Sqli and Indian Websites:Unmasking the Truth

Leo Joy
Department of Computer Science
Santhigiri College of Computer Sciences,Vazhithala
Thodupuzha, Kerala, India

Bijimol T.K
Department of Computer Science
Santhigiri College of Computer Sciences,Vazhithala
Thodupuzha, Kerala, India

***Abstract*—Cyber Security one of the most discussed topics in this modern age and therefore researches and studies in this area is important and relevant. Cyber Security is defined as the security offered through services which are taken and given through internet to protect your information/data given in internet. Most of the people believe that their data are safe and secure. They don't have to worry. But the fact is everyone is vulnerable and everything is vulnerable in cyberspace. There are mainly three types of hackers. Ethical hacker (White hat hacker), black hat hacker and grey hat hacker. Ethical hacker is a legal hacker who has great ethics and moral value along with the governmental or other authoritative powers. They are permitted to hack to find the vulnerabilities of the system. But both black and grey hat hackers work on their will and they hack systems on their will and harms the victims. This work conducted a survey on a group of Indian hackers and identified that the main vulnerability seen in the Indian websites is SQL injection. This work also discusses the types of hackers and vulnerabilities seen in the websites including SQLI (Structured Query Language Injection).**

Keywords—Ethical hacking, Vulnerability, SQL injection, Types of SQL injection

I. INTRODUCTION

Cyber security in its true sense is defined as the security offered through online-services to protect your online information. Now a days attacks and crimes in the cyber space had been increased inconsistently and shockingly. As the beneficiaries of the services of internet, we have to deal or have to understand, how these cyber-attacks and online frauding and all other crimes affect us and others. This is the main factor that this work takes critical analysis on types of vulnerabilities most probably seeing in Indian websites. The brief of the reports on Indian cyber security is being revealed through this paper along with the possible solutions and counter measures that could protect Indian cyber space from the attacks of the black hands of the black hats or the unethical hackers. Along with concentrating on securing websites this work also revealing study reports on possibilities of android hacking and the importance of knowing about it.

II. HANDS ON CYBER SECURITY

A. *Defining Cyber Security*

Cyber Security means "the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide"[7]. Now it had become the need of the hour and the call of the day speak about the need of proper awareness on Cyber Security. As we all are living in a computer era, all of us should be aware of the darker sides or the consequences of over trusting these manmade illogical electronic devices. On speaking about it, mentioning the types of fraud stings that are being happened in the cyber space are also needed. The main among them are identity theft and related crimes.

B. *Hacking-A New Glimpse Of Light*

Hacking in general is "the unauthorized intervention of someone into the privacy of another." Hacking is misunderstood as a serious crime by so many common men. But the fact is that it is the most useful method to secure the identity, security and all other factors of a citizen of a country. As there are two sides for a coin, there are two sides of hacking. The three sides in where the goodness and devilishness and the combination of both remains in a twine line. They are:

1. Ethical Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

III. TYPES OF HACKERS

There are three types of hackers in general (more subdivisions are also there). They are being listed out along with a small description.

A. *Ethical Hackers (White Hat Hackers)*

Ethical hackers (White hat hackers) are hackers who work with the intentions of securing the systems by finding loopholes which can be used by an unethical hacker (Black hat hackers). They are either certified from cyber security trainers or either assigned by the company or hacks after seeking permission of the company or the site owner. There won't be any illegal activities from their side and also they use their skills for social service more than making money.

B. *Unethical Hackers (Black Hat Hackers)*

Unethical hackers (Black hat hackers) are hackers who don't have any ethics and makes harms to the system or systems of the victims. They purely work with the intention of making money for their personal needs in an illegal way. They will be difficult to be traced and they are much brilliant and talented that even their closest ones will not know that they are black hats.

C. *Grey Hat Hackers*

These are a type of hackers who belongs to both ethical and unethical hackers. It means, on the same time they are working for a noble cause but through illegal ways. They use illegal ways to solve offences and also they will be using the same methods of black hats.

IV. CONSTRUCTOR BOOMERANG

SQL is the language that is specially designed and used for dealing with databases. The database could be constructed, manipulated, controlled and other operations could only be done with the help of SQL. A constructor always constructs a value. Just like that SQL also constructs some certain

operations. But here the constructor could be a destructor. It could destruct the reliability, the privacy and also even the website itself in the case of websites. As the study progresses one of the most basic methods of website hacking, SQLI will be the area that we deal. Its relevance is that no one had noticed or given much importance to this type of vulnerability and hadn't got enough studies on the possibility of SQLI in Indian websites. An illustration on the process of SQLI is shown in figure 1[6].

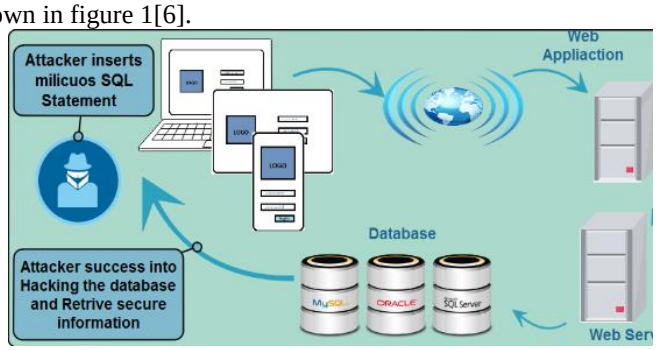


Figure. 1: Process of SQLI [1]

The process of SQLI progresses is that the attacker (hacker) injects certain malicious codes into the web application through an injection point and then the webserver will connect it to the database and if the site is vulnerable, then the system will return a positive response to the attacker and also the full database.

V. TYPES OF SQL INJECTION

There are mainly six types of SQL injections to get database from a SQL vulnerable website. All the types of SQL injections with codes are added below.

1. Tautology based attacks

They work by injecting code by giving one or more conditional SQL statements so as to evaluate the SQL command as a true condition. This is the most common technique in SQL injection to bypass the user authentication on websites. A sample code is given below[1] :

```
Select * from employees where
employee_ID='1'or '1=1'--'AND
employee_password='1234';
```

2. Piggy – backed query attacks

In this type of attack, the attacker compromises the database using a query delimiter, to inject additional queries to the original query. The key seriousness of this attack is that, the attacker could inject any query to the database and could modify the database. An example of the query is given below[1]:

```
SELECT pass FROM userTable WHERE
user_Id='user1' AND Password = 0; drop
userTable
```

3. Logically Incorrect method

In this type of attack, the attacker injects certain incorrect queries to the database and checks the error message given by the database. These error messages could reveal the safety of the website. And also it allows the attacker to find the vulnerable point in the website and also in the database schema. An example for the query is given below[4]:

```
SELECT * FROM userTable WHERE
user Id='1111' AND password='1234'
AND CONVERT (char, no)
```

4. Union Query attacks

This attack is also known as statement injection attack. In this type of attack, the attacker injects additional statements to the original SQL statements. The attack can be done by inserting a UNION query to the vulnerable point. The example code for this attack is given below[4]:

```
SELECT * FROM userTable WHERE
user_Id='1111' UNION SELECT * FROM
memberTable WHERE member_Id='admin' –'
AND password='1234';
```

5. Stored procedure attacks

In this type of attack, the attacker uses the stored procedures inside the system. Stored procedures can be directly run by the system. Stored procedures returns true or false values for the authorized and unauthorized clients. An example for the code used for this type of injection is given below[5]:

```
SELECT Username FROM UserTable
WHERE user_name= 'user1' AND pass=' ';
SHUTDOWN;
```

6. Inference attacks

This method is used by an attacker to change the behavior of the database or application. This attack can be classified into two:

A) Blind Injection

This is a serious type of attack which is possible only by the faults of the programmers. This attack is possible only when the programmer forgets to hide an error message which causes the application insecure. The attacker injects several logical statement codes to the database to compromise the data. An example for this type of attack is shown below[1]:

```
SELECT pass FROM userTable WHERE username=
'user' and 1 =0 – AND pass = AND pin= 0
SELECT info FROM userTable WHERE username=
'user' and = 1 – AND pass = AND pass= 0
```

B) Timing attacks

In these types of attacks, the attacker collects information from the database by observing the delay in the database response. These attacks use if conditions to achieve a time delay purpose. The attacker can delay the response by using the keyword WAITFOR by a specified time. An example of the code is given below[1]:

```
declare @ varchar (8000) select @s =
db name () if (ascii (substring (@s, 1, 1)) &
(power (2, 0))) > 0 waitfor delay '0:0:5'
```

7. Alternate Encoding attacks

This type of attack occurs when attacker modify the injection query via using alternate encoding, such as hexadecimal, ASCII, and Unicode. By means of this way, the attacker can escape from developer's filter, which scan input

queries for special known "bad character". When this type of attack combines with other attack techniques it could be strong, because it can target different layers in the application. An example for the code is given below[4]:

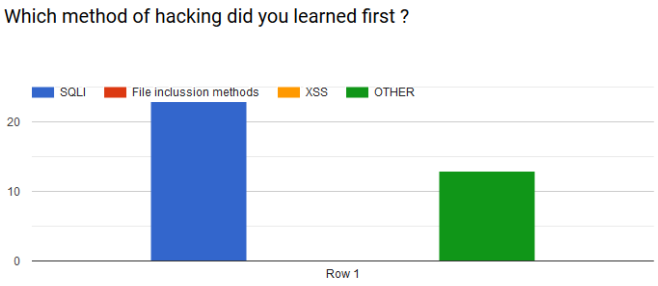
```
SELECT accounts FROM userTable WHERE
login='' AND pin=0; exec
(char(0x73687574646f776e))
```

There are so many new types of SQL injections possible now and the work doesn't deal with them. All the SQL injections are for one result, for exploiting the database.

VI. RESULTS AND DISCUSSIONS

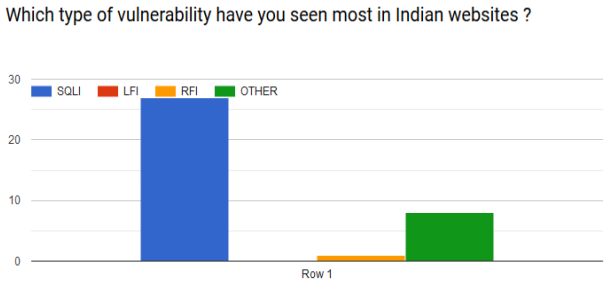
In order to know the most common vulnerabilities found in the Indian websites, we conducted a survey among a group of hackers and found out that SQL injection is the most common vulnerability found in the Indian websites and also almost all the hackers start their hacking carrier by learning SQL injection, which shows that it is the most basic and simplest way of website hacking.

For collecting samples, a questionnaire of about 10 questions were prepared and distributed among a hacker community containing around 100 hackers. The survey lasted for two days and 55 responses were recorded. Among that, 20 were rejected due to partial filling and the remaining 35 responses were counted and remaining 35 responses were considered for study.



Graph 1: Methods of hacking

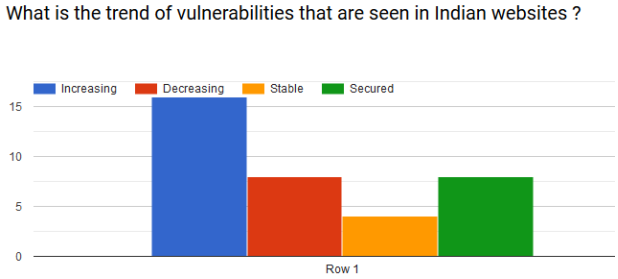
This graph shows that almost 64% of the hackers learn SQL injection during the starting period of their hacking carrier itself and only 26% of hackers leave SQL injection behind.



Graph 2: Types of Vlnerability

This graph shows that, the most common vulnerability found in Indian websites are SQL injections. 75% of hackers states that the most common vulnerability seen in the Indian websites are SQL injection and 3% hackersb says that RFI is the most common vulnerability in Indian websites and 22% hackers says that other types of attacks are common in Indian websites.

In order to know the present condition of the Indian websites, we also asked a question on the trend of vulnerability found in Indian website. The graph of the result is given below.



Graph 3: Trends of Vulnerabilities

The graph says that the trend of vulnerabilities seen in Indian websites are increasing. From the graph, 44% of hackers says that the trend of vulnerabilities in Indian websites are increasing and 22% of hackers says that the trend of vulnerabilities found in Indian websites are decreasing while 11% says that the trend of vulnerabilities in Indian websites are neither increasing nor decreasing and 22% says that the Indian websites are secured.

As per the data collected, the work conducted a survey on Indian websites and the results are shown in the table below:

Table 1: Vulnerability Status on Indian Websites

Vulnerability Check Results			
Method used	***Number of Websites checked***	***Number of vulnerable websites***	***Number of non-vulnerable websites***
SQLI (AUTOMATED)	50	45	5

[a.] Analysis of websites

This work took 50 random Indian vulnerable websites with common vulnerability dork '**php?id=**' and found that 45 websites, which means around 90% of the Indian websites with this common dork in its URL is vulnerable for SQL injection. Among those, 30 websites doesn't have login page and 5 have IP restriction security and 10 grants access to the normal hackers.

VII. CONCLUSION

The possibility of a cyber war is not a myth now because all the transactions and identity verifications are being done online. So many website owners are not aware of this. They are thinking that what happens if the data leaks. But the fact is that, their existence remains in the security of the data of the client. If the site owner cannot even secure the data of the client, how could he trust the credibility of that country?

And also the foreign hackers are invading into our websites daily and approximately, 100 websites are being hacked by the foreign hackers per day. This is not being noted because of the appropriate intervention of hackers communities like KCW, KCP, MCS, KCD and all. They are monitoring the foreign hackers and also our websites for keeping the data of the citizens of our country safe and secure.

Most of the students are also not even aware of the basics of SQLI even though they are learning to write SQL queries and also.

ACKNOWLEDGEMENT

As the work had come to an end, would like to thank all those who have helped me during the study period, especially my master Suji master (Master Trainer and practitioner, ISMA KALARI MUTTOM), Principal Fr. Dr. Boby Antony CMI, Mrs. Dhanya Job, Mr.Sebastian Cyriac , Mrs. Resmi K R,(Principal, HOD, Asst. Professors, Santhigiri College of Computer Sciences, Vazhithala, Idukki, Kerala), Mr. Anil Mathew and all other MCA students of Santhigiri College of Computer Sciences, Vazhithala, Idukki, Kerala and all those who supported and guided me.

REFERENCES

[1] A. Alazab , A. Khresiat , " New Strategy for Mitigating of SQL Injection Attack", International Journal of Computer Applications(IJCA),Volume 154,paper No.11, November 2016
[2] Jai Puneet Singh, "Analysis of SQL Injection Detection Techniques", Theoretical and Applied Informatics(TAAI), Volume.28,Number.1-2, pages 37--55 2016
[3] R.Elmasri, S.B. Navathe, "FUNDAMENTALS OF Database Systems", sixth edition, Addison-Wesley, United States of America,2011.
[4] V. Nithya,,R.Regan, J.vijayaraghavan, "A Survey on SQL Injection attacks, their Detection and Prevention Techniques", International Journal Of Engineering And Computer Science(IJECS), Volume 2 Issue 4 Page No. 886-905, April, 2013
[5] S. Som, S. Sinha, R.Kataria, "STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND PREVENTION", International Journal of Engineering Applied Sciences and Technology(IJEAST), Vol. 1, Issue 8, ISSN No. 2455-2143, 2016,
[6] https://www.ijcsmc.com/docs/papers/August2017/V6I8201701.pdf
[7] https://en.wikipedia.org/wiki/Computer_security