Vulnerability Detection For Sql Injection Attacks: An Experimental Survey

Premveer, Ankur Srivastava, Anurag jain
Department of IT, USICT, GGSIPU

Abstract

SQL Injection attacks are a type of attacks in which malicious data is appended in a user data to access, delete or modify user data.SQL Injection attacks are possible because of lack of input validation at server side. SQL Injection attacks are not detectable by Firewall or Intrusion detection system(IDS) because SQL Injection attacks are performed by Ports which are open in Firewall and IDS work on network and IP layers while SQL Injection attacks work on application layer. This paper focuses on detecting vulnerabilities for sql injection attacks on different types of domains , for which different tools have been selected which are available in market.

Keyword

SQL Injection Attacks, Detection, Evaluation

1. Introduction

SQL Injection Attacks are most effective method for stealing the data from backend[1].In this type of attacks hacker attacks the data by appending Sql keywords in user inserted query without enabling the user to come to know that query has been modified.

2. Types of Sql injection attacks

There are several types of attacks. Some of them are discussed in this paper.

2.1 Tautologies

In this type of attacks malicious code is inserted in such a way that query statement is always evaluated to be true.

"Select * from stud where id='111' and pwd='abc' or '1'='1'"

In above query by using '1'='1' result will always be true whether pwd is correct or not.

2.2 Union Query

In this type of query unauthorised query is attached with authorised by using UNION clause.

Select name, address from user where id=1

When attacked by sql injection we will have the following query:

Select name, address from user where id= 1 UNION ALL Select phone_number from biodatatable.

which will join the result of the original query with biodatatable.

2.3 Piggy-backed query

In this type of attack, attacker exploit database by using query delimiter like ";", to append unauthorised query to original query.

Select name from stud where id=1;drop table stud

Because ";" is appended in query so drop table will be executed after authorised query and it will delete the table stud.

2.4 Boolean SQL injection

Boolean SQL injection means that no error messages are sent in the response, but there is a difference between the response sent for a valid query and the response sent for an invalid query.

examples:

www.example.org/display.php?item=1

will sent the info for item 1

www.example.org/display.php?item=1'

will trigger an error, but suppresses it so no information is shown. But it is still possible to send SQL requests to the database and determine what is true and what is false.

2.5 Cross-site Scripting

XSS (Cross-site Scripting) allows an attacker to execute a dynamic script such as *Javascript, VbScript* etc[2]. This allows several different attacks opportunities for attackers, mostly hijacking the current session of the user.

2.6 URL-Based

URL-Based SQL injection is an attack that can be executed directly from the browser's address bar[3], in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.

3. SQL Injection Detection tools

The tools which are used in this research paper are available in market but for this research paper one month trial versions of tool have been used.

3.1 Sqlmap[3]

sqlmap is an open source testing tool which is used for detection and exploitation of SQL injection

flaws and taking over of database servers. It has advanced detection engine, it is suitable for the ultimate penetration testing.

3.2 Netsparker[4]

Netsparker is the web application security scanner. It discover the flaws that could leave user dangerously exposed. Netsparker is a powerful web application security scanner, which can crawl, attack and identify vulnerabilities in all types of web application - whatever platform and technology it's built on. Netsparker can help user identify web application vulnerabilities such as Cross-site Scripting (XSS), and many more with an easy-to-use and intuitive user interface. Netsparker helps web application developers or penetration testers to secure web applications easily and with the minimum of fuss.

3.3 Webcruiser[5]

WebCruiser is a web vulnerability scanner, an effective and powerful web penetration testing tool that helps in auditing website. It has a vulnerability scanner and a series of security tools. It can scan website for web vulnerabilities cross-site scripting, URL sql injectioin etc.

3.4 Havij[6]

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

4. Comparison of tools with respect to vulnerabilities when run on different types domains.

In this research paper, 38 websites, which belong to different domain types (like product based, portal etc) have been checked for vulnerability using above mentioned tools. Result is shown in the table given below:

Table-1 Comparison of tools with respected to vulnerabilities

Sno	Website type	Website domain	Tools and type of attacks detected by tools			
			Netsparker	Sqlmap	Webcruiser	Havij
1.	Product based	Quiltchalet.com	Cross-site scripting, Boolean based sql injection	Boolean based blind	Cross-site scripting	Not able to find attack
2.	Product based	Sigmaspa.com	Cross-site scripting,	Not able to find error	Cross-site scripting	Not able to find attack
3.	Product based	Kbnusa.com	Cross-site scripting, boolean based sql injection	Not able to find error	Cross-site scripting	Not able to find attack
4.	Domain and host based	Emergingdesignnetworks.com	Cross-site scripting	Boolean based and Union injectable	Cross-site scripting	Not able to find attack
5.	Portal	Userngatheartministries.com	Cross-site scripting	Boolean based, union injectable	Cross-site scripting	Not able to find error
6.	Product based	Saleemcarpets.com	Not able to find attack	Union injectable	Cross-site scripting	Not able to find attack
7.	Product based	Webakku.hu	Cross-site scripting	Not able to find any attack	Cookie sql injection	Not able to find attack
8.	Product based	Micatrone.se	Not able to find any attack	Not able to find any attack	Cross-site scripting	Not able to find attack
9.	Portal	Rubenracing.com	Not able to find attack	Not able to fing any attack	Not able to find attack	Not able to find attack
10.	Product based	Witec.de	Not able to find attack	Not able to find attack	Cross-site scripting	Not able to find attack
11.	Publishing	Lcoastpress.com	Cross-site scripting	Not able to find attack	Cross-site scripting	Not able to find attack
12.	Publishing	Travellers-tales.co.uk	Cross-site scripting	Boolean based	Cross-site scripting	Not able to find attack
13.	Product and services	Arrowvalves.co.uk	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack
14.	Product based	Reaplasrack.co.uk	Cross-site scripting	Union query injectable	Url sql injection	Not able to find attack
15.	Education	Woodlandsschool.	Cross-site scripting,	Not able to find	Not able to find	Not able to

		org	Blind sql injection	attack	attack	find attack
16.	Construction	Qwc.org.uk	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack
17.	Business solution	Vx10.co.uk	Cross-site scripting	Not able to find attack	Cross-site scripting	Not able to find attack
18.	Publishing	Readingmatters.co.uk	Cross-site scripting, Boolean sql injection	Not able to find attack	Not able to find attack	Not able to find attack
19.	Automobile	Topgears-cars.co.uk	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack
20.	Social site	Thehopeforamerica.com	Not able to find attack	Boolean based	Cross-site scripting, url sql injection	Not able to find attack
21.	Business solution	Woodfines.co.uk	Cross-site scripting and Boolean sql injection	Boolean based injection	Not able to find attack	Not able to find attack
22.	Food services	Areuserreadytoorder.co.uk	Cross-site scripting	Union injectable	Cross-site scripting	Not able to find attack
23.	portal	Robertsmith.co.uk	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack
24.	publishing	Athenapress.com	Cross-site scripting, Boolean based sql injection	Not able to find attack	Cross-site scripting	Not able to find attack
25.	portal	Abslation.co.uk	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack
26.	portal	Standardbred.org	Cross-site scripting, Boolean based sql injection	Not able to find attack	Cross-site scripting	Not able to find attack
27.	Manufacturing	Tek-tite.com	Cross-site scripting	Boolean based	Not able to find attack	Not able to find attack
28.	Travelling	Thedockyard.co.uk	Cross-site scripting	Appear not to be injectable	Not able to find any attack	Not able to find any attack
29.	Portal	Blackhistorycanada.ca	Cross-site scripting,	Not able to find attack	Not able to find attack	Not able to find attack
30.	Social site	Twitney.co.uk	Cross-site scripting, Boolean based sql injection	Boolean based blind	Not able to find attack	Not able to find attack
31.	Community	Minesandcommunites.org	Cross-site scripting, Boolean based sql injection	Boolean based	Not able to find attack	Not able to find attack
32.	Retail	Coastal-koi.com	Cross-site scripting	Boolean based blind	Not able to find attack	Not able to find attack
33.	Social site	Musicinthearound.co.uk	Cross-site scripting	Not able to find attack	Cookie sql injection	Not able to find attack
34.	Gov.	Nahipa.org	Cross-site scripting	Not able to find attack	Cross-site scripting	Not able to find attack
35.	Social networking	Facebook.com	Cross-site scripting	Not able to find attack	Cookie sql injection	Not able to find attack
36.	Social networking	Twitter.com	Not able to find attack	Not able to find attack	Cookie sql injection	Not able to find attack
37.	E-commerce	Ibibo.com	Not able to find attack	Not able to find attack	Cross-site scripting	Not able to find attack
38.	E-commerce	Flipkart.com	Not able to find attack	Not able to find attack	Not able to find attack	Not able to find attack

5. Evaluation of tools

In above table 38 websites have been checked for vulnerabilities out of these 38 websites, 9 are product based websites,5 are social sites, 6 are portals, 4 are publishing websites, 2 belong to e-commerce and remaining 12 are kept in category of others.

Table-2 Evaluation of tools

Tools	Domains checked for vulnerabilities(no. of websites in each category)					
	Product based	Social sites	Portals	Publishing	E-commerce	Others
Netsparker	9 websites have been checked for vulnerabilities. In all, able to detect cross-site scripting	5 websites have been checked for vulnerabilities . In 3 websites, able to detect cross-site scripting.And in remaining 2 not able to detect any error	6 websites have been checked for vulnerabilities. In 3 websites able to detect cross-site scripting and in remaining not able to detect any error	4 websites have been checked for vulnerabilities. In all able to detect cross-site scripting	2 websites have been checked for vulnerabilities. In both not able to detect any error	12 websites have been checked for vulnerabilities. In 9 websites able to detect cross-site scripting and in remaining not able to detect any error
Webcruiser	9 websites have been checked for vulnerabilities. In 6 websites able to detect cross-site scripting, in one website able to detect url sql injection and in remaining not able to detect any error	5 websites have been checked for vulnerabilities . Only In one website able to detect cross-site scripting and in remaining not able to detect any error	6 websites have been checked for vulnerabilities. In 2 websites able to detect cross-site scripting and in remaining not able to detect any error	4 websites have been checked for vulnerabilities. In 3 websites able to detect cross-site scripting and in remaining able to detect url sql injection	2 websites have been checked for vulnerabilities. In one website able to detect cross-site scripting and in remaining not able to detect any error	12 websites have been checked for vulnerabilities. In 4 websites able to detect cross-site scripting and in remaining not able to detect any error
Sqlmap	9 websites have been checked for vulnerabilities. In one website, able to detect Boolean sql injection, in 2 websites able to detect union and in remaining 7 not able to detect any error	5 websites have been checked for vulnerabilities . In one , able to detect Boolean based and in remaining not able to detect any error	6 websites have been checked for vulnerabilities. In one website , able to detect both Boolean and union and in remaining not able to detect any error	4 websites have been checked for vulnerabilities. In one website, able to detect Boolean based and in remaining not able to detect any error	2 websites have been checked for vulnerabilities. In both not able to detect any error	12 websites have been checked for vulnerabilities. In 5 websites able to detect Boolean, in 2 websites able to detect union sql and in remaining not able to detect any error
Havij	9 websites have been checked for vulnerabilities. In all not able to find any error	5 websites have been checked for vulnerabilities . In all not able to find any error	6 websites have been checked for vulnerabilities. In all not able to find any error	4 websites have been checked for vulnerabilities. In all not able to find any error	2 websites have been checked for vulnerabilities. In all not able to find any error	12 websites have been checked for vulnerabilities. In all not able to find any error

6. Conclusion

Based on the above result , in which four different sql injection detection tools are used, on different Websites belong to different types(like production based, portal, social site etc), to detect vulnerability for sql injection attacks, it is found that Netsparker is able to detect Cross-site scripting and Boolean sql injection. Sqlmap is able to detect Boolean based and Union query. Webcruiser is able to

detect Cross-site scripting and url sql injection. And Havij is not able to detect any discussed attack. And it is also found that websites which belong to product based are more vulnerable to SQL injection attack. So on the basis of above result it can be concluded that no tool is able to detect all vulnerabilities for sql injection attacks.

7. References

[1]Puspendra Kumar."A Survey on SQL Injection Attacks, Detection and Prevention Techniques" ICCCNT 2012.
[2]Atefeh Tajpour and Maslin Masrom. "SQL Injection Detection and Prevention Tools Assessment" IEEE 2010.
[3]Sqlmap.org.
[4]www.mavitunasecurity.com/netsparker
[5]sec4app.com
[6]www.itsecteam.com/products/havij-v116-advanced-sql-injection