Crawl Vulnerabilites For Detecting And Preventing Web Application

Jayanthi V[1], Abirami R[2] and Brindha R[3]

[1, 2, 3] Computer science & Engineering
V.R.S College of Engineering & Technology
Arasur, Villupuram. 605602

ABSTRACT

Today in the field of information technology people can get any information by just single click on web applications. Web application plays very important role. Many organizations are mapping their business from a room to the world with the help of these web apps. Each web apps consist of three tier architecture in which database is third tier. As use of web apps increases day by day many kind of attacks also increases on them. Some attacks are SQL INJECTION, BANNER GRABBING, QUERY STRING & UNION. There have been proposed vulnerability scanners but none of them are able to detect these attacks completely. Apart from that i propose an approach to find possibility of vulnerability on web apps and generate report based on it.

Keywords: *Vulnerability, Crawler,Scanner,Banner grabbing, Injection attacks, Query String, Union attacks*

1. INTRODUCTION

Web application facilitates us by introduced new way where we have the facility to book our bus, railway as well as flight tickets. We can deposit money from home to other account.

We can buy products, submit our bills, recharge our mobiles phones etc, just on a single click [5]. It also saves our time and effort. Each web application consists of three tier architecture where at first tier client submit their request and on second tier application server perform the logic operation according to the request. Last tier is the database work which is use for Storing the records of clients. So Database is most important assets in any web application. But it is also vulnerable for so many attacks. Some of them are SQL INJECTION, UNION, QUERYSTRING & BANNER GRABBING. These four attacks are Most dangerous attack against any web application. There are many techniques available to deal with these attacks. Where various vulnerability scanners are used to detect the attacks but non Provide full coverage. One major issue with vulnerability scanner is their performance impact on the devices they are scanning. On the one hand if we want the scan to be able to be performed in the background without affecting the application. On the other hand we want to be sure that the application scan should be through for which it is create [3].

Server Pages or's) and user supplied inputs become part of the query generation process without proper validation. As a result, the execution of these queries might cause unexpected results such as authentication by passing; Leaking of private information etc [7].The lower figure shows the execution of SQL commands inside the web application. SQL related vulnerabilities rank among the top three vulnerabilities over the past few years. Moreover, successful exploitations of SQLIV have already caused significant financial loss.

An application is said to have vulnerabilities when queries are generated using an implementation language (e.g., Java Therefore, testing an application for SQLIV is important for ensuring software quality. In recent years, a number of techniques have been proposed to address SQLIV other than testing. These include input character filtering or input validation, static analysis [4], runtime monitoring [2] etc. In this paper i am proposing a technique which is effective to detect these Vulnerabilities. If we scan the whole application before being deployed to public by use scanner then we can find vulnerabilities inside it. For that we crawl the whole web application and for each page we generate the attack payload perform the attack simulation and then prevent them to be get executed,analyze the response and create report based on it.

Whole paper is divided into three sections. First section explores the description of some attack for which web application can be vulnerable and show how it affect my application. Second section shows an approach to prevent these attacks and in last section show the result of this approach.

2. DISCRIPTION OF ATTACKS

QUERY STRING ATTACK: - Query string manipulation attack is most common method of attacking a vulnerableweb application. Query string attack access the database of a website through a URL. I am showing this attack by taking an example of web application having information of products and each product contain some id in numeric form.

Original Query
www.site.com/product.php?product-id=10

Injected Query
www.site.com/product.php?product-id=10**; drop table user—**”

Attacker append “drop table users—“sentence with the original query and in the effect user table resides in database will be drop.

UNION ATTACK :- Original query is concatenated to the injected query by using the sql key word “UNION’ togather information related to web apps.In UNION attack an attacker exploits a vulnerable parameter to change the data set returned for a given query from a table. Attacker does this by injecting a statement of the term: UNION SELECT (rest of injected query). Because attacker completely controls the second /injected query to retrieve information of apps.lets take an example of it.

Original Query
SELECT accounts FROM users WHERE login==“xxxx” and password=‘xxxx’

Injected Query
SELECT accounts FROM users WHERE login=”**UNION SELECT card no. from credit cards where acctno.=10032- - AND pass=**”

In this query database would return column ‘cardno’foraccount 10032. By use of this kind of attack we can alsoretrieve password of any admin account’s show the effect of this attack in web app like this inside our database willbe drop. In my application I show the effect of this query like this. Each time when attacker fire this query thenuser table will be drop in the cause of This attack and we will lose all user information. this kind of attack is verydangerous for business which have a large Amount of information related to their customer.

SQL INJECTION: - This kind of vulnerability affects any web application very badly. In this attack, hacker gives theuser name and password in the query string itself instead of the log in page and get enter into system very easily.
Here is the example of this attack:-

Original Query
Select accountno, balance from accounts where loginid=‟abc‟ and pwd=‟xxxxx‟

Injected Query
Select accountno, balance from accounts where loginid=‘**or 1=1;/***‘ and pwd=‘*/--’

One show in red color is the cause of this attack. how this affect application is shown above.
By this attack hacker can now able to enter into system which is illegal. This is all about these four vulnerabilities. Move on to propose work to safe web application from these attacks.

In upper case the hacker will try to first find the user name and then try to get the password of the user in the user detail table by using union query.

BANNER GRABBING: - Successful banner grabbing attack may provide server information leakage via softwarevendor and version. This attack can be used to determine information about services that are being run on a computer. In computer networking term banner typically refers to a message that a service transmits when program connects to it. Default banners often consist of information about a service such as the version number.

let’s take example of this attack:-

Original Query
www.site.com/product.php?productid=10

Injected Query
www.site.com/product.php?productid=10**and substring(@@version);**
Displays Mysql 4 and a blank or error page

Text after 10 is the reason of this attack .this query will extract detail that the database used in sql server. After get database information attacker can revel other authenticate information.

3. PROPOSED WORK

Proposed work to detect this kind of attack contains some steps.

1.Create a web application.
2.Create a java crawler application to check for possible attacks on the web application.
3.Automate the crawling process on the web application.
4.Generate attack on application and take effect as a result.
5.Apply prevention approach on them and finally generate report .

4. IMPLEMENTATION DETAIL

To implement web application I use java web application. Create local host web application with login function. To enter in this submit user name and password which is already created by registered user. New user can also get register.

To implement java crawler to crawl whole web application the basic structure will be represented in the form of treelike below figure.

In this figure a.php is represented as a home page and all child node of a.php are b.php, c.php, and d. php are otherrespective pages of web application.

Scanning will perform in following way-

1. Create fifo queue with two fields URL (primary key), STATUS
2. Analyzing front page and retrieve its target URL and insert its entire URL in fifo queue and set status 0.
3. Update status 1 and analyzing all related url insert them into fifo queued and set status 0.
4. Go to step 3 while status =0 else go to step5 5. Finish

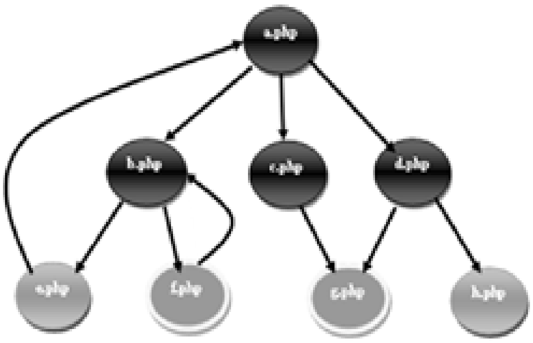

Fig1. Tree Structure of a Web application

5. PREVENTATION APPROACH

In this section I review these four kinds of attacks. For each attack identify a pattern of attack. A pattern or signatureof the attack is a sequence of characters that will always appear in the url for that particular attack type.Basic aim isto extract a signature of this attack and then use these to prevent such attack.
I want to extract bad characters from strings.After analysis these strings i found some signatures related to theseattacks.
Like for union hacking to be execute there should be a Sql Meta character “UNION” using Brute force String Matching algorithm.

```
**Algorithm** *BruteForceStringMatch*($T[0...n-1]$, $P[0...m-1]$)
    **for** $i \leftarrow 0$ **to** $n-m$ **do**
        $j \leftarrow 0$
        **while** $j < m$ **and** $P[j] = T[i+j]$ **do**
            $j$++
        **if** $j = m$ **then return** $i$
    **return** -1
```

Like wise for query string attack to be execute here signature is (“), (;), (-), (--) and meta char “DROP” For Sqlinjection signature is “1” “—“,“-“ using Longest common subsequencealgorithm.Soif we prevent these bad characters or symbols to be execute then we can prevent all these attacks.

$$LCS(X_i, Y_j) = \begin{cases} \emptyset & \text{if } i = 0 \text{ or } j = 0 \\ LCS(X_{i-1}, Y_{j-1}) + 1 & \text{if } x_i = y_j \\ \text{longest}\left(LCS(X_i, Y_{j-1}), LCS(X_{i-1}, Y_j)\right) & \text{if } x_i \neq y_j \end{cases}$$

In this module we list the all bad characters,symbols ,numbers which can be add with query and when we found any of these pattern attach with sql query that means application is in under effect of hacking. Let user getaware of this attack by message and generate a message like “Hacker Identified”.
I want to extract bad characters from strings. After analysis these strings i found some signatures related to these
After prevention we generate report based on number of successful attacks versus failure attacks of each kind.

5.1 FINAL REPORT

Final report shows number of successful failure attempt of these vulnerabilities when they were trying to enter into application.
Successfully prevention of these is possible by catching their pattern of attack.

Name of Attack	Number of Successful attempt	Prevent
Query string	10	Yes
Banner grabbing	1	Yes
Sql injection	1	Yes
Union	20	Yes

6. CONCLUSION

This paper proposes an approach to scan all the pages of web application which are vulnerable to query string kind of attack. This helps to programmer to work and fix only vulnerable pages and focus on only bad pages rather than whole web application. In future we can involve more different attack and prevent them by this method.

REFERENCES

[1]. Yang Haixia nan zhihong ,"A Database Security Testing Scheme Of Web Application" , pp. 953-955, 978-4244-3521.2009 IEEE.

[2]. Neha Singh , Ravendra Kumar Purwar "Sql Injection – A Hazard to Web Application" , pp 36-40 ,june 2012 ijarcsse.

[3]. Dr.RPmahapatra and mrs.Subi khan "Preventing Sql Injection Attacks in Stored Procedure" IJCSE survey vol no.3 june 2012 PP. 55-74

[4]. Kewei, M.muthuprasanna "A Survey of Vulnerability Countermeasures" ,pp 35-39 IJCSSE vol.3 issue3. 2009

[5]. "Sql injection attacks and defnce" don boneh white paper pp 1-22 ,winter 2009

[6]. sangitaroy , avinashkumarsingh and ashoksinghsairamAnalysingsql meta character and preventing sql injection attacks using meta filter IJASCSE vol 1, issue 1 2012 june 30 pp 1-12

[7]. KasraAmirtahmasebi, Seyed Reza A Survey of SQL Injection Defense Mechanisms Jalalinia and SagharKhadem, Chalmers University of Technology, Sweden IJRREST VOL.1 ISSUE 1 JUNE 2012 PP 21-26