www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 5 Issue 11 Nov. 2016, Page No. 19155-19158*

# Exposure Of Sql Injection In Packet Stream

***M.Sharada Varalakshmi[1], V.Harika Naidu[2], Shreya Valluri[3]***

[1]Associate Professor of Computer Science dept., St. Peter`s engineering college, Hyderabad
*sharada.mangipudi07@gmail.com*

[2]Student of Computer Science dept., St. Peter`s engineering college, Hyderabad
*harrynk1.0@gmail.com*

[3]Student of Computer Science dept., St. Peter`s engineering college, Hyderabad
*shreya.valluri1@gmail.com*

**Abstract**: ***Capture the data flowing from client application to the server in a network as pcap files. And then, analyze them to detect if they contain sql injection type string patterns. SQL injection is an attack in which malignant code is inserted into strings that are eventually passed as an instance of sql server.***

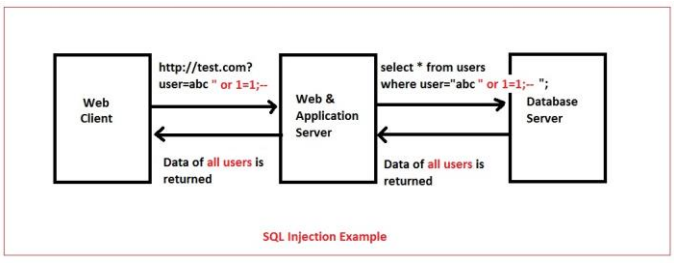
**Keywords:** SQL Injection, PCAP programming.

## 1. Introduction

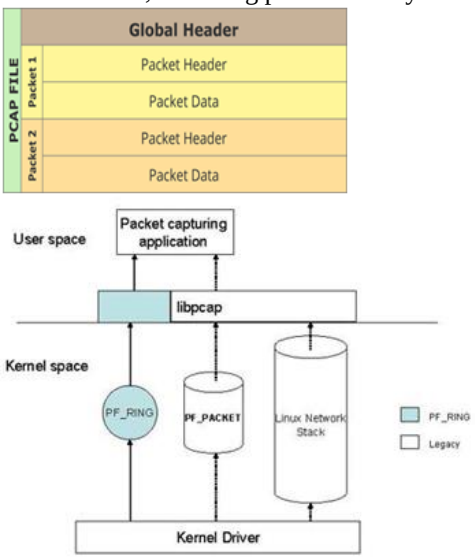
Sql is a programming language that lets us manage data stored in rdbms. Therefore, sql can be used to access, modify and delete data. Rdbms can also run commands on the operating system from a sql statement.

Keeping the above in mind, it's easier to understand how advantageous a successful SQL injection attack can be for an attacker. [2]

- An attacker can use sql injection to avoid authentication or even portray as specific users.
- One of sql primary functions is to select query and generate result of that query. Sql injection vulnerability allows complete disclosure of data present on a database server.
- Since web applications use sql to modify data within a database, an attacker could use sql injection to manipulate data stored in a database. Modifying the data affects data integrity and could cause numerous issues, for instance, issues such as invalid transactions, altering balances and other valuable records.
- As we know Sql is also used to delete records from a database. An attacker could use sql injection vulnerability to delete data from a database. [2]




**PCAP** (Packet Capture) is a procedure or set of rules for wireless Internet communication that allows a computer to receive incoming radio signals from other device and convert those signals into required and usable information. Libpcap provides functions for user-level packet capture, which is used in low-level network monitoring. It mainly provides the packet-capture and filtering engines of many open source and certain network tools, including protocol analyzers.




## 2. Literature survey

As we know sql injection has ability to destroy users key details so, many organizations have conducted research in order to avoid this crucial problem. Some of them can be listed as; [5]

- Web application firewalls play a key role in filtering out the malicious data. So, to some extent this sql injection can be avoided by the firewalls.
- Encrypting all the stored data instead of keeping them in a plain text format. So that even if attackers dump your database, they'll extract less content from it.
- Usage of parameterized equations is a simple technique to avoid sql injections.

- Almost all SQL databases and programming languages are pretty much vulnerable to MS SQL Server, Oracle, DB2, MS Access, MY SQL Informix, etc.

It is an input validation problem that needs to be considered and programmed by the web application developer.

SQL injection attack not only occurs on SQL databases but also occur on PHP applications. Because of all such scenarios Microsoft has give preventive advisories to the users in order to protect the data. Tools that they created to avoid Sql injections are: [5]

- URL scanner: It prevents some harmful requests from reaching the web application and SQL Server. It works on IIS 5.1 and later and IIS 7.0 for Windows Server 2008.
- HP Scrawlr: can detect and identify whether your website is susceptible to an SQL injection attack.
- Microsoft source code analyzer for SQL injection: Tool analyzes your static ASP source code written in VBScript (not ASP.NET) and reveals possible vulnerabilities to SQL injection attacks. The tool then generates a report detailing the vulnerabilities it detected and possible remedies.[5]

## 3. Proposed work

Sql injection is a malicious code injection technique, used to attack data-driven applications, in which dreadful sql statements are inserted into an entry field .Sql injection exploits a security vulnerability in an application's software. Sql injection is mostly known as an attack medium for websites that can be used to attack any type of Sql database. [2]

**Impacts of a SQL Injection:**

If a web application is vulnerable to sql injection, a hacker can execute any malicious sql query through the web application. Thereby, he has privileges to retrieve all the data stored in the database such as customer's valuable information, credit card or debit card details, security numbers and credential to access administrator portal. By a sql injection it is also possible to drop tables from the database. Therefore with a sql injection the user has full access to the database. Depending on your hardware and software setup and the type of server being used, by sql injection vulnerability some hackers might also be able to write to a file or execute operating system commands. With such immense privileges this might result into a total server hack. [2]

**Example of a basic sql injection:**

- For this SQL injection example we will consider a login page where users enter their credentials to login to a website or portal.

- When a user submits login details like username and password, the web application uses these credentials in an sql query and thereby sent to the backend database to get executed and depending on the result of the query, the web server determines if the login credentials are valid or not, thus allowing the user to access the portal or denying access.

- E.g. if the username is "admin" and the password is "12345678", the web application sends an sql query that is exactly similar to the one below the database to verify the login credentials: [1] [3]

  SELECT * FROM Users WHERE name = 'admin' AND password = '12345678'

- Suppose a hacker enters something like "test' OR 1 = 1--" instead of the username and anything else as password. In this case the SQL query will look like the below: [4]

- SELECT * FROM Users WHERE name = 'test' OR 1 = 1 --' AND password = 'xxxxx'

The above sql statement will always return true because: [4]

1. Name= 'test' or 1 = 1 will anyways return a true statement (1 OR 1 = 1)
2. The rest of the sql statement after -- sign is commented out, i.e. that particular part of the query is not executed.

Since the database returns a true value, the hacker is able to trick the web applications server and henceforth, manages to gain access to a logged in session. This type of injection vulnerability can also be used to further retrieve data from the database, such as table names and their content. [1] [3]

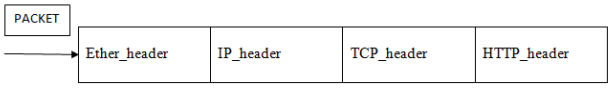
**PCAP** is the backbone for most commercial wireless programs. It essentially converts digital information into radio signals which are known as packets, by using a specific algorithm. A wireless device can then receive and convert those packets back into certain

information by decoding radio signals with the same algorithm that is used. Pcap also provides security for a wireless network. It can be used as a protocol analyzer, traffic generator, network tester, network monitor, network intrusion detection system. Libcap, is a library or a package which is used to grab packets right as they come off from the network card.

Compiling a pcap program requires linking with the pcap lib. In order to install use syntax: **sudo apt-get install libpcap-dev.**

## 4. Implementation

- Capturing the packets and retrieving the content of the packet.




- Moving the packet pointer to IP_header.

DOI: 10.18535/ijecs/v5i11.79

- Moving the pointer from IP_header to TCP_header.
- Moving a pointer from TCP_header to HTTP_header.
- Retrieving the content of the http header.
- Comparing the packet contents with existing payloads list and log them if any payloads existing in a packet.

**Algorithm**

**STEP 1**: Create a text file listing different payloads.

**STEP 2:** Find the list of devices available using pcap_findalldevs ().

**STEP 3**: Select a device along with the number of packets to be captured.

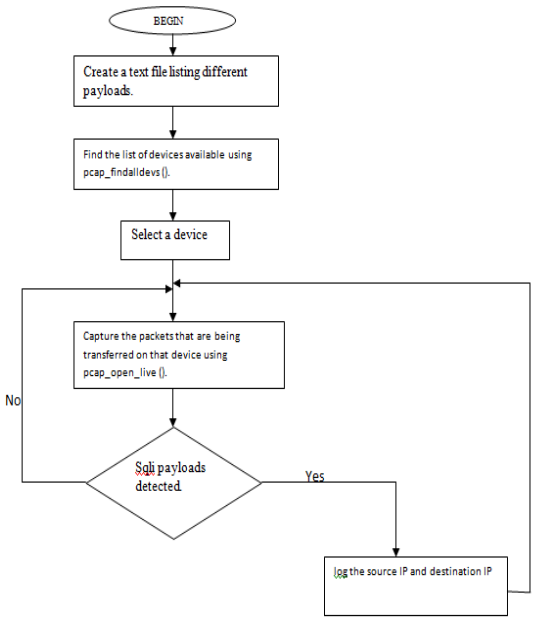
**STEP 4**: Capture the packets that are being transferred on that device using pcap_open_live ().

**STEP 5**: Check whether the packet information contains SQLI payloads.

**STEP 6**: If SQLI payloads detected then log the source IP and destination IP.

**STEP 7**: Repeat 4 – 6.

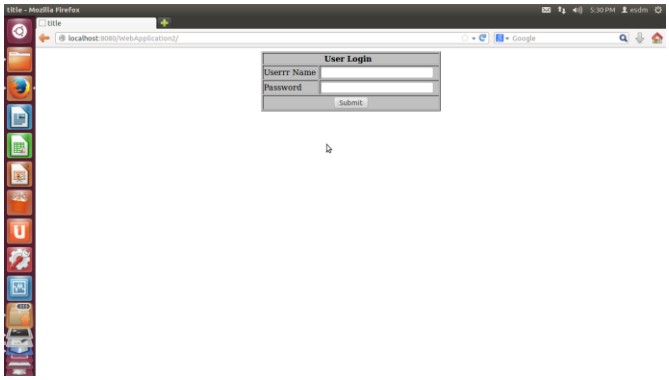
**Flowchart**

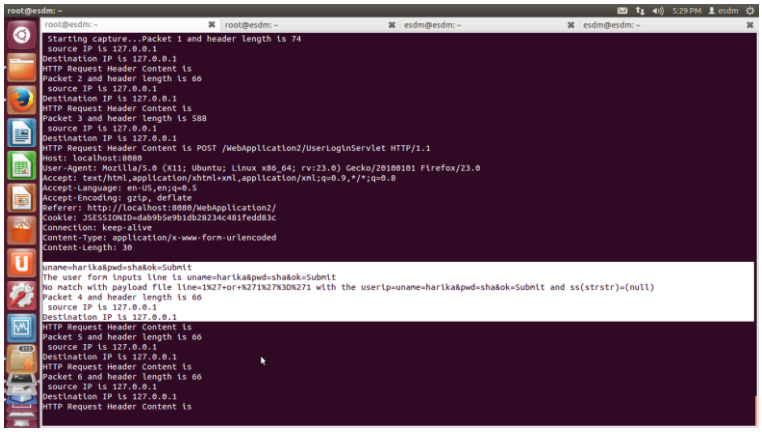



## 5. Result and analysis

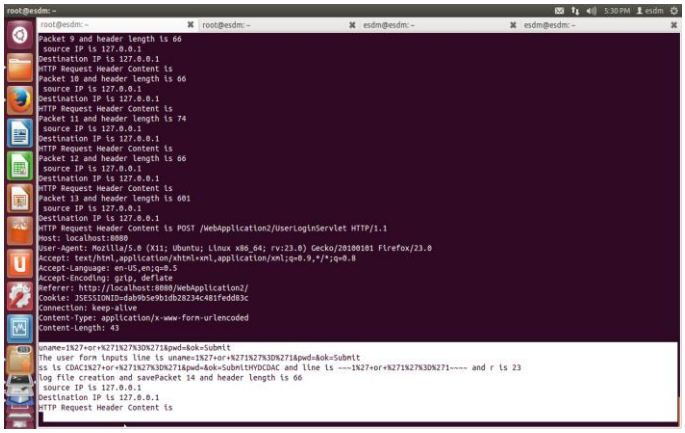
Using a web application on local host.

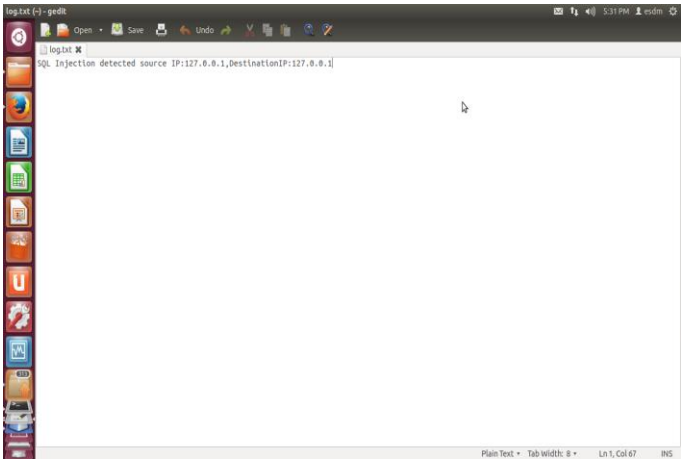
- When the given input doesn`t have any payloads, except the information in the database.



- When payloads are given as input,






## 6. Conclusion

This paper mainly consist of the information which helps to log the source IP and destination IP, if there`re any payloads in the packets that are being transferred over a network. In addition to this blocking of the payloads can be done to avoid exploitation of any data.

There are certain preventive mechanisms to avoid a sql injection:

- Comprehensive data sanitization.
- Use a web application firewall.
- Limit database privileges by context**.**
- Avoid constructing sql queries with user input**.**

## References

[1] SQL Injection Attacks: "Techniques and Protection Mechanisms- Nikita Patel , Fahim Mohammed Santosh Soni" International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Jan 2011.

[2] Detection and prevention of sql injection attacks using novel method in web applications Tejinderdeep Singh Kalsi, Navjot Kaur. - International Journal of Advanced Engineering Technology, Int J Adv Engg Tech/Vol. VI/Issue IV/Oct.-Dec.,2015/11-15.

[3] Advanced SQL Injection In SQL Server Applications Chris Anley- An NGSSoftware Insight Security Research (NISR) Publication.

[4] Sql injection attacks and prevention techniques- Sampada Gadgil,Sanoop Pillai,Sushant Pujari, International Journal on Recent and Innovation Trends in Computing and Communication- Vol-1 / Issue-4.

[5] Effective sql injection attack reconstruction using network recording by Allen Pomeroy, Athabasca university- June, 2010