2019 4th International Conference on Information Systems and Computer Networks (ISCON)
GLA University, Mathura, UP, India. Nov 21-22, 2019

Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application

Arvind Goutam
Department of Computer Science & Engineering with Specialization in Cyber Security
Centre for Advanced Studies, AKTU
Lucknow, India
Gautamarvind91@gmail.com

Vijay Tiwari
Department of Computer Science & Engineering with Specialization in Cyber Security
Centre for Advanced Studies, AKTU
Lucknow, India
vktiwari@gmail.com

***Abstract*— In the present scenario, the usage of internet is enormous and is escalating day by day. Internet facilities are employed in almost every field of work and people are becoming depending on it, with the increasing dependency on the internet, concern regarding information security has been increased. Because most of the work, e-commerce, chatting, payment of the bill, etc. are work through over the internet. That is why security is most important for any web site. Basically, such security concern is high in the field of organizations, institutions, and the financial sector. This problem is greater in the field of the finance sector, this problem is greater in this field not only because the financial capital associated but also organizations and client sensitive and private data. If this data hack by the attacker then attacker or unauthorized user can use this data in the wrong way. To test the security in web applications, the company performs penetration testing which identifies web applications vulnerabilities and attackers actions. This paper is focused on web application security. In this proposed research work, a framework has been built to test the vulnerabilities. This framework has the same working module as that of a financial institutions website. After penetration testing, based on the vulnerability further, a framework will be designed which will provide more security to such web sites. The developed framework can be used in several institutions, company, Organization to test the vulnerability.**

Keywords—Penetration Testing; Finance sector; Web Security; Vulnerability; Manual testing ; Automated testing

I. INTRODUCTION

Security is an important subject for organizations. In few years attackers attacked many websites. Hacking is increasing fastly from few years. Security is most important because most of the work payments of the bill, chatting, e-commerce, e-governing, online banking all this activity going through the internet[1]. If a website is hacked then the attacker can steal confidential data and can affect web application availability. Thus securing web applications is crucial. Through Vulnerability Assessment and Penetration Testing loopholes of web applications are observed and penetration tester scans loophole in the website[2] [15]. The financial sector is one of the most popular assets in the field of information technology. Some examples are the client's important data, banking account information, and transactions. There is a need for security and confidentiality because they communicate with their client's by web platform. To enhance the security financial institution are investing in penetration testing[3].

My main contribution of this paper is the vulnerability assessment and penetration testing of web applications, for this purpose, a financial web application has been developed that is based on .net technology.

Another contribution of this paper is that after penetration testing on the basis of observed vulnerability, a framework has been developed further. This will give more security to the web site. This framework can act as a blueprint for the upcoming websites so that the developers can create their website which can be safe enough against such kinds of attacks. This paper ensures that the developed project will be more secure than the running project in the finance sector.

The paper is organized as follows. Section II shows the related work in the finance sector, penetration testing, and web application security. Section III shows the methodology of vulnerability assessment and penetration testing. In Section IV discussed in details the proposed model. In section V discussed the results. And in section VI conclude the paper and shows the future work.

II. LITERATURE REVIEW

In the field of web application and on the financial web applications many types of research have been done. Basically, many researchers focused on the cross-site scripting, SQL injection, cross-site request forgery attack and focused on many other attacks on the financial web application. Some related works are as follows:

Tiago Vieira, Carlos Serrao presented a paper, in this research work focuses on security audits results analysis, which has conducted on various financial web applications, used automated tools to check web application security[4].

Abdullah Ahmed Ali, Mohd. Zamri Murah, in this paper focused on the different Libya government websites attacks and vulnerabilities, and conduct a penetration testing on different- different Libya government websites, fixed the vulnerability and used SSL encryption for data transactions, because some websites were not using SSL encryption[5].

In table 1 shows some of the approaches that are focused on different types of attacks, penetration testing on web applications security.

978-1-7281-3651-6/19/$31.00 ©2019 IEEE

TABLE I. RELATED WORK FOR VAPT AND WEB SECURITY

Sr. No.	Author	year	Issues addressed
1.	Sugandh Shah, B. M. Mhetre	2014	In this paper focuses on the NetNirikshak tool for analyses security posture, and detects SQLi vulnerability.
2.	Ramos Somya, Danny Manongga.	2018	Focuses on, the Service-oriented Business Intelligence (SoBI) will be implemented to integrate academic and financial data at SWC University into Data Warehouse.
3.	Jai Narayan Goel, BM Mehtre.	2015	In this paper described vulnerability assessment techniques and VAPT tools, and how to use VAPT as a powerful cyber defence technology.
4.	Sangeeta Nagpure,Sonal Kurkure	2017	Describes the analysis of web application vulnerability assessment and penetration testing methods.
5.	Afsana Begum, Md. Hasan Sharif.	2016	Evaluated 153 vulnerable websites and study on exploitation of RFI and SQLi-based LFI vulnerability and techniques.
6.	Hessa M. Zaheer Al Shebli, Babak D. Beheshti.	2018	This paper focused on importance of penetration testing, factors and components while conducting penetration testing.

III. PENETRATION TESTING METHOD

The present work focuses on the vulnerability assessment and penetration testing of financial web application and presents a framework for secure access to the financial web application[6]. Figure 1 show the complete process of penetration testing method is as follows:

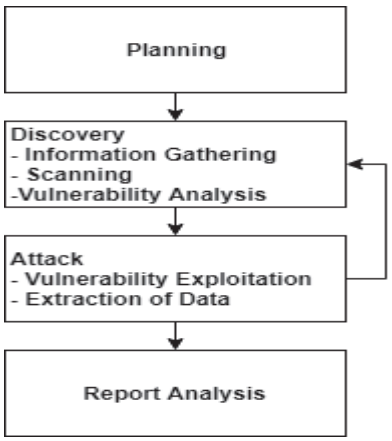

Fig. 1. Penetration Testing Method

A. Planning

In this phase, rules are identified and set the goals for testing. Through the planning phase develops a blueprint for successful penetration testing.

In this phase, before gathering the information it must be going through the assessment process. The assessment process includes goals and objective and scope, in goals and objective phase determined and examined the target web applications threats.

B. Discovery

In this first part gather the information, second part is scanning, and the third part is vulnerability analysis.

1) **Information gathering**: Penetration testing approaches successful, when gathering the information about the target it will succeed by the SQL injection. SQL injection used for the data access from the database. Below some SQL query is used in this paper:
   - 'or '1' = '1
   - admin ' --
   - ' or 1=1/*
   - 1 or 1 = 1
   - 'or 1 = 1; --
   - ') or ('1' = '1--

   Through this code bypassed the login page, for this developed a framework not a real web site, and another command are Google dork command Inurl through this find the vulnerable input links. 'Inurl' dork retrieves links and variable can access the important data from the database, and retrieve unauthorized information, the variable is vulnerable input fields through this inject malicious query, and retrieve unauthorized information[7]. Other information such as hostname, IP address, contact, and customer information gathered from it in this face.
2) **Scanning**: When the login page has bypassed, then scan the target web application to finds the weaknesses in this phase, and find which ports are open and which services are running on that port. Through these results vulnerability types and which attacks are suitable is determined.
3) **Vulnerability analysis**: In vulnerability analysis phase appropriate and probable threats are determined. In the first part SQLi threat found for the web application. For generating error messages, different SQL queries are injected in the input fields, Found in the first part. If an error message is found that shows that SQLi vulnerability is found.

C. Vulnerability exploitation

Basically in this phase attack actions performs. Attempt to perform vulnerability exploitation and extraction of data is part of the attack, through vulnerability exploitation phase malicious query is inserted in the web application on the input part. Attack techniques vary on the basis of error message information which is found in the vulnerability detection phase.

D. Data Extraction

In the extraction phase when an attack is successful, that is SQLi. Through SQL injection attack extraction is performed and extract the table data, column names and all other sensitive information that is stored in the database like password, access system files and user information the pen tester can send the malware through it and can be compromised all the website network[8].

In this paper, the database is not manipulated in any way nor do the networks while the testing. The purpose is to find the database column names and table name where the user information is stored.

When all the steps of planning, discovery, vulnerability exploitation and data extraction performed, a conclusion is made depending upon the results. On the basis of the report, new strategies are developed. Mostly the penetration testing methodology doesn't work straight. As shown in figure 1. Then this process rotates back from the attack phase to the discovery phase.

On the basis of vulnerability, this paper proposes a framework to give more security to a web application basically a financial institutions web application. The vulnerability after penetration testing method has been shown in the results portion (Section V). The model is as follows –

IV. Proposed Model

Several financial institutions are "the most vulnerable" to getting hacked. Several financial institutions have complained about unwanted transaction done from their web site. In these cases, the financial institute security system becomes so insecure that a hacker can hack that system by any means. The attacker can extracts out user information like debit/credit card number and registered mobile.

In this paper, propose a model that will give more security than the running project in the financial institutions web sites. Basically, hackers hack a developed system from gathering information about the user and do unwanted activity. Hence we need a well-programmed and fully tested system that system may be a web/windows based system that will give an assurance to users that the created system is more secure from hackers.

Figure 2 shows the block diagram of the proposed algorithm. According to this developed algorithm, the user will log in this framework to their login id and password. If login details are correct sends the OTP to Mobile and Email, OTP will be verified if correct then ask for a reference number, otherwise will go back to the login page. Reference numbers are auto-generated at the time when a customer is registering with their login details and it will not be saved in the user details table in the database. It will show only to the customer on the registration page when the customer will create an account, the customer either can note down it or can remember it. If the reference number is correct then the money will successfully transfer otherwise will be asked for security questions. Security questions are auto-generated at the time of customer account opening. Reference number and security questions are saved in a separate table in the database that will not be saved in user details in the database. User will fill security questions if they are the correct, transfer of money will be successfully done otherwise framework will show that it is unauthorized user and block the account for some hours. And admin page will generate all this activity if any suspicious activity happens on it. And inform the customer that his/her account is blocked for some hours.

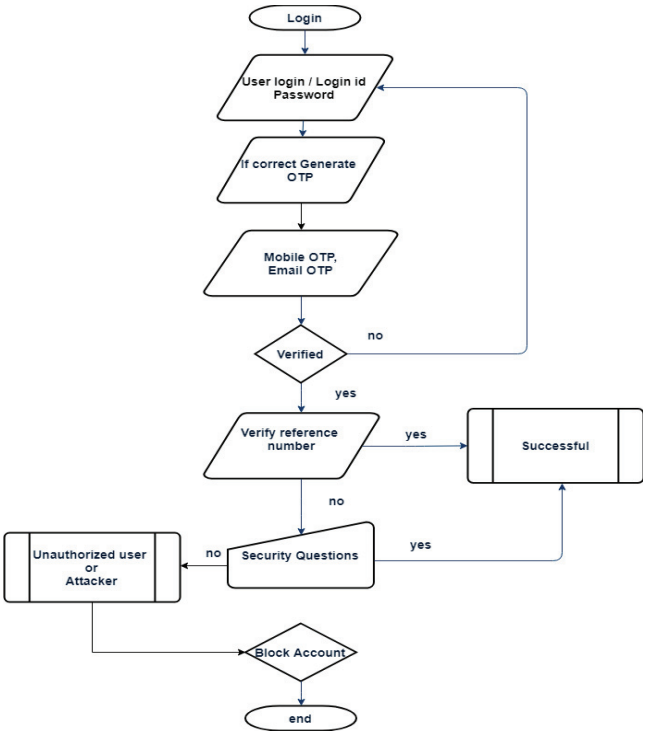

Fig. 2. Block diagram of Proposed Framework

All the procedures of the proposed framework are discussed below.

A. Two factor Authentication

In this project developed a framework it gives two-way authentication is a powerful technique for securing consumer accounts one is mobile OTP and the second one through email. Despite the effectiveness of the method, several major financial institutions don‘t use two-factor authentication to protect consumer accounts. Like in Bangladesh and some other Asian countries[9].

B. Reference number and security questions

And also it gives a framework to verify a reference number or security questions, reference number and security questions are auto-generated on the time of customer account opening. These securities-related questions will not be saved in the user details table it will be saved in a separate table in the database. It will show only to the customer on the account opening page when the customer will open an account and customer either note down it or can remember it. If any unauthorized user or attacker will want to do transaction, firstly the attacker or unauthorized user will have to bypass the login page and then two-factor authentication and then through this framework which requires a reference number that is auto-generated on the time of account opening. The attacker will not bypass without a reference number as it is not saved in customer details in the database [10]. Reference number and security questions are saved in a separate table in the database that will not be saved in user details in the database.

And if attacker or unauthorized user tries to bypass login page the second time of the same customer then this framework requires a security questions, security questions also auto-generated on the time of customer account opening and will not saved in customer details in the database, so attacker cannot find that questions than cannot bypass it, As soon as entering the wrong answer after one wrong attempt, in second wrong attempt the customer account will be blocked for some hours and admin page will generate all this activity if any suspicious activity happens on it. And will inform the customer that his/her account has been blocked for some hours.

C. Login Time Pattern

To enhance the security on this framework, Login time pattern method is used to generate the login pattern, through this user login details like system IP, and the host-name will be checked. In this framework, if user login in this framework first time through his username and password the framework will save his system IP address, Hostname then sends OTP to mobile and email. When system IP address, hostname saved once then if user login on the same system then it will not require OTP on mobile and email.

In this designed framework system checks that if user system IP, Hostname exists then the user will be login with their login details. Otherwise, this framework will send the OTP to his mobile and email.

V. RESULTS AND DISCUSSION

The vulnerability as shown in figure 3 came in this research work after penetration testing on vulnerable financial web application, used manual testing as shown in figure 1.

- X-Frame-Options header is not included in the HTTP response to protect against 'Click Jacking' attacks.
  - **http://localhost:49220/abc_Security/User/Default.aspx**
- Cross-site-scripting (XSS) protection not enabled.
  - **http://localhost:49220/abc_Security/User/Default.aspx**
  - **http://localhost:49220/abc_Security/User/page-register.html**
- SQL injection vulnerability.
  - **http://localhost:49220/abc_Security/User/Default.aspx**
- Private IP disclosure which is helpful for further attacks targeting internal systems.
  - **http://localhost:49220/sitemap.xml**

Summary of Alerts:

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	0

Alert Details:

Medium (Medium)	X-Frame-Options Header Not Set
URL	http://localhost:49220/abc_Security/User/Default.aspx
Method	GET
Parameter	X-Frame-Options

Low	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled
URL	http://localhost:49220/abc_Security/User/Default.aspx
Method	POST
Parameter	X-XSS-Protection
URL	http://localhost:49220/abc_Security/User/page-register.html
Method	GET
Parameter	X-XSS-Protection

Low	SQL injection
URL	http://localhost:49220/abc_Security/User/Default.aspx

Low	Private IP Disclosure
Description	A private IP or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://localhost:49220/sitemap.xml
Method	GET

Fig. 3. Found Vulnerability after penetration testing

After that did automation testing also on the vulnerable financial web application[11]. In automated testing used tools are Nessus and owasp zap.

The results obtained from manual and automated testing performed on vulnerable financial institution web application framework, results are shown in figure 3 and figure 4 respectively. It is observed that there is very slight difference in results obtained from manual and automated testing. Manual testing is shown in figure 1.

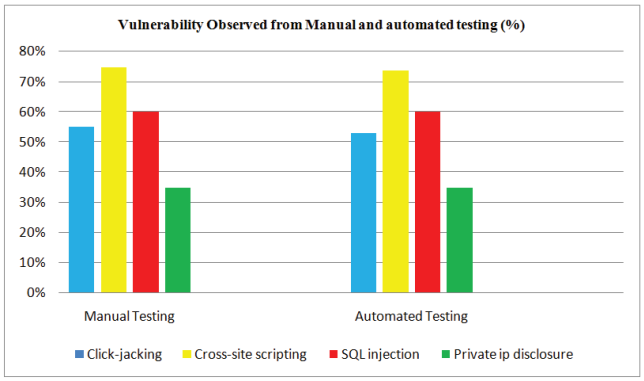

Fig. 4. Vulnerability Observed from Manual and automated testing (%).

TABLE II. STATISTICS OF WEB APPLICATION VULNERABILITY.

Testing Method	Click-jacking	Cross-site scripting	SQL injection	Private ip disclosure
Manual Testing	55%	75%	60%	35%
Automated Testing	53%	74%	60%	35%

Table 2 shows the results obtained in percentage for the vulnerabilities such as cross-site scripting, SQL injection, click-jacking, private IP disclosure discovered when performing testing on the vulnerable financial web application framework.

We solve this vulnerability and present a framework. Which is discussed above in proposed model (Section IV), after that, we did automation testing on the proposed framework. The results as shown in figure 5. Found that proposed framework has no vulnerability[12]. The report after automated testing is as follows:

Summary of Alerts:

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	0

Fig. 5. Result after automated testing on proposed framework.

VI. CONCLUSION

As hacking increasing day by day, security concern is also important for every organization especially in the finance sector where the transaction of money every day every hour and every minute[13]. Each vulnerability can be exploited in different ways and can be compromised. This paper develops a framework this framework has the same working module as that of a financial institutions website and penetration testing (manual and automated) is done, observed vulnerability after testing, solved this vulnerability and further a framework is presented which enhances the security of this proposed framework. Automation testing tool is used to check the vulnerabilities of the proposed framework. In this project framework, web application services based on .Net technologies, some vulnerability may exist in .Net technology but .Net technologies framework SQLinjection-free and have defense mechanisms from the injection. It is important for the analysis of the vulnerability of web application.

Further research can be used other web applications for penetration testing which are using the financial transaction.

And other research areas for Penetration testing, It can be used in hotel accommodation web application also, hotel websites are also too vulnerable, hotel websites uses most of the transaction through web application if the web application is the vulnerable unauthorized user can steal the data, Customer sensitive data like credit card details, and can change the data according to his use.

This paper ensures the developed project is more secure than the running financial web applications every organization should be doing penetration testing to find the vulnerability and secure them before hacking [14].

REFERENCES

[1] T. D. B. Weerasinghe and C. Disanayake, "Usage of RC4 cipher in SSL configurations in web portals of Sri Lankan banking / non-banking financial institutes and Awareness levels of relevant staff about it .," *2018 Natl. Inf. Technol. Conf.*, pp. 1–6, 2018.

[2] A. Das, "Information assurance architecture with storyboarding models," *Proc. IEEE Int. Symp. High Assur. Syst. Eng.*, pp. 377–378, 2007.

[3] M. Walker, T. Green, J. Mckenzie, S. Evans, L. Watson, and J. Lewis, *ALL IN ONE CEH Certified Ethical Hacker EXAM GUIDE Proofreader*. 2012.

[4] T. Vieira and C. Serrao, "Web security in the finance sector," *2016 11th Int. Conf. Internet Technol. Secur. Trans. ICITST 2016*, pp. 255–259, 2017.

[5] A. A. Ali and M. Zamri Murah, "Security Assessment of Libyan Government Websites," *Proc. 2018 Cyber Resil. Conf. CRC 2018*, pp. 1–4, 2019.

[6] J. N. Goel, M. H. Asghar, V. Kumar, and S. K. Pandey, "Ensemble based approach to increase vulnerability assessment and penetration testing accuracy," *2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016*, no. Iciccs, pp. 330–335, 2016.

[7] B. Qu, B. Liang, S. Jiang, and C. Ye, "Design of automatic vulnerability detection system for Web application program," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, pp. 89–92, 2013.

[8] P. S. Shinde and S. B. Ardhapurkar, "Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," *IEEE Spons. World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave)*, pp. 1–5, 2016.

[9] R. Adaimy, W. El-Hajj, G. Ben Brahim, H. Hajj, and H. Safa, "A framework for secure information flow analysis in web applications," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2015-April, pp. 434–441, 2015.

[10] C. Singh, A. Nivangune, and M. Patwardhan, "Function code based vulnerability analysis of DNP3," *2016 IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2016*, 2017.

[11] K. Vijayalakshmi and A. A. Leema, "Extenuating web vulnerability with a detection and protection mechanism for a secure web access," *2017 4th Int. Conf. Signal Process. Commun. Networking, ICSCN 2017*, pp. 16–19, 2017.

[12] A. W. Marashdih and Z. F. Zaaba, "Detection and removing cross site scripting vulnerability in PHP web application," *Proc. - 2017 Int. Conf. Promis. Electron. Technol. ICPET 2017*, pp. 26–31, 2017.

[13] S. Shah and B. M. Mehtre, "A reliable strategy for proactive self-defence in cyber space using VAPT tools and techniques," *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, 2013.

[14] E. W. Drew, "Prototyping a computer-based simulation of the finance sector," *Proc. - Cybersecurity Appl. Technol. Conf. Homel. Secur. CATCH 2009*, pp. 319–324, 2009.

[15] Sangeeta Nagpure, Sonal Kurkure. "Vulnerability Assessment and Penetration Testing of Web Application", 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017