Security Performance Analysis Of Photography Service System

Nur Khairani Kamarudin[1], Farah Shazwani Ismail[2], Mahfudzah Othman[3], Nurul Hidayah Ahmad Zukri[4], Mohd Faris Mohd Fuzi[4]
[1,2,3,4,5]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Perlis Branch, Malaysia*

Corresponding author: nurkhairani@perlis.uitm.edu.my
Received Date: 10 July 2019
Accepted Date: 12 November 2019

ABSTRACT

Photography business become more popular and trending among the most of people who likes photography. Photography Service System was developed to help photography companies to deliver photos and videos to their customers. Photography Service System enable user to access and share the data faster. The system can be used by photography companies as a method to send photos and videos to their customers. A penetration testing was conducted in order to test the security performance by conducting four security attacks which were Denial of Service (DoS), SQL injection, Cross Site Scripting, and sniffing password. The purpose of these attacks were conducted is to testing and finding the vulnerabilities of the system because the system deals with the customers' privacy data which is the photos and the videos owned by the customers. This is crucial to secure a system where the first step taken as a prevention to introduce the system to the public, vulnerability assessments was performed to determine the weaknesses of the system. Scanning and vulnerability assessment are done using tools which is Vega Scanning Tool, Wireshark, and Low Orbit Ion Cannon (LOIC). It is found that the system are vulnerable to DoS attack, SQL injection attack, cross site scripting and also password sniffing.

Keyword: *Denial of Service (DoS), SQL injection, Cross Site Scripting, sniffing password*

INTRODUCTION

Photography business and services have become more popular in these days. The methods for the photography company to deliver their customers' photo are hardcopy and softcopy. Customers often request to get the softcopy of the photos as soon as they can get them so that they can post the pictures on their social media such as Facebook, Instagram, and Twitter. A photography company usually delivers the softcopy of the photos to the customers through WhatsApp, Telegram, or cloud storage such as Google Drive and Dropbox. Cloud computing attracts more attention from business companies (Aishwarya & Malliga,2014). Photography Service System will be the best choice of delivering the softcopy of the customers' photos since the quality of the photos or files uploaded to the system will not be reduced and can deliver the photos quickly.

The service system enables users to outsource their data to a server and access data remotely over the Internet (Anu, 2017). The system allows users to store and maintain data on a remote server that is managed by Cloud Service Provider (CSP) like Yahoo and Google (Dinis & Serrao, 2014). Users can process their data on their computers, and use the data on other devices such as mobile phones (Ghafarian, 2017). By using the system to deliver the photos to the customers, the customers can easily receive the photos since they can use their computers or mobile phones to receive the photos.

This research project is purposely done to test the system to determine the security flaws and vulnerabilities in this system. Security is one of the efficiency standards where it is the main indicator and guideline of the performance level. Security is essential to the system because it protects the

system from threats. Security in the system is a highly sensitive and important factor because it deals with confidential data in the system (Goyal & Goyal, 2017). Every system should provide a strong security protection and privacy to protect the data of its customers who are using the system. The system should avoid security threats. For example, Denial of Service (DoS) attack, SQL injection, Cross Site Scripting (XSS), and sniffing password. These attacks are attempted to prevent a system from performing its normal functions.

METHODOLOGY

Sotware Description

The software used for this research project was VMWare Workstation, LOIC – Low ORBIT Ion Cannon, Wireshark, and Vega.

1) VMWare Workstation

VMWare Workstation is a virtual machine software that is used for x86 and x86-64 computers to run multiple operating systems over a single physical host computer. Each virtual machine can run a single instance of any operating system (Microsoft Linux, etc) simultaneously (Nagpure & Kurkure, 2017).

2) LOIC – Low Orbit Ion Cannon

LOIC is an open-source network stress testing and denial-of-service attack application, written in C. It was initially developed by Praetox Technologies but was later released into the public domain and now is hosted on several open source platform (Dinis B., & Serrao C., 2014).

3) Wireshark

Wireshark is an open-source packet analyzer. It is used for network troubleshooting, analysis, software and communication protocol development, and education. It is originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues (Gupta, Jain, Saini, & Gupta, 2016).

4) Vega Scanning Tool

Vega is a free and open-source web security scanner and web security testing platform to test the security of web applications. Vega can help find and validate SQL Injection, Cross Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities.

Hardware Description

Asus Laptop was used for the research project. The processor is Intel Core i5-4200U, the RAM of a laptop used is 8.00 GB, and system type of the laptop used is 64-bit operating system, x-64-based processor.

Testbed Architecture

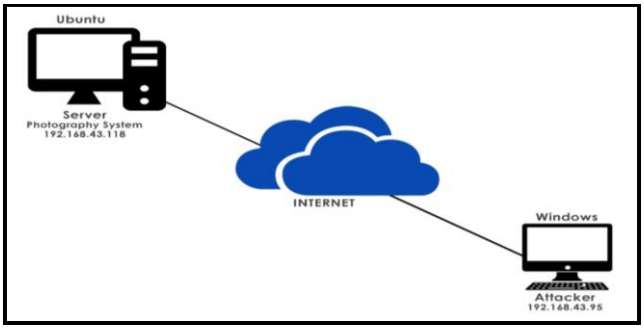

Figure 1 Testbed Architecture

The web server of photography service system's IP address is 192.168.43.118 while the attacker's IP address is 192.168.43.95. The attacker will act as white hat hacker who wants to test the photography service system performance based on Denial of Service (DoS) attack, SQL injection attack, Cross Site Scripting (XSS) attack, and sniffing password attack.

RESULT AND FINDINGS

In this research project, a pilot study was conducted to ensure all equipment were working properly. Processes that have been done during pilot study including installation of all the required software and tools to conduct the experiment.

Performance Analysis Based Response Time without Dos Attack

Table 1 shows the result for the testing on response time without implementing DoS attack. From the result, it can be concluded that the photography system performance is going well and not vulnerable.

Table 1 Result Response Time without DoS

Packet captured for 5 times	Response Time (seconds)	Source Address	Destination Address	Protocol
677	0.025447000	192.168.43.118	192.168.43.95	HTTP
220	0.003354000	192.168.43.118	192.168.43.95	HTTP
403	0.110870000	192.168.43.118	192.168.43.95	HTTP
303	0.100420000	192.168.43.118	192.168.43.95	HTTP
456	0.096910000	192.168.43.118	192.168.43.95	HTTP

As shown in the graph in Figure 2, depict the measurement response time graph without DoS attack.

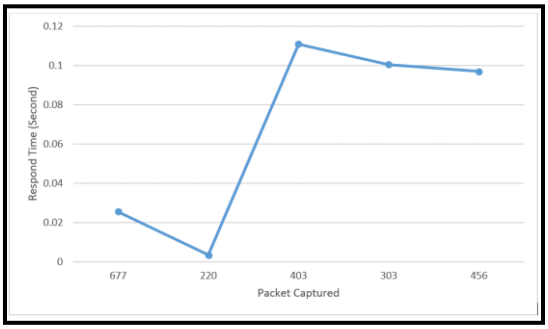

Figure 2 Response Time Graph without DoS

Figure 2 shows the response time for each packet captured for 5 times without DoS attack took less than 1 second while doing any activities in the system. The activities including key-in clients data, update clients information, and delete the data. The response time shows proves that the photography system perform well without DoS attack.

Performance Analysis Based on Response Time with DoS Attack

Next, the photography system was testes based on response time with DoS attack using Wireshark. From the result, the response time for each packet captured for 5 times took more than 1 second. It is achieved by launching a series of data packets very rapidly at the photography system. The target system becomes slow as its central processing unit (CPU) attempts to handle the requests and serve responses.
As shown in Table 2, packet captured at 79240, the response time recorded was 16.524329000 seconds. This is the time when the web server response to the client slower after doing any activities in the system with DoS attack.

Table 2 Result response time with DoS attack

Packet captured for 5 times	Response Time (seconds)	Source Address	Destination Address	Protocol
79240	16.524329000	192.168.43.118	192.168.43.95	HTTP
47195	11.813878000	192.168.43.118	192.168.43.95	HTTP
63025	15.138708900	192.168.43.118	192.168.43.95	HTTP
55303	14.256420980	192.168.43.118	192.168.43.95	HTTP
34576	10.996914620	192.168.43.118	192.168.43.95	HTTP

Figure 3 illustrate the measurement of response time graph with implementing DoS attack.

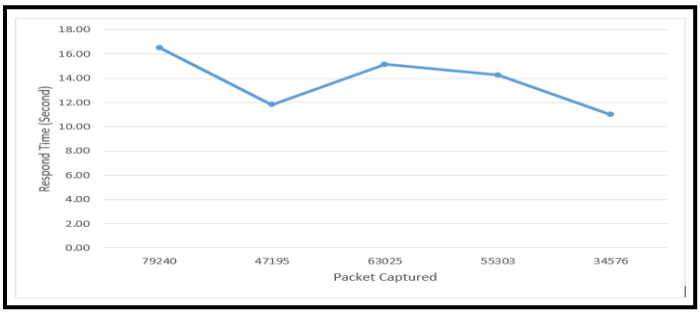

Figure 3 Response Time Graph with Dos Attack

A DoS attack was automated attempt using LOIC (Low Orbit Ion Cannon) to overload a target system with a large volume of requests to render it unavailable for use. From Figure 3, shows the result of the response time graph after this experiment was conducted.

SQL Injection

SQL injection is a type of security exploit where the SQL queries are executed without proper validation of user inputs, to access or alter the data.

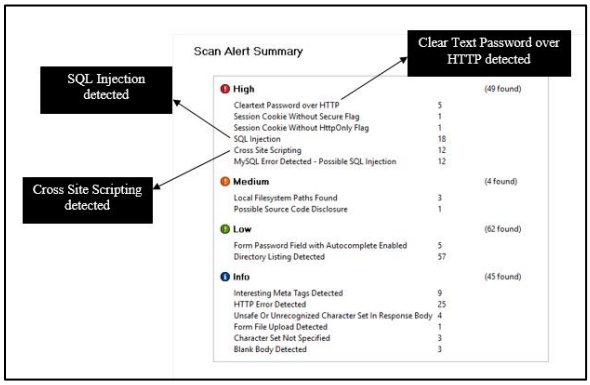

Figure 4 Result for scanning vulnerabilities

After scan the vulnerabilities of the system, SQL injection attack was conducted. After inject with "OR '1'='1" code, it is found that the following code able to breach illegally into the system.

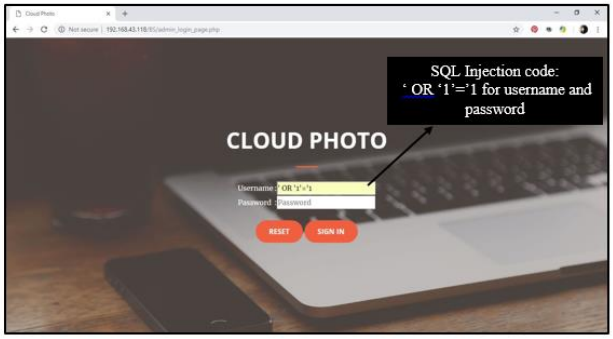

Figure 5 SQL Injection Code

Figure 5 shows that show the two examples of SQL injection code to bypass authentication using the following queries in the user input which are:

- ' OR '1' = '1
- 'or 1=1 –

Cross Site Scripting

The fourth test criteria tested was XSS attack. Cross Site Scripting attacks can be carried out using HTML, JavaScript, and other client-side languages. This attack has the ability to gather the information and important data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising. This attack also can lead to a breach of security when customer details are stolen or manipulated. This attack involves three parties where the attacker, a client, and the web site. Figure 6 shows that the photography system is vulnerable to XSS attack.

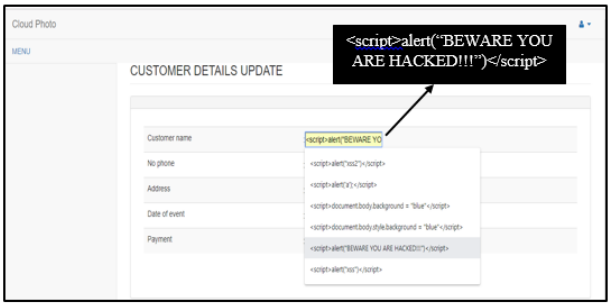

Figure 6 XSS code

Password Sniffing

Password sniffing attack is the attack when attacker want the user's password by sniffing to bypass the authentication of the system. The purpose is to know either the username and password that input by user were encrypt or not. Furthermore, website that are vulnerable usually transmit username and password as clear-text and plain-text.

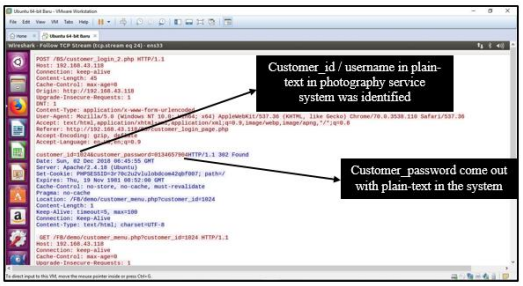

Figure 7 Password Sniffing

Figure 7 shows the result of sniffing password attack was successfully identified. From this system, the tester can view the 'customer_id=1024' and 'customer_password=0134657904' with plain-text without encryption. The tester find out the attacker can use the id and password to gain access on the system.

CONCLUSION

In conclusion, from scanning and vulnerability assessment that have been made, it shows the photography service system has many weaknesses. In exploitation, the photography service system can be breached and exploited via SQL injection, Cross site scripting and password sniffing. This photography system needs to improve its security performance before being introduce and used by the customer. In addition, this paper helps other web developer in evaluating their web system security performance by using software and hardware used.

REFERENCES

Aishwarya, R., & Malliga, S. (2014). Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment. *2014 International Conference on Recent Trends in Information Technology, ICRTIT 2014*.

Anu, P. (2017). A survey on sniffing attacks on computer networks.

Dinis, B., & Serrao, C. (2014). External footprinting security assessments security assessments, 313–318.

Ghafarian, A. (2017). A Hybrid Method for Detection and Prevention of SQL Injection Attacks, (July), 833–838. https://doi.org/10.1109/SAI.2017.8252192

Goyal, P., & Goyal, A. (2017). Comparative Study of two Most Popular Packet Sniffing Tools-Tcpdump and Wireshark, 77–81. https://doi.org/10.1109/CICN.2017.19

Gupta, N., Jain, A., Saini, P., & Gupta, V. (2016). DDoS attack algorithm using ICMP flood, 4082–4084.

Nagpure, S., & Kurkure, S. (2017). Vulnerability Assessment and Penetration Testing of Web Application. *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463920