- [4] https://www.w3schools.com/js/js_json_sql.asp
- [5] <http://www.json.org/>
- [6] <http://www.pentestingexperts.com/jsql-injection-java-based-automated-sql-injection-tool>