International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis and Penetration Testing Eprocurement Application with SQL Injection

Muhammad Rizal Efendi[1], Novrina[2]
[1,2]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424

Abstract**—** *Eprocurement is a web-based application that is used for processing goods and services in one of social security company. Security in applications is certainly the main thing because organizational data must be kept confidential. On the other hand, this application can be accessed via internet.*

ISO 27001 A12.6 Control Objective (Technical Vulnerability Management) states that "information about the technical vulnerability of the information system used must be obtained in a timely manner, the organization's exposure to the vulnerability is evaluated and appropriate actions taken to address the associated risks". One attempt to evaluate the security of a system is by doing penetration testing. Penetration testing helps identify vulnerability gaps and provides details about vulnerabilities or threats that exist on the system, and provides guidance on how to overcome them. Therefore in this study an analysis and penetration testing of the eprocurement application for SQL Injection was carried out using the blackbox method.

From the test results will get eprocurement application vulnerabilities along with recommendations for handling sql injection.

Keywords**—** *Eprocurement Application, SQL Injection, Blackbox Testing.*

I. INTRODUCTION

E-procurement application is a web-based application that is used for processing goods and services in the procurement process. There are two E-procurement applications in this institution, namely Internal and External. Internal is used for employees and private using VPN (Virtual Private Network). External is used by third parties as vendors and public (accessible via internet). In operation, there are many obstacles related to data inconsistencies such as eprocurement application login accounts that contain a lot of space, causing errors on the application side. Security in external E-procurement application is of course the main thing, because there are organizational data that must be kept confidential.

ISO 27001 Control Objective A12.6 (Technical Vulnerability Management) states that "information about the technical vulnerabilities of the information system used must be obtained in a timely manner, the organization's exposure to the vulnerability is evaluated and appropriate action is taken to address related risks". Penetration testing helps identify vulnerability gaps and provides details about vulnerability gaps or threats that are present in the system, as well as providing guidance on how to overcome them. On the other hand based on information from the OWASP (Open Web Application Security Project) which has been recorded since 2003 various types of hacking attacks, where SQL Injection attacks are still ranked first as the most frequent hacking attacks [11].

In the previous research, Adamu Bin Ibrahim was conducted in 2018 with the title "Penetration Testing Using SQL Injection to Recognize the Vulnerability Point on Web Pages" which is explained the penetration testing stage to obtain security holes in a web application [1]. In this study will do analysis and penetration testing of the eprocurement application system for SQL Injection using the blackbox method.

1.1 Eprocurement Application

The following is an illustration of the external and internal server eprocurement application architecture used as research objects.

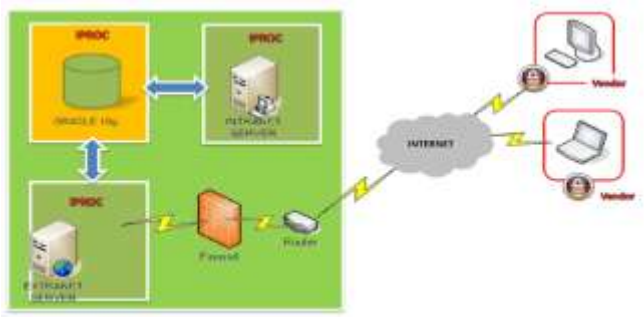

Fig. 1.1 Architecture Eprocurement Application

1.2 Security System

System security is closely related to several parts ranging from network, database, and application. How good is the security of a system can be known by conducting penetration testing which is a security testing activity on a system that aims to simulate how an anonymous user can control the network, system or database.

The following are 3 types of penetration testing methods [2]:

1. Black Box

   It is assumed the tester does not know the infrastructure of the target pentest. Thus in this black box test the tester must try to dig up from the beginning all the information needed then conduct an analysis and determine the type of attack to be carried out.
2. White Box

   In the White box testing the opposite occurs, the tester knows all the information needed to perform the pentest
3. Gray Box

   It's a combination of black box and white box conditions.

Muhammad Rizal Efendi and Novrina, "Analysis and Penetration Testing Eprocurement Application with SQL Injection," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 366-368, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

1.3 SQL Injection

SQL Injection is a technique that exploits a web application using data provided or inserted in an SQL query [12]. The way it works is by entering SQL queries or commands as possible inputs via web pages. Where web pages take parameters from the user, then make an SQL query into the database. One of them is on the user login page, where on the web page will make an SQL query to the database to check the correct username and password

Fig. 1.2 Ilustration SQL Injection

Based on information from the OWASP (Open Web Application Security Project), it has been averaging since 2003 various types of hacking attacks. Where SQL Injection is still ranked first as the most frequent hacking attacks carried out [11]. Even today, OWASP has released the latest edition of OWASP TOP 10 2017.

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

Fig. 1.3 OWASP Top 10

II. METHODOLOGY

The method used in penetration testing is Blackbox in accordance with OWASP Web Application Penetration Testing v4 [11]. The target of penetration testing is an external E-Procurement Web Application. The following stages are carried out in testing.

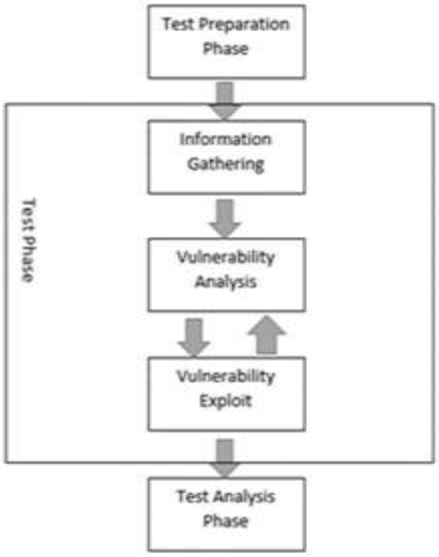

Fig. 2.1 Step of Penetration Testing

2.1 Information Gathering

The initial step in the penetration testing process is to carry out Information Gathering, which is looking for information related to the Web Application Procurement that is used as a supporting factor in searching for application security vulnerable points.

The following is some information about the E-Procurement Web application that is carried out during the information gathering phase which is used by nmap tools in searching information.

1. Determine the location of the application based on IP address or domain
   The process of identifying the location of the ip address is needed to trace where the location so that it can help identification to carry out penetration testing web application Eprocurement.
2. Get WHOIS information
   WHOIS is a service that is used to identify domain names in the form of names and contact information of domain registrants, date of registration, server name, email address, validity period and other important information.
3. Get port information and services used
   Used to find out which ports are open and what services are used on the Eprocurement application. So that attacks can be carried out through open ports
4. Obtain firewall information used
   Used to determine whether the e-procurement application side controls and regulates network traffic if there is a firewall.

2.2 Vulnerability Analysis

In the vulnerability analysis process, the acunetix scanner 11.0 trial version is used to determine the vulnerable points of the Eprocurement web application by scanning thoroughly. From the scanning process, a vulnerability point will be obtained which will then be followed up at a later stage, especially against SQL Injection.

Muhammad Rizal Efendi and Novrina, "Analysis and Penetration Testing Eprocurement Application with SQL Injection," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 366-368, 2019.

2.3 Vulnerability Exploit

Fig. 2.2 Step of Vulnerability Exploit

This stage is the process of exploitation with SQL Injection. Which is done via the login input form from the Epocurement application. In the exploit process sqlmap is used to test. But before it is done through sqlmap, an experiment is carried out manually through the input form contained in the Eprocurement application in order to find out the characters of the sql can be injected on the input form of the Eprocurement application.

Fig. 2.3 Form input Login

SQL Injection can't only be done on the input form, but can also be done via URL injection. The URL can be modified to obtain the expected response. Requests from users can be obtained by the POST and GET methods. The type of request sent via the URL is called the GET method, which allows the user to see the data sent. For example localhost/testing_php/?Page=news&cat=Programming&id_news=1, the question mark contained in the URL means that what comes after the question mark is the parameter and the request value sent. This request can be a parameter that will be combined with a query such as when a user sends a request to an input form using the POST method. It also provides an opportunity for the user to manipulate the database by adding certain characters or inserting query statements in the URL, so that operations that can't be carried out by unauthorized users. However, sending requests with the GET method provides a greater chance of security loopholes compared to the POST method, because the user can see the desired data and modify requests sent in such a way that can get the information in the database.

After manual testing, then using sqlmap to try all the possibilities that occur that become the vulnerability point of the Eprocurement web application.

REFERENCES

[1] Adamu Bin Ibarhim, S. K,.Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages. International Journal of Applied Engineering, 13,8, 2018
[2] G. Bacudio, A. G, An Overview of Penetration Testing. International Journal of Network Security & Its Applications (IJNSA), 3,6, 2011.
[3] Clarke, J, SQL Injection Attack and Defense. USA:Elsevier, 2012.
[4] Consulting, A, Aplikasi E-Procurement Jaminan Sosial. Lembaga Jaminan Sosial, 2014.
[5] Daniel, M. I, Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang. SHaP-SITI, 2015
[6] Gadgil Sampada, Pillai Sanoop, Poojary Sushant, SQL Injection Attack and Prevention Techniques, International Journal on Recent and Innovation Trends in Computing and Communication, 1,4, 2013.
[7] Indrajit, P. R. E, Konsep Dan Strategi Keamanan Informasi di dunia Cyber. Yogyakarta: Graha Ilmu, 2011.
[8] Jain., C. S. D. D. S. C, Analysis and Classification of SQL Injection Vulnerabilities and Attack on Web Applications, IEEE, 1,2, 2014.
[9] Pangalia, R, Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra, 2015.
[10] Sharma, Chandershekhar, SQL Injection Attack on Web Application, International Journal of Advanced Research in Computer Science and Software Engineering, 4,3, 2014.
[11] Torsten Gigler, B. G., Neil Smithline, Andrew Van Der Stock, The OWASP Top 10 2017, The ten Most Critical Web Application Security Risks. OWASP, 2017.
[12] Zam, E, Teknik Hacking dengan SQL Injection. Jakarta: PT Elex Media Komputindo, 2014.