SQL Injection Prevention

Anshuman Singh¹, Suresh Kumar N.²

¹Galgotias University Department of Computer Science and Engineering
²Guide, Galgotias University Department of Computer Science and Engineering

Abstract: As internet applications began to kind thousands per-day therefore did the technology behind them however today’s application is found to dangerous vulnerability and since 2003 SQL injection remains the prime most in the application security list that the company is wrestling with. As application area unit growing chop-chop application security is conjointly a concern for the business. however even through these threats their area unit straightforward things that we have a tendency to will do to shield ourself from these attacks. Internet security is nothing however protective the application against all the threads one of them is SQL injection. Organisations United Nations agency area unit failing to secure there internet application run the risk of being attacked. It is largely due to the vulnerability gift in their application. In order to avoid these attacks we have a tendency to want to perceive that however these attacks area unit performed. Once having the information of however these attacks area unit performed we have a tendency to can be in a position to defend ourself from these sort of attacks. internet sites area unit static and dynamic therefore we have a tendency to want to tack together them consequently. As the employment of web full-growngrownupgrownupgrownupgrownupchop-chop therefore the likelihood of being compromised conjointly grown. In this world of web our each data is on-line therefore the wrongdoer will exploit those knowledge and will use my knowledge against Maine to launch an attack. The nature of the attack might vary various.

1. Introduction

In recent years the use of net has been inflated exponentially with the advancement of technology. these days net is used by general population for the purpose such as money group action, education and myriad different activities. the posh of transferring cash from one place to another by a finger tip comes with security risk. Today’s websites and applications square measure operating laborious to keep there user’s knowledge confidential. In this method there is a race between the company and the offender. The offender finds new ways in which to attack the websites and application wherever because the company tries to secure them and fix the bugs. Let’s currently strive to perceive what is truly SQL injection is? SQL injection is a code injection technique used to execute malicious SQL statements. A SQL question or a info question is generated on internet application and it fetches with the info and relevant info is sent to the user. The user have solely management over the SQL question input thus user have to input the question thus logically that it ought to come back the price as true. SQL question is in one means AN application interacts with info.

2. Literature Survey

In the section of literature survey I undergo with a number of papers available on the internet. Their are a number of works done on it. There are also a large number of people currently working on this topic.

As a comprehensive study guide i used on of a master’s project by ‘Jagdish Halde’ on the topic “SQL injection analysis, Detection and prevention” in “San jose state University.

I also undergo some of the papers published in IEEE journal which are mention below.

Ethical Hacking: SQL-injection by Sean Oriyano (2016)

A second-order SQL-injection detection methods by Chen Ping Detection of SQL-injection attacks by removing the parameters values of SQL query by Rajashree A. Kotole, Swati S. Sherekar. Thus one can find a number of resources for the purpose of literary survey.

3. Methods

SQL injection is one of the top possible attacks on websites and web applications for a long time. A SQL injection occurs when an application fails to sanitize the user input data. An attacker can use specially crafted SQL commands to control web application’s database server. A attacker can add modify and sometime delete records in a database affecting data integrity. Using this vulnerability the attacker can do unimaginable things. Let’s understand this with a non-technical example. Let’s assume a fully automated bus. It works on instruction given by human through a stander web form. The form may look like as:

Drive through <route> and <where should the bus stop?> if <when should the bus stop?>

Sample Populated form

Drive through route77 and stop at the bus stop if there are people at the bus stop.

Now if Someone manages to input these instruction.

Drive through route77 and do not stop at the bus stop and ignore the rest of the does exactly what it is told to do. We are and the supplied data are not separated properly. So the automated bus does not differentiate between the instruction and the data. It simply does anything that it is fixed with.

SQL injection attack: Technical Explanation

An SQL injection needs two conditions to exist which is a relational database that uses SQL and a user controlled input which is directly used in a SQL query.

For example

$ statement = “SELECT”
form. If there are people at the bus stop.
Now Since the bus is fully automated it
able to do that because the query structure
FROM users
WHERE username = ' $ user'
AND password = ' $ password'
Now if the codes are not properly sanitized
by the web application the attacker can
easily search some malicious SQL statement.
For example:
$ Statement = " SELECT * 
FROM users
WHERE username = ' dean or 
'1' = '1' --'
AND password = '12345'

Here we need to note that ‘1’="1' is a condition which will
always be true there for it is accepted as a valid input. And
here the double hyphen(--) is used to tell SQL that the rest
part is a comment and should not be executed. So the part
that is password part will be ignored. Here we are trying to
bypass the password authentication process.

Impact of SQL injection attack SQL injection attack can
cause unimaginable damage to websites and web application.
It can extract sensitive information like social security
number, credit card details. It can misuse authentication
details. The attacker can get the data and use them during
other attacks. The attacker can also alter the data in database
without authorization. He can add extra users and remove the
previous records. The attacker can also control the behaviour
of application. The attacker can also delete and drop tables
from the database.

We are aware of the fact that how much damage SQL attack
can cause to the database of any website and web
application.
Now we will focus on the different types of SQL attacks that
are possible and how our system will be able to tackle them.
SQL attacks are mainly divided into three categories In-Band
SQL, Blind SQL, Out-of-band.

In-band SQL
Channels of communication in this attack is same. It means
that they launch their attack and gather results through same
channel. It is the most common kind of attack as a result of
of it’s simplicity. It is additional divided into 2 types: Error-
based SQL— Attacker do such activities therefore that the
info provides error messages. The wrongdoer uses those info
made by error messages. Someday these info is therefore
important that it will cause a vital damage. Union-based
SQL— In this kind of attack the wrongdoer takes the
advantage of union-operator. In this methodology multiple
statement ar combined to get a single protocol response. This
single response might contain important info.

Blind SQL
In this attack the offender sends varied requests to the server
and with varied payloads. The offender observes the
responses given by the server and strive to squeeze some
helpful info. It is grasp as the blind SQL attack as a result of
of the truth that the offender is not ready to see the info
returning out of the server. Since all depends on the
behaviour of the server thus it is terribly slow method.
Boolean— That offender sends a SQL question to the info
forcing the applying to send a result. The result can relying
on whether or not the question is true or false. based mostly
on the result, the info at intervals the communications
protocol response can modify or keep unchanged. The
offender will then work out if the message generated a true
or false result.

Time-based— offender sends a SQL question to the info,
that makes the info wait (for a time in seconds) before it will
react. The offender will see from the time the info takes to
respond, whether or not a question is true or false. On the
basis result, AN communications protocol response can be
generated instantly or once a waiting amount. The offender
will therefore guess out if the message they used came true
or false, while not depending on information from the info.

Out-of-band SQL
Attacker will do this attack solely their ar some options
out there in the information server used by the internet
application. The attacked is used as a substitute to the in-
band attack. It is done once the aggressor is not in a position
to use the same channel to attack the information and gather
info. It is conjointly most well-liked once a server is terribly
slow or unstable to launch a attack. These techniques count
on the capability of the server to produce DNS or hypertext
transfer protocol requests to transfer knowledge to associate
aggressor.

Proposed System
Stephen Thomas and Laurie Williams explained well
concerning the strategies that square measure used to
forestall AN SQL injection attacks: 1 Static analysis 2 Run
time analysis These techniques square measure supported the
hold on procedures, Authors’ has used management flow
graph that notifies what user inputs to the dynamic designed
SQL statement. management flow graphs square measure
terribly helpful to reduce the set of SQL statements to verify
users input. In run time analysis we have a tendency to
access info concerning hold on statement from Finite State
Automaton to slim the verification procedure and to point the
user’s inputs true or false

Static analysis
In static analysis authors’ provides the program referred to as
hold on procedure program that is used to extracts the
“control flow graph” from the saved procedures, we are able
to see intimately about the management graph in following
section. At the beginning, we tend to label each execution
statement within the management flow graph so use the
backtracking methodology to verify all statements
participated within the formation of the SQL statement
within the management flow graph.

Run Time Analysis
In dynamic analysis, SQL injection attack checker perform is
employed to reason the user input. during this methodology,
author used “current session” symbol to spot the input taken
from user, and exploitation same session id, builds a finite
state automaton, to ascertain legitimacy of SQL statement
received from user, the SQL statement along side user inputs
is compared with corresponding SQL statement of finite state
automaton.

**SQL Prevention**

There are numerous effective ways that stop SQL attacks from taking place, as well as protective against them, ought to they occur. The initial step is input validation (a.k.a. sanitization), that is the observe of writing code that will establish illegitimate user inputs. While input validation ought to continually be thought-about best observe, it is seldom a foolproof answer. The reality is that, in most cases, it is merely not possible to map out all legal and banned inputs—at least not while not inflicting a massive variety of false positives, that interfere with user experience and an application’s practicality. For this reason, a net application firewall (WAF) is usually used to filter out SQL, as well as alternative on-line threats. To do so, a WAF usually depends on a massive, and perpetually updated, list of meticulously crafted signatures that enable it to surgically weed out malicious SQL queries. Usually, such a list holds signatures to address specific attack vectors and is often patched to introduce obstruction rules for freshly discovered vulnerabilities.

4. **Conclusion**

As we tend to saw that even a variety of work and analysis is done on SQL-injection instead of these SQL-injection remains in the high of the threads offered to internet application. Thus to overcome with this drawback we tend to have to build our internetsites and web application such that they have all the conditions and methodologies to shield them from attacks. We have to properly sanitise our code therefore that the aggressor will not misuse them. We tend to additionally use varied SQL injection symbol tools to apprehend the drawback and fix them. We tend to will use the tools like SQL map, JSQL injection, BBQSQL, NoSQL map, DSSS and several additional.

5. **Future Work**

As future work, we wish to guage ways mistreatment totally different internet based mostly application script with property right to attain nice accuracy in SQL injection interference approaches. Integrate SQLiX with nikto HTTP scanner, HTTP scanning proxies, and with metasploit can helps to find different internet vulnerabilities. additionally add feature to dump venerable info and info schema.

**References**


