International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5935-5942

Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages

Adamu Bin Ibrahim[1] and Shri Kant[2]

[1]*Department of Computer Science & Engineering, School of Engineering and Technology, Sharda University, Greater Noida, 201303, India.*

[2]*Researches and Technology Development Centre, School of Engineering and Technology, Sharda University, Greater Noida, 201303, India.*

Abstract

A penetration testing using Structural Query Language (SQL) injection to recognize the vulnerable point on web pages may result from weak passwords, software bugs, computer virus, script code injection malware and SQL vulnerability. The main objective of this research work is to demonstrate a penetration testing that can automatically and manually discovers the weaknesses that are occurring on web pages by using Network Mapper (Nmap) for identifying both active and inactive ports, Acunetix Web Vulnerability Scanner (Acunetix WVS) as a scanning tool for vulnerability scanning and SQL injection techniques for exploitation. It evaluates the security posture of web pages on a network; and also provides the all-round investigation for finding the vulnerability and security threats in different web pages on a network. This paper explains the complete penetration testing methodology and the prevalent tools and techniques for setting target, information gathering, scanning, SQL injection and report generation.

Keywords Acunetix Web Vulnerability Scanner, Information Gathering, Penetration Testing, SQL Injection and Web Pages

NTRODUCTION

Web pages vulnerabilities have been exploited since early `90s against user oriented applications such as email, online shopping, and Web banking [1]. Penetration testing is a technique for finding vulnerability or loop holes that exist in web pages which can help for ruling out illegal access to the database [2]. A penetration testing for web pages vulnerabilities continues to be a significant problem, as more and more user-oriented applications are deployed to the web such as Facebook and Twitter [3]. A web pages is a process of collection a dynamic scripts, compiled code or both, that resides on a web or application server and potentially interacting with database and other sources of dynamic content [4]. Web pages are becoming important part of our daily activities. As an important role of web application, the web security is becoming critical. Because of the wide use of web applications, all web vulnerability is observed and exploited by hackers, and through which it can be easily access the database [2]. Many web pages security vulnerabilities result from generic input validation problems. Examples of such vulnerabilities are SQL injection, cross-site scripting (XSS) or weak password [3], [5]. Although the majority of web vulnerabilities are easy to understand and avoid, many web and database developers are unfortunately not having security awareness, as a result there exist a large number of vulnerable database pages on a web [3].

There are three approaches to make penetration testing on web pages; namely white box or white heart attack, black box or black heart attack and gray box or gray heart attack. In white box testing or white heart attack, the source code of the web pages is analyzed in an attempt to crack down defective or vulnerable lines of code, is often done with authorization. In black-box testing or black heart attack, the source code of web pages is examined indirectly and malicious code are generated and sent to the web pages. Then, the results by the web pages are analyzed for the unexpected behavior that indicates error or vulnerabilities. In gray-box testing or gray heart attack this is a combination of black-box (black heart attack) and white-box (white heart attack) [5]. In this research work, black-box testing (heart attack) vulnerabilities scanners are used to discover security weakness in web pages. These tools operate by launching attacks against web application and observing its response to these attacks [2], [6].

The fundamental reason for performing penetration testing on web pages is to check out vulnerability before an attacker does and fix them on time. Attackers are using many tools and techniques to perform different types of network attacks for entering into the web pages. The penetration testing helps the management to get the security view of their web pages from attacker point of view.

The penetration tester aims at finding the ways into the web pages vulnerabilities and to fix them before some hacker finds and uses the same loop holes. Sometimes though the administrator and the users of the network are aware of the vulnerabilities, but they need a penetration tester report. With its help, they justify to the management to sanction the budget for fixing the vulnerabilities.

Penetration testing can be used to check the secure configuration of our networks. The report of the penetration test helps in verifying that the security team of our organization is doing a good job or not. This test does not increase the security of web pages or network but it finds the gaps between desired and actual implementation. It helps the organizations to meet the government legal requirements for doing the business. Finally, penetration testing is used for testing new technology. The new technology should be tested before production and

the process of performing a penetration test on new technologies is easy and cheap because no user is relying on it. When it goes to the hand of users, it becomes the costly affair [7-9].

The main aim of the present work is to demonstrate a penetration testing methodology which can detect unusual behavior from a source outside or inside the web application in an organization. To help organization in identifying the methodologies and steps that they need to undertake to build and operate the penetration testing on their web pages which is contaminated with SQL vulnerability. This guide can be used as a reference and also in determining the gaps between their current scanning, exploiting of existing vulnerability and industry best practices by using Nmap, Acunetix WVS and SQL injection attack.

The rest of the paper is organized as follows Section 2 deals with the previous related work done and the research gap. Section 3 discuses: The methodology of Penetration testing using SQL injection to recognize the vulnerable point on web pages. The experimental set up and result are demonstrated in section 4. Finally section 5 divulges conclusion and future work.

PREVIOUS RELATED WORKS AND TECHNOLOGICAL GAP

The concept of penetrating testing has been described by many authors, based on different perspective. In fact Almubairik and Wills [7], explain the process of penetration testing as threat model driven approach for automated penetration testing. Liu et al. [6], discuss the methodology of penetration testing with the help of SQL Injection Vulnerability (SQLIV) penetration test approach based on Finite System Model (FSM). Reddy and Yalla [8], discusses the latest trends in mathematical analysis of penetration testing and vulnerability countermeasures. This explains a penetration test as a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities including OS improper configurations, service and application flows and even risky end-user behaviour. Singh, et al [2], describes the penetration testing through analyzing the security of the network by hacker's mind and complete life cycle of vulnerability assessment and penetration testing on systems or networks. Jiajia [9], introduces penetration test based on mobile Internet, putting forward a kind of penetration test method based on mobile Internet. The study builds a test platform with the actual network and then designs an execution plan of penetration test program through the vulnerabilities of mobile Internet. Goel and Mehtre [4], explained the vulnerability assessment and penetration testing as a cyber defence technology. In their work they explained how vulnerability assessment and penetration testing can be used as an effective cyber defence technology. Salas and Martins [5], analyzed the robustness of web services by fault injection with WSInject, which allows emulation and generation of attacks. However, the process is delayed and often not automated. In their researched, they emulated the Cross-site Scripting (XSS) attack. Mirjalili, et al [10] analyse a survey on web penetration testing describing four phases: reconnaissance, scanning, exploitation and maintaining access. But no experimental study. Yaqoob [12] present the penetration testing and vulnerability assessment by using CIA techniques. CIA is abbreviated Confidentiality, Integrity and Availability. All three goals refer your data to keep secure and not to go in wrong hands. Confidentiality refers to the concept of keeping data out of reach of unauthorized persons, integrity refers the data must not be alters in case on unauthorized access and availability refers to the concept of high availability i.e. data is available to all the users when needed. So in vulnerability assessment they find week point of the system and in penetration testing they proposed how to keep the system secure from hackers and prohibit possible attacks. Scandariato, et al [15] presented static analysis versus penetration testing in a controlled experiment. They analyzed the differences between performing a white box security analysis (static analysis supported by a scanning tool) and a black box security analysis.

In all the above studies mentioned, none have clearly demonstrated the step-by-step procedure for conducting penetration testing against web pages, particularly using both automatic and manual techniques. The main contribution of this paper is to demonstrate how easy it is to discover and exploit level of vulnerabilities in web pages with the help of Acunetix scanner for vulnerability assessment, network mapper for port assessments, different types of SQL injection techniques (in experimental form). Hence the current work intends to fill this gap.

PRESENT METHODOLOGY ADOPTED

The methodology adopted in carrying out this work involves a mixture of experimental and descriptive researches. It is experimental on one hand, in the sense that, every stage of the demonstration is being practicalized to portray the expected results, and described, hence descriptive research as well.

The present work, thus, demonstrate the different types of SQL injection vulnerability present in web application by using: Acunetix WVS as a scanning tools for identifying different types of SQL vulnerability, Nmap as a port scanner that can identify both open and close port (live and unlived network). The research further introduces the concept of SQL injection attack on web pages such as: blind SQL injection, Havij SQL injection, Normal SQL injection (manual method), and SQL map.

Detecting vulnerabilities is widely not an easy task, and not all of the common vulnerabilities can be successfully detected by automated scanners [10], [11]. The method to be followed here involves setting a target, gathering information about that target, making series of scanning by the use of Acunetix web vulnerability scanner to detect the types of the vulnerabilities. After detecting the vulnerabilities then, SQL injection technique will be used to exploit the target and also generate useful report [10]. These steps are presented in figure 1 as a flow chart.

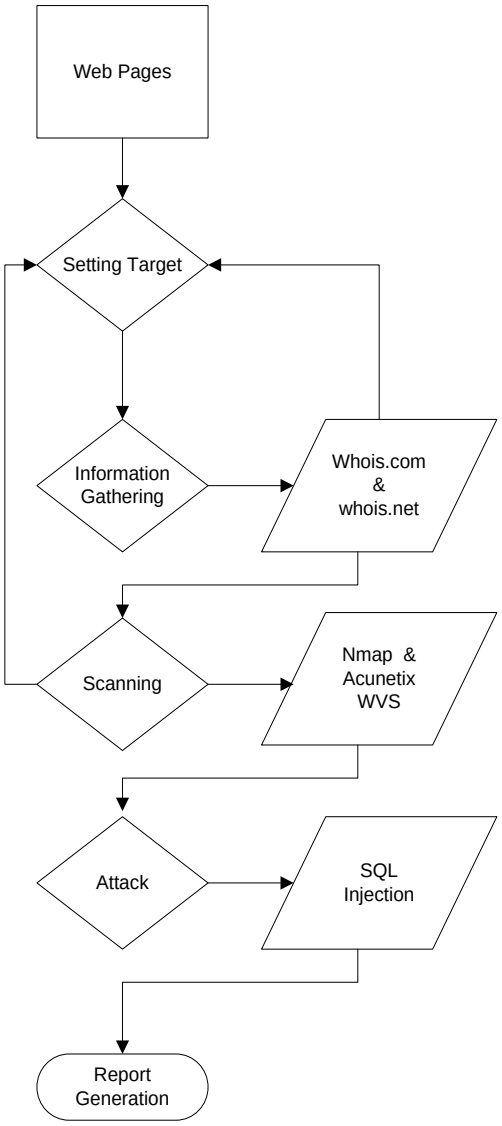


Figure 1: Steps to use penetration testing on web pages using SQL Injection

EXPERIMENTAL SETUP

To evaluate the experimental prototype of this work, this paper involves a mixture of experimental and descriptive techniques. It is experimental on one hand, in the sense that, every stage of the demonstration is being practicalized to portray the expected results, and described, hence descriptive research as well.

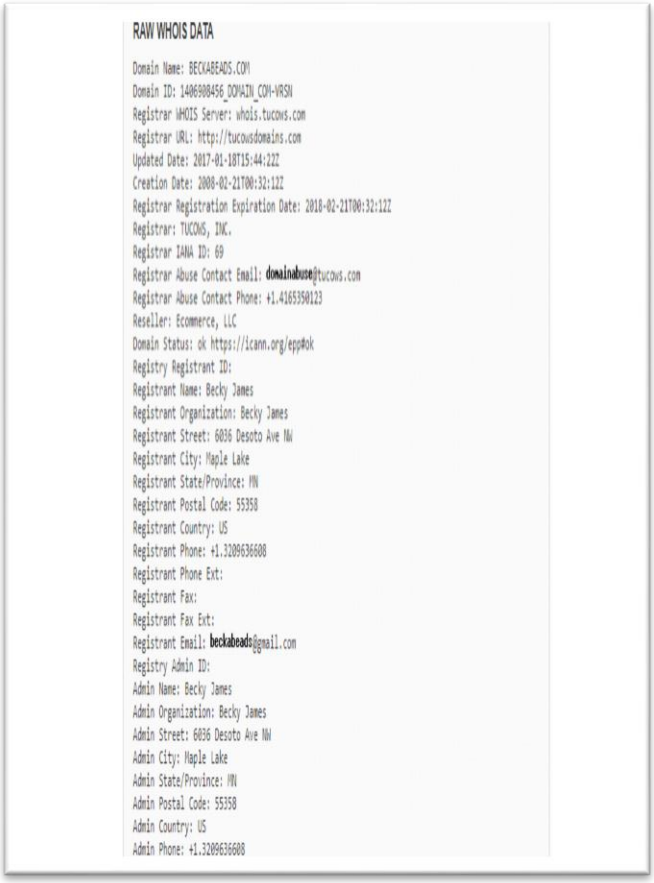
Setting target

In the first stage we decide about the system, network or web application where the penetration test is to be performed. The Scope of the test is defined in terms of the attacker profile that the penetration tester will use and about the duration of test [2], [10].

Information Gathering

Information gathering is the first step of penetration testing, is the process of collecting all information about the target. It is also drawn as preparatory phase where penetration tester gather information's of a target for launching the attack. Still in this paper, the penetration tester draws a competitive intelligence to understand more about the target web pages. Social Engineering is also a part of it where penetration tester gathers Information by smooth-talks. Information gathering consist of foot printing and reconnaissance [11], [10].

Foot printing refers to collecting as much information as possible about the target, while reconnaissance is how to gather information about the target site [2]. In this work information about the target site can be obtained through Google search engine using; whois.com and whois.net. These command checks the server where target site is hosted, how many other web sites are running on same server.


RAW WHOIS DATA

Domain Name: BECKABEADS.COM
Domain ID: 1406908456_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2017-01-18T15:44:22Z
Creation Date: 2008-02-21T00:32:12Z
Registrar Registration Expiration Date: 2018-02-21T00:32:12Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Ecommerce, LLC
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Becky James
Registrant Organization: Becky James
Registrant Street: 6036 Desoto Ave NW
Registrant City: Maple Lake
Registrant State/Province: MN
Registrant Postal Code: 55358
Registrant Country: US
Registrant Phone: +1.3209636608
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: beckabeads@gmail.com
Registry Admin ID:
Admin Name: Becky James
Admin Organization: Becky James
Admin Street: 6036 Desoto Ave NW
Admin City: Maple Lake
Admin State/Province: MN
Admin Postal Code: 55358
Admin Country: US
Admin Phone: +1.3209636608

Figure 2. Result obtained by using Whois.com

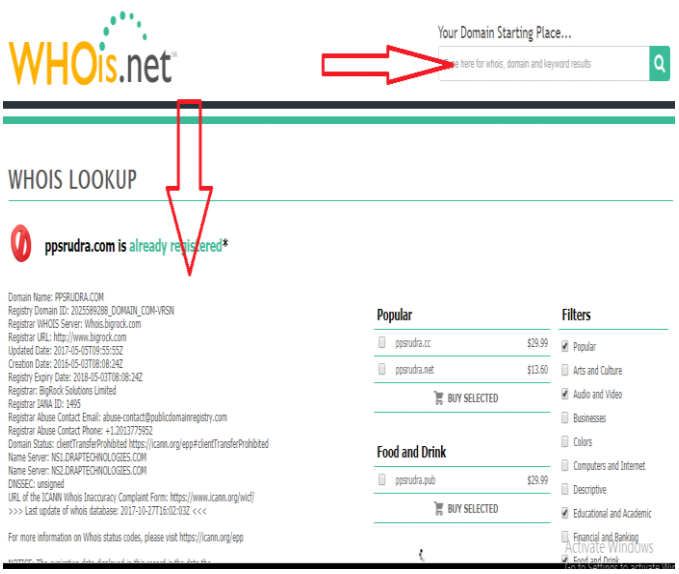


Figure 3. Result obtained by using Whois.net.

Differences were detected in the results of gathering information where whois.com (Figure 2) and whis.net (Figure 3) gives slightly similar information, although whois.net gives more accuracy and details than whois.com.

Scanning

After information gathering, scanning is the second phase of information gathering that pen tester use for vulnerability analysis. Scanning refers to the process of running a series of automated tools against IP addresses or IP ranges to target and identify known and potential vulnerabilities and unpatched or mis-configured systems. Scans create a high-level, invalidated overview and generic reporting of targeted environments [12], [13]. The purpose of a vulnerability scan is to identify unknown vulnerabilities, so that it can be remediated [14].

Network Mapper (Nmap)

Nmap has been use to check whether the network is active or not. It is also used to scans host on a network. It has the ability of detecting different applications running on a system as well as services and operating system (OS). It is one of the most widely used network scanners, because it is very effective, and easily detectable. The flowing Nmap commands are used in this research: Option (–A) is selected by default to enable aggressive scanning. Aggressive Scanning will enable OS detection (-O), version detection (-Sv), Script Scanning (-Sc) and trace route (--trace route).

Figure 4 is the result obtained after using Nmap, open port means there is a live or active network running on a particular port while close is indicating the port is inactive.

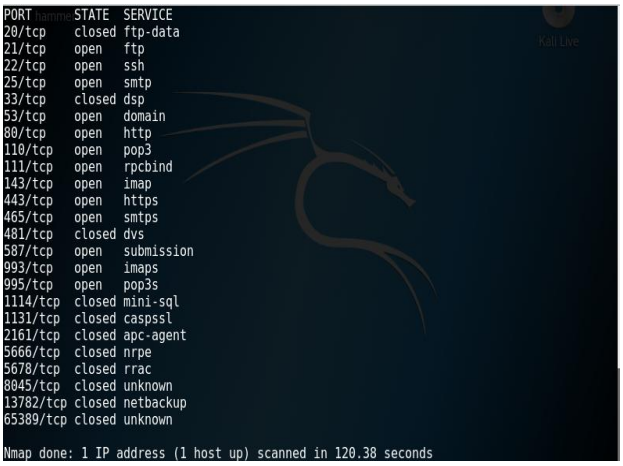


Figure 4. Nmap result after scanning

Acunetix Web Vulnerability Scanner

This is an automated tool for web application security testing which can audits the web applications by checking the vulnerabilities such as SQL Injection, Cross site Scripting, and other exploitable vulnerabilities [15]. Steps involve in Acunetix scanner include: click on new scan paste the target name in start URL and then click on next to scan the target. We scan all SQL transactions which is taking place between a web application and database. We notice hooks between the web application and database is also able to trace SQL injection vulnerabilities in the code without relying on database errors like other typical scanners do.

Two different SQL injection vulnerabilities were detected as shown in figures 5 and 6 namely blind SQL injection and normal SQL injection.

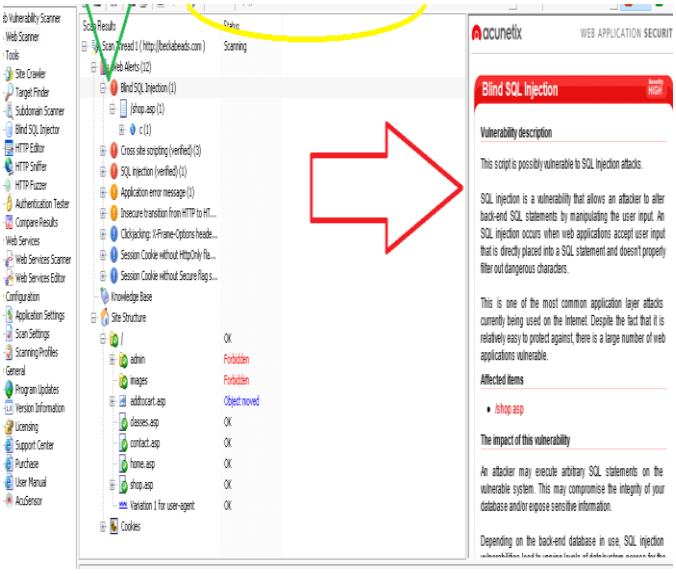


Figure 5. Blind SQL vulnerability result via Acunetix WVS

Figure 6. Acunetix Result with Normal SQL Injection verified

SQL Injection Attack against web Pages

SQL injection attack is a computer attack in which malicious data is embedded in a poorly – designed application and passed to the backend database, it also produces database query results or actions that should never have been executed [6], [15]. In the present work we propose to demonstrate four types of SQL Injection namely: Blind SQL Injection, Havij SQL Injection, normal SQL and SQL map.

Blind SQL

Blind SQL injection is the process of throwing an error to cause the application showing that it's not encapsulating quotes correctly. Code to be entered in username & password is given below:

1'OR'1'='1 ', 0=0 --," 0=0 – etc.

Takes the target site which is already scanned and vulnerable by blind SQL injection, then find the admin page of the website by open Google and type; admin and URL name (figure 7). After searching the web page, if error messages appear, it's a clear indication of blind SQL injection vulnerability. When clicking the error message, it will display the admin login page (figure 8).

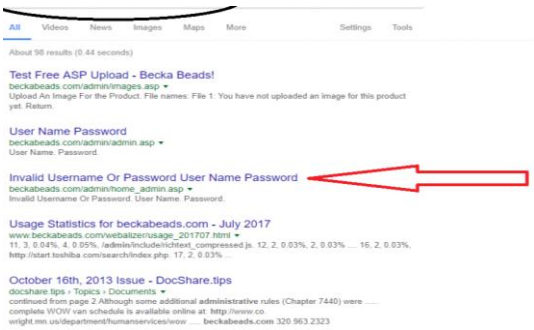


Figure 7. Vulnerable website with Blind SQL injection

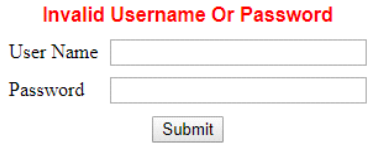


Figure 8: Vulnerable website

Upon Pasting the blind SQL Injection code in the target site as user name and password (figure 9), it will directly take to main database (figure 10).

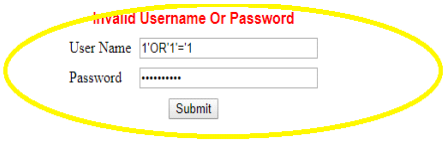


Figure 9. Vulnerable website with Blind SQL user name and password

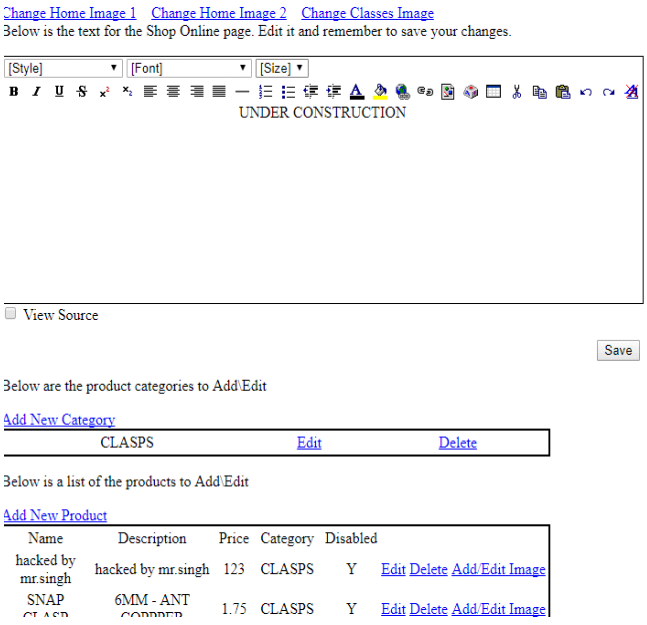


Figure 10. Attacked page by using SQL injection attack.

Now we have full access to the web pages, which we can edit, save, delete, anything from this website.

Havij Tool

Havij is an automated tool which helps penetration testers for finding and exploits SQL Injection vulnerabilities on a web page. Penetration tester can perform back-end database fingerprint, retrieve DBMS and password hashes. In this research work we dumped tables and columns, fetching data from the database, running SQL statements and even accessing the un-

derlying file system and execute commands on the operating system. We observe that, the strength of Havij makes it different from related tools in injection technique. The success rate is more than 95% at injecting vulnerable targets using Havij. Then open Havij Software and paste target website as indicated below.

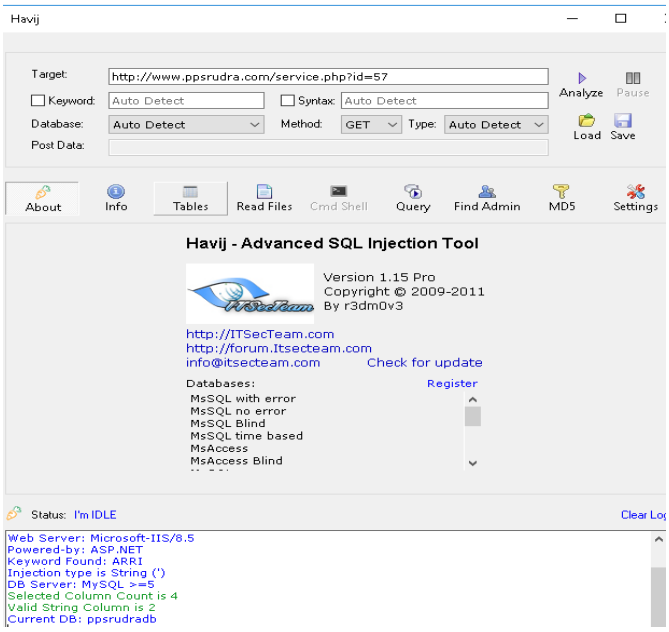


Figure 11: Havij General Interface

Normal SQL injection (Manual method)

By using manual method, you need to focus on some aspect of the SQL from the perspective of a web application penetration testing against web pages. This section presents the basic as they relate to penetration testing effort and SQL injection attacks in particular, obviously the deeper you dive in, the sharper your instinct will be when performing pen tests. One note about terminology: a query is not limited to a request of data. The query can ask for information from the database (DB), write new data to the DB, update existing information in the DB, or delete records from the DB.

Steps for SQL injection by using manual method:

- ✓ www.xyz.com/index.php?id=1
- ✓ first check the website for vulnerability by adding (‘) to the URL on the address bar. Example: www.xyz.com/index.php?id=1’
- ✓ If web site gives an error it means web site is vulnerable for SQL injection, then find the number of columns by using “order by method” command, example;
- ✓ www.xyz.com/index.php?id=1 order by 1 no error
- ✓ www.xyz.com/index.php?id=1 order by 2 no error
- ✓ www.xyz.com/index.php?id=1 order by 3 error
- ✓ It means there are 2 columns that are affected
- ✓ Next step is to find the vulnerable column
- ✓ It gives error on step 3, it means 2 column are vulnerable
- ✓ Then find the version of column by the use “union select” command below
- ✓ www.xyz.com/index.php?id=1 union select 1, @@version
- ✓ Now find the database name as:
- ✓ www.xyz.com/index.php?id=1 union select1, group_concat(database())
- ✓ Then find the name of table:
- ✓ www.xyz.com/index.php?id=1 union select1,group_concat(table_name) from information_schama.tables where table_schama=database)--
- ✓ Then open md5 string to hex converter and convert the admin to hex
- ✓ www.xyz.com/index.php?id=1 union select1, group_concat (column_name) from information_schema.columns where table_name=0xhexvalue
- ✓ Findf the user name and password www.xyz.com/index.php?id=1 union select1,group_concat (username,ox3a,password) from table name-
- ✓ http://www.bbss.com.pk/index.php?id=478%20union%20select%201,2,3,4,5,group_concat(name,0x3a,password,0x3a.id),7,8,9,10,11%20from%20admin_login--

Figure 12 show the result of vulnerable page after using manual method (String base).

Figure 12. Attacked page by using manual method

SQL map

Using Sqlmap tools: in terminal open sqlmap and go with following commands.

- ✓ Sqlmap -u testphp. Vulnweb.com/artists.php?artist=3 -D acuart – tables
- ✓ Sqlmap -u testphp.vulnweb.com/artists.php?artist=3 -D acuart -T user—columns
- ✓ Sqlmap -u testphp.vulnweb.com/artists.php?artist=3 -D acuart -T user -C uname,pass---dump if we want to perform whole database (--dump-all).

Figure 13 demonstrate the result of dump database by using sqlmap method, user name and password clearly indicated

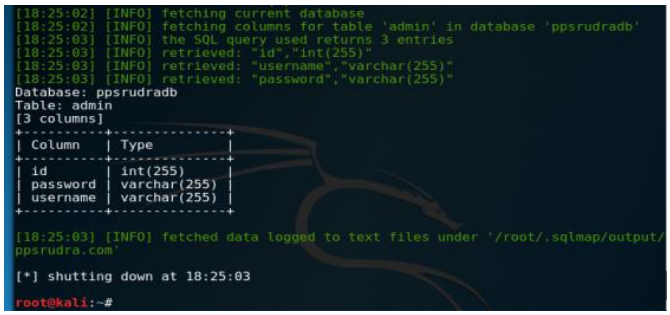


Figure 13. Dump database by using SQLmap

ANALYSIS AND REPORT

The component of the analysis has to parse and interpret the response of database server prior to the series of an attack. An analysis component uses attack-specific response criteria and keywords to measure the accuracy value and decide if the attack is successful or any weak-hole (vulnerability) are observed. Finally, generates a report of which vulnerability was found by penetration testing on the web page. The report will be generated category-wise to highlight the activities that have been carried out in the process of conducting the penetrating testing and vulnerability-wise to portray how vulnerable the system is found to be based on the results of the various scans conducted and risk level-wise brings on the attention of the organization how risky their systems are on the current setting based on the successful attacks that can be targeted on their systems.

CONCLUSION AND FUTURE WORK

The main contribution of this paper is to demonstrate how easy it is to identify and exploit web application level of vulnerabilities in a large number of web applications with help of Acunetix scanner for vulnerability assessment and different types of SQL injection. Many web pages vulnerabilities result from generic input validation problems, such as SQL Injection. Notwithstanding the majority of web pages vulnerabilities are easy to understand by the help of SQL injection attack, but many web developers are unfortunately not security aware and there is general consensus that there exist a huge number of vulnerable pages on a web. In this work, Acunetix web vulnerability scanner was used to verify whether web based pages are vulnerable or secured when they are subjected to malicious code. Acunetix WVS is a tool designed to discover security holes in the web applications that an attacker can use to access the database of an organization by looking for multiple vulnerabilities such as SQL injection. Thus in future studies, there is a need to demonstrate more SQL injection techniques (manual and automated methods) for conducting penetration testing on web pages.

REFERENCES

[1] Andreu A. "Professional pen testing for Web applications." *John Wiley and Sons,* pp. 9-10, 2006.

[2] Singh H., Surender J. and Pankaj K. V. "Penetration Testing: Analyzing the Security of the Network by Hacker's Mind." *Volume V IJLTEMAS,* pp 56 – 60, 2016.

[3] Wang X., Luhua W, Gengyu W, Dongmei Z, and Yixian Y. "Hidden web crawling for SQL injection detection."*3rdIEEE. International Conference on*, *Broadband Network and Multimedia Technology (IC-BNMT),* pp. 14-18, 2010.

[4] Goel, J. N., and Mehtre B. M. "Vulnerability assessment and penetration testing as a cyber defence technology." *57 Procedia Computer Science,* pp.710-715, 2015.

[5] Salas, M. I. P., and Martins E. "Security testing methodology for vulnerabilities detection of xss in web services and ws-security." *302 Electronic Notes in Theoretical Computer Science*, pp. 133-154, 2014.

[6] Liu L., Xu J., Guo C., Kang J., Xu S., and Zhang B. "Exposing SQL Injection Vulnerability through Penetration Test based on Finite State Machine." *2nd IEEE International Conference* on *Computer and Communications (ICCC),* pp. 1171-1175, 2016.

[7] Almubairik, N. A., and Wills, G. "Automated penetration testing based on a threat model." *11th IEEE International Conference on Internet Technology and Secured Transactions (ICITST),* pp. 413-414, 2016.

[8] Reddy M. R., and Yalla, P. "Mathematical analysis of Penetration Testing and vulnerability countermeasures." *2nd IEEE International Conference on Engineering and Technology (ICETECH),* pp. 26-30, 2016.

[9] Jiajia, W. "Research of penetration test based on mobile Internet." *2nd IEEE International Conference on Computer and Communications (ICCC),* pp. 2542 – 2545, 2016.

[10] Mirjalili M., Nowroozi A., and Alidoosti M. "A survey on web penetration test." *Vol. 3, Issue 6, No.12, Inter-*

national Journal, in *Advances Computer Science: 3(6)* pp. 107-121, 2014.

[11] Shah, S, and Babu M. M. "An overview of vulnerability assessment and penetration testing techniques." *Journal of Computer Virology and Hacking Techniques 11(1)* (2015) pp. 27-49, 2015.

[12] Yaqoob I., Hussain S. A., Mamoon, S., Naseer, N., Akram, J., and Rehman, A. "Penetration Testing and Vulnerability Assessment." *Volume 7, Journal of Network Communications and Emerging Technologies (JNCET),* pp. 10 – 18, 2017.

[13] Kals S. Engin K., Christopher K., and Nenad Jovanovic. "Secubat: a web vulnerability scanner." *15th international conference on World Wide Web*, *on Proceedings,* pp. 247-256, 2016.

[14] Meierhold N., Spehr M., Schilling A., Gumhold S., and Maas, H. G. "Automatic feature matching between digital images and 2D representations of a 3D laser scanner point cloud." *Volume 3, Int. Arch. Photogram. On Remote Sens. Spat. Inf. Sci.* Pp. 446-451, 2010.

[15] Scandariato, R., Walden, J. Joosen, W. "Static analysis versus penetration testing a controlled experiment." *24th IEEE International Symposium* on *Software Reliability Engineering (ISSRE),* pp. 451-460, 2013.