SOLUTIONS FOR AUTO-TESTING AND AUTO-WARNING WEBSITE ERRORS BASED ON THE RESULTS OF THE WEBSITE ERROR SCANNING TOOLS

Pham Duy Loc[a*], Phan Thị Thanh Nga[a]

[a] *The Faculty of Information Technology, Dalat University, Lamdong, Vietnam*

Article history
Received: January 04th, 2016
Received in revised form: March 21st, 2016
Accepted: March 31st, 2016

Abstract

Nowadays, there are commercial and free tools to automatically test websites' security which is considered to be the positive point for pen-tester. In contrast, these tools might also produce false alerts. To minimize these false alerts, it is necessary to develop a tool which helps pen-tester verify alerts manually or automatically with cross-checking results collected from many pen-test tools. We name this tool PAT (Pen-Test Assistance Tool). PAT is able to save experiences from previous successful checking for future check. PAT also can check vulnerabilities automatically based on report of pen-test tools and warn website errors to web-masters automatically via email. In the first version of PAT, we focus on SQL Injection vulnerabilities in ASP.NET websites.

Keywords: SQL injection attacks; PAT; Web vulnerability scanner.

1. INTRODUCTION

Internet users are facing huge problems from hackers. The growth of the Internet helps individual users and business users advertise their images to the world via online services and applications ranged from Instant Messaging, emails to ecommerce. Websites offering those services are becoming more and more popular. However, websites might face threats from hackers as hackers are developing in size and number. In the past, the hackers targeted passwords to change the homepage's interface. Hackers these days are more dangerous when they might even threaten the national sercurity.

* Corresponding author: locpd@dlu.edu.vn

Besides, it is concerned not only serious hackers but also “young and green” hackers who just want to show off their talent or make jokes at the Internet users.

The security of the Internet is being threatened. The hackers are more and more intelligent to find different ways to attack the Internet system. Owning to the huge amount of security errors, it is hard to check all of them manually. That explains the existence of many security checking softwares in the market. The main disadvantage of these commercial softwares is that they give many false alerts. Pen-tester has to manually determine whether each alert is true or not, or whether they are exploited or not. This approach requires high interactions between pen-tester and the system. Moreover, the results are strongly dependent on the pen-tester’s experiences as well as the devoted time for the task. From the practice of Pen-testingactivity, we see the need of having the software tool which (1) allows the use of existent pen-test tool as front-end of pen-testing and (2) assists pen-tester follow the procedure of the test in order to produce complete and stable (i.e. independent from person who does the test) results.

2. SQL INJECTION VULNERABILITIES

2.1. Introduction

SQL injection is a technique exploiting the vulnerability in Web application by using SQL queries that do not filter some special characters such as ‘,+,<,>… and some special strings like UNION, HAVING,…

SQL injection vulnerability was recognized more than 10 years ago but today many websites still have this. The web application having SQL injection vulnerability is very vulnerable because it allows hackers to execute some commands to modify, delete, insert… in its database. The hackers later escalate privileges and in the end, they have full permission in the web’s database or system. This vulnerability often occurs in some database management systems such as Microsoft SQL Server, MySQL, Oracle, DB2...

According to a report of BKIS – The biggest security center in Viet Nam, more than 50 percent of websites in Viet Nam have SQL injection vulnerability. Therefore, those websites are dangerously vulnerable and the consequences are very big. In this

project, we tried to learn many kinds of SQL injection attacks and we used the results from some popular penetration testing softwares combining with my experiences about SQL injection attack techniques to generate some guidelines on how to verify these results manually: Whether they are falsely positive or falsely negative; or it can automatically test these results for the available exploit.

Some famous website error scanning tools such as NetSparker, Accunetix,… can scan SQL injection of websites and give the report of errors but it is hard for those tools to check security because too many kinds of SQL injection errors. Almost every tools can give reports to pen-tester but they export in different formats of XML, HTML, Plan Text… so pen-tester would find it difficult to use reports and check website manually.

2.2. Example of SQL Injection vulnerabilities

Taking ecommerce websites as a typical example, those websites often build login page to require a user input his or her user name and password. After the user inputs his or her information, the system will check whether the user name and password are valid or not. If the information is valid, the user is allowed to login and he or she can do some trading activities on the website.

In this example, we used three pages: Login page (Login.aspx), Admin page (Admin.aspx) and Error page (Error.aspx).

Code snippet for login page is similar to that of Figure 1.

When we login with the user name: admin and the password: duyloc, the system allows me to login normally and then redirects to Admin.aspx page.

SQL query will be: Select * from UserAccount where UserName = 'admin' and Password = 'duy loc'

Login.aspx

```
string StringConnection =
"server=laptop;database=Demo;user=sa;password=;";
SqlConnection connection = new SqlConnection(StringConnection);
try{
    if (connection.State != ConnectionState.Open){
        connection.Open();
    }
    string StringCommand = "select * from UserAccount where UserName = '";
    StringCommand += this.txtUserName.Text;
    StringCommand += "' and Password= '";
    StringCommand += this.txtPassword.Text;
    StringCommand += "'";
    SqlCommand command = new SqlCommand(StringCommand, connection);
    SqlDataAdapter adapter = new SqlDataAdapter(command);
    object obj = command.ExecuteScalar();
    if (obj == null)
        Response.Redirect("Error.aspx");
    else
        Response.Redirect("Admin.aspx");
}
catch{}
finally{
    connection.Close();
}
```

Figure 1. Code snippet for login page

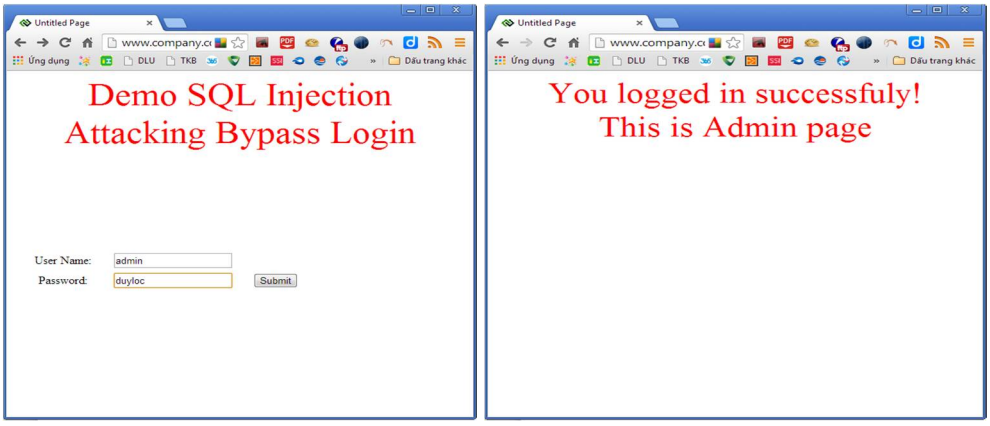

Figure 2. Login with permitted account

After that, we login with account: ' or 1=1--, password: "" (blank password)

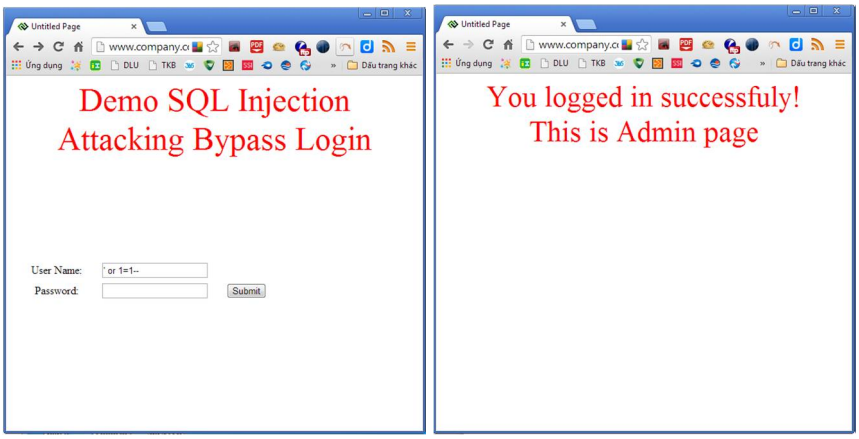

Figure 3. Login successfully with user: 'or 1=1--

Login process is still successful. We will research deeply into database query to see what will occur when we login by user name: 'or 1=1-- and blank password

The query like that: *Select * from UserAccount where UserName ='' **or 1=1--' and Password =''***

The bold part is inserted by hacker and we easily see that the query after -- sign would be ignored because it is the comment sign of SQL Server, so the query is just like this: *Select * from UserAccount where UserName = '' or 1=1*

Because query "1=1" is always true so this query will have return data and hacker will redirect to Admin.aspx page.

2.3. Other SQL Injection attack techniques

- Attacking by using Select command
- SQL Attacking using Union
- SQL Attacking using comma sign
- SQL injection using HAVING
- SQL injection using system tables
- Advanced SQL injection attacking techniques

- SQL injection attacking using system stored procedures
- SQL injection two tiers
- SQL injection attacking by using bypass filtering techniques
- Blind SQL injection attacking
- Bypass IDS with advanced Blind SQL Injection technique

Because the limit of the paper so we don't show the details of the attack techniques above. Some of them can be found in [1], [2], [3], [4], [5], [6], [7], [8], [9], [10].

3. BUILDING PAT (PEN-TEST ASSISTANCE TOOL)

Today, we have many commercial and free tools to test security of websites automatically which are very helpful to pen-testers but these tools often give us many false alerts. Therefore, we are determined to develop PAT (Pen-Test Assistance Tool) to help pen-testers verify these alerts by cross checking results among many famous pen-test tools or pen-testers can verify such alert manually with the help of this tool or this tool can check some known vulnerabilities automatically.

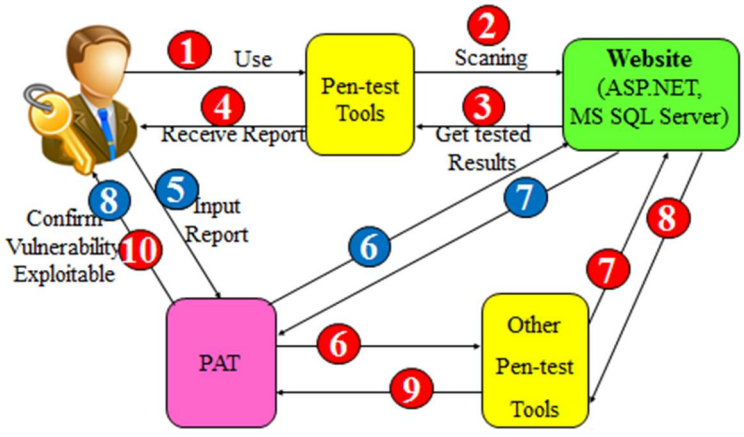

Figure 4. Steps for testing vulnerabilities of a website

PAT has ability to input results from Pen-test tools, some of famous tools can be found in [11], [12], [13], [14], [15], [16]. Next, it extracts some important information from scanner reports and loads in application. After that, pen-tester can choose one or

some critical vulnerabilities and checks them again with other Pen-test tools to confirm whether these vulnerabilities can be exploited or not with the help of PAT. Pen-testers can check some vulnerability by using automatic checking feature of PAT to confirm these vulnerabilities.

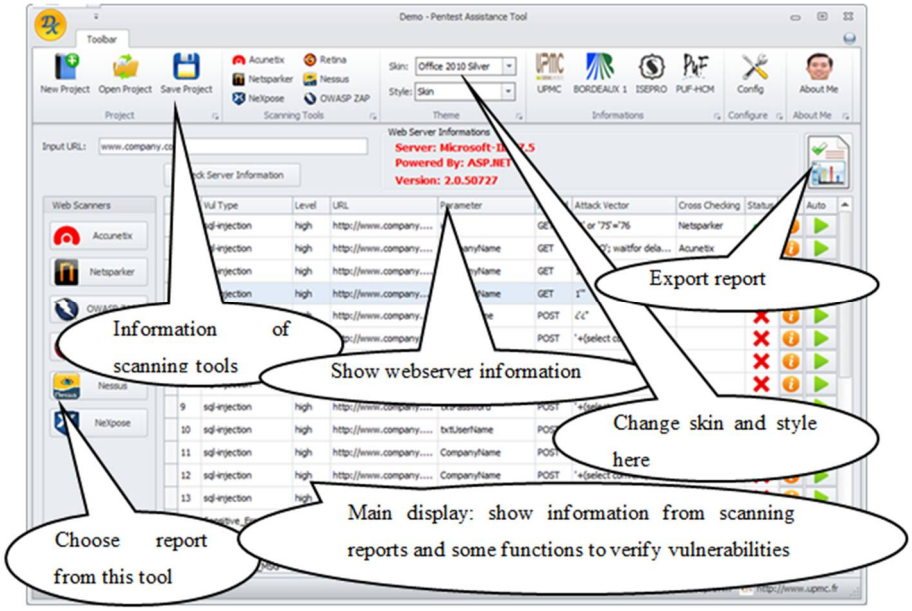

Figure 5. Main screen of PAT

Pen-test tools give us very different reports so we must read these reports and standardize them. The reports shown in application include: vulnerability kind, level of risk, URL which can be exploited, attack vector, information about these vulnerabilities, etc.

Features of PAT:

- Standard reports from other scanners and input into PAT
- Cross-check reports of one scanner by other scanners
- Automatically check vulnerabilities based on scanner's report
- Save experiences of pen-testers after successfully testing for future uses
- Save current project, open project, create new project

- Make report (export to PDF, XML, CSV, Excel…)
- Check server information of a website
- Automatically report the test results to preconfigure email address

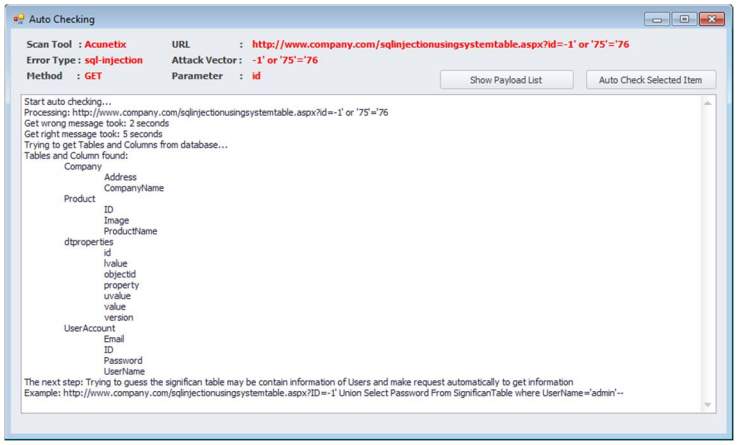

Figure 6. Checking result of one error

4. CONCLUSIONS AND FUTURE WORKS

4.1. Conclusions

With the developing of PAT, pen-testers has availability to confirm vulnerabilities of pen-test tools. Pen-testers can use PAT like a helping tool besides other pen-test tools to easily testing security of a website. Instead of using very expensive commercial vulnerability scanner, pen-testers can use some free pen-test tools in combination with limited trial commercial versions and PAT to check full vulnerabilities of websites. To reduce the time for checking vulnerabilities, pen-testers can use automatically checking feature of PAT to direct checking website security and warning the testing results to web masters automatically via email.

4.2. Future works

- PAT can check SQL injection vulnerabilities of PHP website with MySql database.
- PAT can check other vulnerabilities like XSS, directory traversal, XSRF, user name enumeration…

- PAT can detect some missing vulnerabilities of other pen-test tools.

REFERENCES

[1] Mihir Gandhi, JwalantBaria, "SQL INJECTION Attacks in Web Application", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-6, January (2013).

[2] AtefehTajpour, Suhaimi Ibrahim, Mohammad Sharifi, "Web Application Security by SQL Injection DetectionTools", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March (2012).

[3] Priyanka, Vijay Kumar Bohat, "Detection of SQL Injection Attack and Various Prevention Strategies", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April (2013).

[4] Chad Dougherty, "Practical Identification of SQL Injection Vulnerabilities", United States Computer Emergency Readiness Team (US-CERT), October 25, (2012).

[5] Inyong Lee , Soonki Jeong Sangsoo Yeoc, Jongsub Moond, "A novel method for SQL injection attack detection based on removing SQL query attribute", Journal Of mathematical and computer modeling, Elsevier (2011).

[6] Z. Su and G. Wassermann "The essence of command injection attacks in web applications", In ACM Symposium on Principles of Programming Languages, Jan. (2006).

[7] S. Thomas, L. Williams, and T. Xie, "On automated prepared statement generation to remove SQL injection vulnerabilities", Information and Software Technology 51, 589–598, (2009).

[8] K. Ahmad, J. Shekhar, and K.P. Yadav, "A Potential Solution to Mitigate SQL Injection Attack" VSRD Technical & Non-Technical Journal, 145-152, Vol. I, (2010).

[9] L. Kishori and K. Sunil, "Detection And Prevention of SQL-Injection Attacks of Web Application Using Comparing Length of SQL Query", ISSN: 2278- 5140, Volume-1, Issue February, (2012).

[10] Wikipedia, http://en.wikipedia.org/wiki/SQL_injection

[11] Acunetix Web Vulnerability Scanner, http://www.acunetix.com

[12] Netsparker Web Vulnerability Scanner, www.mavitunasecurity.com

[13] Nexpose, http://www.rapid7.com/products/nexpose

[14] Retina Web Security Scanner, www.beyondtrust.com

[15] Nessus Vulnerability Scanner, www.tenable.com

[16] OWASP Zed Attack Proxy Project, www.owasp.org

GIẢI PHÁP KIỂM TRA VÀ CẢNH BÁO LỖI CÁC TRANG WEB TỰ ĐỘNG DỰA VÀO KẾT QUẢ QUÉT CỦA CÁC CÔNG CỤ QUÉT LỖI WEB

Phạm Duy Lộc[a*], Phan Thị Thanh Nga[a]

[a]Khoa Công nghệ Thông tin, Trường Đại học Đà Lạt, Lâm Đồng, Việt Nam
[*]Tác giả liên hệ: Email: locpd@dlu.edu.vn

Nhận ngày 04 tháng 01 năm 2016
Chỉnh sửa ngày 21 tháng 03 năm 2016 | Chấp nhận đăng ngày 31 tháng 03 năm 2016

Tóm tắt

Ngày nay, có nhiều công cụ miễn phí kiểm tra bảo mật của các trang web một cách tự động đây là một điểm thuận lợi cho những người kiểm tra bảo mật. Nhưng ngược lại, những công cụ này cũng phát sinh ra các cảnh báo sai. Để giảm thiểu những cảnh báo sai này, chúng tôi đã phát triển một công cụ giúp đỡ những người làm bảo mật kiểm tra các cảnh báo bằng tay hoặc tự động với các kết quả kiểm tra chéo được thu thập từ các công cụ quét lỗi. Chúng tôi đặt tên cho công cụ này là PAT (Pen-Test Assistance Tool). PAT có thể lưu lại kinh nghiệm của những người đã kiểm tra bảo mật thành công trước đó để sử dụng về sau. PAT cũng có thể kiểm tra lỗ hổng bảo mật một cách tự động dựa vào bản báo cáo của các công cụ quét và cảnh báo lỗi web tự động cho nhà quản trị web qua email. Trong phiên bản đầu tiên của PAT, chúng tôi tập trung vào lỗi SQL Injection ở các trang web được lập trình bằng ngôn ngữ ASP.NET.

Từ khóa: PAT; SQL injection attacks; Web vulnerability scanner.