WEBSITE HACKING USING GRABBER AND SQLMAP

Roni P James
Department of Computer Applications
AmalJyothi College of Engineering, Kanjirappally , India
ronipjames@mca.ajce.in

Jiss Maria Joseph
Department of Computer Applications
AmalJyothi College of Engineering, Kanjirappally, India
jissmariajoseph@mca.ajce.in

Julie E. S
Department of Computer Applications
AmalJyothi College of Engineering, Kanjirappally, India
juliees@mca.ajce.in

Dr. Juby Mathew
Associate Professor
Department of Computer Applications
AmalJyothi College of Engineering, Kanjirappally, India
jubymathew@amaljyothi.ac.in

I. ABSTRACT

All web applications depend on the internet. Now a day's web applications play an important role in everybody's life. Thousands of transactions and confidential data are done through these applications, 80% out of which are vulnerable to malicious attacks according to the survey by the Open Web Application Security Projects. Website hacking exploits the web pages and database; thus, compromising the confidential and sensitive information in it. The highest security threat for web applications is SQL injections. Here we use two tools for finding the vulnerability in the websites and enables access to the database, viewing data in tables such as users, passwords, backups, phone numbers, credit cards, e-mail addresses, and other confidential and sensitive information. Grabber is a web application scanner which scans for the vulnerability. Sqlmap is a tool that provides penetration testing for the process of detecting and exploiting SQL injection flaws.
Key Words: Website Hacking, Grabber, Sqlmap, SQL Injection

II. INTRODUCTION

Website hacking is used to hack a vulnerable website and enables access to the database and viewing confidential data from the tables such as users, passwords, phone numbers, backups, credit cards, e-mail addresses, and other confidential and sensitive information.

Grabber is a web application scanner which can perform scans and tells where the vulnerability exists and Sqlmap is a tool that penetrates, detects and exploits SQL injection flaws providing its user interface in the terminal. In addition to mapping and detecting vulnerabilities, the software enables access to the database, viewing data in tables such as users, passwords, phone numbers, e-mail addresses, credit cards, backups and other confidential and sensitive information.

PENETRATION TESTING

Penetration testing which is also called pen testing is referred to the process of testing a computer system, network or Web application to find

vulnerabilities that an attacker could exploit and make use of it. Pen tests can be performed manually or it can be done automatically through software applications. The objective of Penetration Testing is to determine Security Weaknesses.

Benefits of Penetration Testing

- Intelligently manage vulnerabilities.
- Avoid the cost of network downtime.
- Meet regulatory requirements and avoid fines.
- Preserve corporate image and customer loyalty.

III. LITERATURE REVIEW

[1] Chandershekhar Sharma, Dr. S.C. Jain mentioned Web application has many interlinked components and each component plays an important role in proper working of the web application. Browser sends the request to the web server and returns the desired result. The communication between web server and database is done with the help of SQL commands. With the help of special crafted SQL commands attacker can access the user information. SQL injection is an attack on web-applications which have vulnerabilities. Actually, these vulnerabilities are the weakness in the design of web application due to logic, syntax or semantics. The attackers can add a crafted query in the form of SQL command which is executed by web application and exposed the back-end database. The attacks occur through user inputs without proper validation.SQL injection is a technique for inserting a spiteful code in user code. Results in leak of confidential information, table structure, adding or modifying data, bypass authentication, performing denial of service, network hacking and even corrupting or deleting the database.

[2] Mr. K.Naveen Durai1 , K. Priyadharsini focused on A Survey on Security Properties and Web Application Scanner. Web Application vulnerability scanning or web application security scanning, drag a website for vulnerabilities within web applications. Web application enables the dynamic information and service delivery. Web application is a gateway of database that holds a critical vulnerability application and asserts. Most web application store the information in databases or in file system bases. The main objective is to find out how effective the tool is in detecting the vulnerabilities of the web application and produce a better result/report effectively. A web application scanner must have identified vulnerabilities in web applications and generate reports/results for vulnerability.

[3] José Fonseca, Marco Vieira, Henrique Madeira proposed a Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. An approach to evaluate and compare web application vulnerability scanners. It is based on the injection of realistic software faults in web applications in order to compare the efficiency of the different tools in the detection of the possible vulnerabilities caused by the injected bugs. The results of the evaluation of three leading web application vulnerability scanners show that different scanners produce quite different results and that all of them leave a considerable percentage of vulnerabilities undetected. The percentage of false positives is very high, ranging from 20% to 77% in the experiments performed. The results obtained also show that the proposed approach allows easy comparison of coverage and false positives of the web vulnerability scanners. In addition to the evaluation and comparison of vulnerability scanners, the proposed approach also can be used to improve the quality of vulnerability scanners, as it easily shows their limitations. For some critical web applications several scanners should be used and a hand scan should not be discarded from the process. For future work we intend to apply this benchmark procedure to other

web applications to better understand the relationship between software faults and vulnerabilities. Knowing what kind of programming mistakes usually lead to security vulnerabilities can be an important tool to help in the detection and prevention of a security flaw. We also want to evaluate different configurations of the same scanner and study the association of scanners to cover a wider range of XSS and SQL Injection vulnerabilities.

[4] Teddy Surya Gunawan, Muhammad Kasim Lim, Mira Kartiwi, Noreha and Abdul Malik, Nanang Ismail in their paper discusses on the Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpres, and WPA2 Attacks. The process of penetration testing starts from identify the system's vulnerabilities, stage an exploitation, vulnerabilities' discovery and reporting,and dissolving the vulnerabilities that can cause harm to the system. According to the process of penetration testing could illustrate the level of severity could be done on the system during the real-life attack thus help the organization to prevent it before it is too late. Moreover, Open Web Application Security Project (OWASP) stated that there are top 10 vulnerabilities which can cause severe impact to web application [1], such as SQL injection (SQLi), cross site scripting (XSS), local file inclusion (LFI), and remote file inclusion (RFI). SQL injection is one of the most serious threat to the Web application, in which an attacker could gain access to restricted database that contain sensitive information

[5] Olivier Bizimana & Taha Belkhouja had done SQL injections and mitigations Scanning and Exploitation using SQLmap. SQL Injection is a web attack mechanism in which a malicious SQL statementis"injected" via the input data field from the client to the data driven web application. It is one of the most common application layer attack techniques employed by attackers today. SQLmap is an open source penetration testing tool developed for finding and exploiting SQLi vulnerabilities. It comes with a collection of features that helps the user specify the intensity of attack and the level of risk they are willing to go through. sqlmap injecting through the parameter by finding works for finding the vulnerable GET request parameter. As of now, they support common databases such as MySQL, PostgreSQL, Oracle, Microsoft SQL Server, IBM DB2, Microsoft Access, SQLite, Sybase, SAP MaxDB, Firebird and HSQLDB.

[6] Angelo Ciampa, Corrado Aaro Visaggio, Massimiliao Di Penta discusses on A heuristic-based approach for detecting SQL-injection vulnerabilities in Web applications. Injection consists in the possibility the user has to inject fragments of SQL queries in Web application input fields. If these fields or the resulting SQL query to be sent to the database are not properly validated, then it might be possible for the attacker to access unauthorized data, reverse engineer the database structure, or even to insert/delete data.

IV. SQL INJECTION

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. SQL Injection Based on 1=1 is Always True. The original purpose of the code was to create an SQL statement to select a user, with a given user id. If there is nothing to prevent a user from entering

"wrong" input, the user can enter some "smart" input like this: 105 OR 1=1.

Then, the SQL statement will look like this:

SELECT * FROM Users WHERE UserId = 105 OR 1=1;

The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.

V. WEB APPLICATION SCANNER

Web application scanning, also referred to as web application vulnerability scanning or web application security scanning, drag a website for vulnerabilities within web applications. After analyzing all the detectable web pages and files, the scanner builds a software structure of the entire website. The web application scanner does not have access to the source code; instead of analyzing the code, vulnerability scanners perform simulated attacks against an application and analyze the results.

A. GRABBER

Grabber is a web application scanner. It detects some kind of vulnerabilities on the website. Grabber is simple, not fast, but portable and adaptable. This software is designed to scan small websites such as personals, forums etc, absolutely not big application it would take a too long time and flood your network.

FEATURES

- Support Cross-Site Scripting
- Full support for SQL Injection File Inclusion
- Backup files check
- Simple AJAX check
- Hybrid analysis/Crystal ball testing for PHP application using PHP-SAT
- JavaScript source code analyzer: Evaluation of the quality/correctness of the JavaScript with JavaScript Lint
- Generation of a file [session_id, time(t)] for next stats analysis.

Step 1: Scanning Website to find the Vulnerability.

Spider the web application to a depth of 1 (–spider 1) and attempt SQL (–sql) and XSS (–xss) attacks at the given URL(–url https://www.webscantest.com):

Step 2: Now collect the list of vulnerable URLs those id is been passed.

VI. VULNERABILITY ATTACKER

vulnerability is a weakness which can be exploited. The vulnerable list of URLs of the website we have found can be exploited using a tool or technique.

B. SQLMAP

Sqlmap is a penetration testing tool that automates the process of detecting and exploiting SQL injection flaws providing its user interface in the terminal. In addition to mapping and detecting vulnerabilities, the software enables access to the

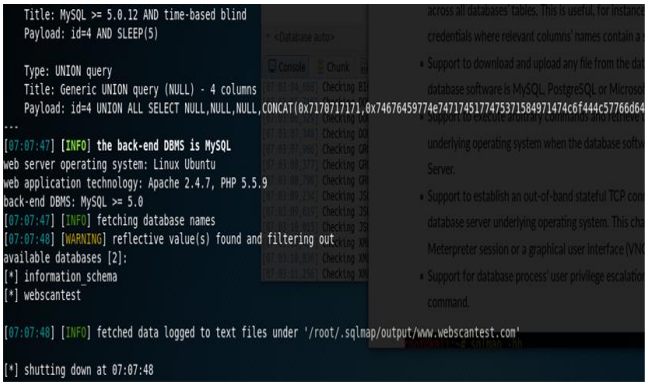
database, viewing data in tables such as users, passwords, backups, phone numbers, e-mail addresses, credit cards, and other confidential and sensitive information.

FEATURES

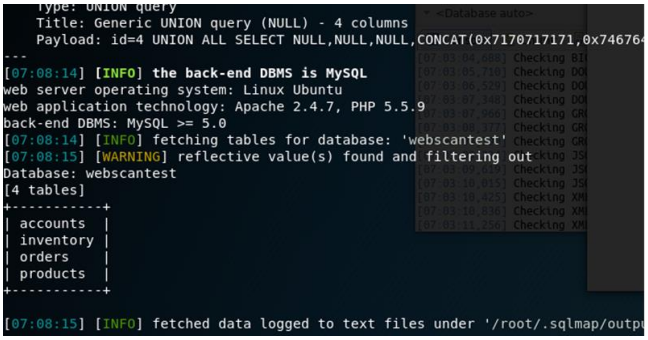
- Full support for database management systems.
- Support of SQL injection techniques.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, port, IP address, and database name.
- Support to enumerate users, password hashes, roles, privileges, tables, databases, and columns.
- Automatic recognition of password hash formats and support for splitting them using a dictionary-based attack.
- Ability to inject backdoors.

VII. IMPLEMENTATION

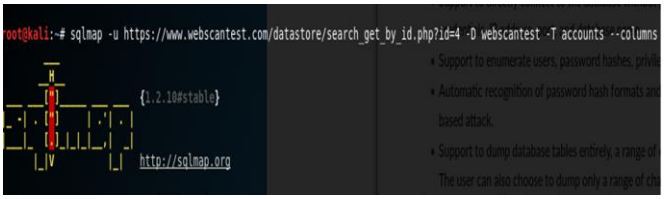
Step 1: List information about the existing databases.

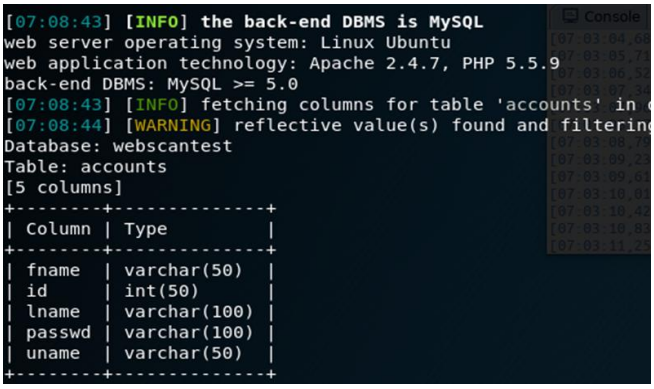


Step 2: List information about Tables present in a particular Database

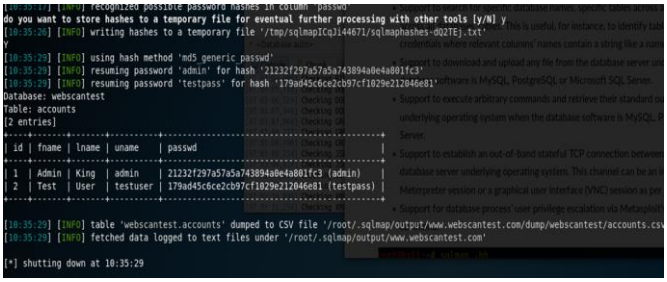


Step 3: List information about the columns of a particular table





Step 4: Dump the data from the columns



VIII. RESULT

Information Gathering of the website from database using Grabber and Sqlmap and viewing confidential data from the tables such as users, passwords, phone numbers, backups, credit cards, e-mail addresses, and other confidential and sensitive information.

IX. CONCLUSION

In this paper we propose an approach to evaluate and compare web application vulnerability by using grabber and sqlmap. Grabber is a web application scanner. Basically, it finds some kind of vulnerabilities in your website. SQLMap is a good tool when it comes to detecting and exploiting SQL injection vulnerabilities. With so many supported options, switches and ability to create and use the customize script, it stands out from the many open-source tools for testing SQL injection vulnerability.

X. REFERENCES

[1] Chandershekhar Sharma, Dr. S.C. Jain: SQL Injection Attacks on Web Applications

[2] Mr. K.Naveen Durai1, K. Priyadharsini : A Survey on Security Properties and Web Application Scanner

[3] José Fonseca,Marco Vieira, Henrique Madeira: Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks

[4] Teddy Surya Gunawan, Muhammad Kasim Lim, Mira Kartiwi, Noreha Abdul Malik, Nanang Ismail: Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpres, and WPA2 Attacks

[5] Olivier Bizimana & Taha Belkhouja: SQL injections and mitigations Scanning and Exploitation using SQLmap

[6] Angelo Ciampa, Corrado Aaron Visaggio, Massimiliano Di Penta: A heuristic-based approach for detecting SQL-injection vulnerabilities in Web applications