International Journal of Computer Science and Engineering Open Access
Research paper Volume-2, Issue-3 E-ISSN: 2347-2693

Attack Generation and Vulnerability Discovery in Penetration Testing using Sql Injection

Jyotsnamayee Upadhyaya[1*], Namita Panda[2] and Arup Abhinna Acharya[3]

[1]*School of computer Engineering, KIIT University, India, ujyotsnamayee@gmail.com
[2] School of computer Engineering, KIIT university, India, npandafcs.kiit@gmail.com
[3]School of computer engineering, KIIT university, India arupacharya.kiit@gmail.com

www.ijcaonline.org

Received: 9 March 2014 Revised: 17 March 2014 Accepted: 22 March 2014 Published: 30 March 2014

Abstract— Now a days the use of the world wide web (www) is increasing rapidly and leading to security breaches of a system so testing the software system has been made iterative. Testing requires effort, time and skilful person. Hacking mostly occur in banking sector and business organizations because they maintain all the confidential information. One of the hacking technique is commonly occur in banking sector is sql injection. Security testing can be done by two ways i.e static analysis which is otherwise known as white box testing and by dynamic analysis which is known as black box testing.In this paper we have shown the penetration testing of web application to detect the sql injection vulnerability. This paper describes the penetration testing processes and mainly focuses on vulnerability discovery, attack generation and obtain the test cases and maintaining a pentester database which store all the attack responses. We have taken an internet banking transaction case study. This paper has the main motivation is to detect the sql injection by the attack generation. In sql injection system the attacker might insert a malicious code in the user input field and trying to gain access the confidential and sensitive information from the database and making the database insecure. Penetration testing is widely used to simulate an attack of the web application and then analysis the attack pattern and give better solution to the system. This paper has given an overview of the penetration testing process and sql injection attack and a pentester database.

Index Term— Testing, Security Testing , Penetration Testing, Sql Injection

I. INTRODUCTION

Now a day's web applications are highly functional and it is a two way communication between a server and a browser where the browser sends some request to the server and the server sends some responses to the browser.Everybody in this world use web applications because message passing between two parties take less time to share their data .Security of a web application become a big issue because vulnerabilities are found in web applications because of improper coding and improper cookies handeling[3].In OWASP[7] there are 10 common vulnerabilities found in the web applications those are (i)unvalidated input,(ii) broken authentication and session management,(iii) cross site scripting,(iv)buffer overflow,(v)sql injection,(vi) improper error handling,(vii) in secure storage,(viii)denial of service,(ix) insecure configuration,(x) broken access control.
Web applications are complex and face a massive amount of attacks, so security testing should be done proactively because it identify the threats in the system and measure its critical vulnerability. Security testing can be done manually and automatic manner. Since manual testing is very hard and time consuming and it has to be done through tester's observations. So automated testing is preferable. There are various types of security testing i.e. vulnerability scanning, security scanning, penetration testing, security auditing, and posture assessment. Penetration testing is the simulation of an attack. Through penetration testing we test the sql injection vulnerability. Penetration testing and static code analysis can be used to assess the vulnerabilities of web applications. Penetration testing is a method through simulation of an attack where static code analysis also known as source code analysis is a code review process which checks the defects without execution.

Sql injection is a vulnerability type where the attacker adds Sql query into a web form input box to gain access the resource or make changes the data. Penetration test is an increasingly significant security test way for detecting web vulnerability, including the SQL injection. and cross site scripting[8]. Software testing is a widely used vulnerability detection technique.The vulnerability detection techniques mainly apply static and dynamic analysis.Static analysis aims to predict all weak points of source code without executing the program,dynamic analysis executes a program with all possible inputs to detect all vulnerabilities[1].

Penetration testing is widely used to ensure for security of web applications as described in figure (1). In penetration testing process the process can be divided into seven phases i.e Information gathering, Automated scanning, Discovered Vulnerability, Attack Generation, Response Analysis ,Report Generation and Pentester Database. The Outline of the Paper

Corresponding Author: *Jyotsnamayee Upadhyaya*

is organized as follows: Section II describe the Basic concepts. The Related works are described in Section III. The proposed approach is discussed in Section IV. Section V describes a case study. Section VI describes the comparison work. Conclusion and future work is discussed in VII.

II. BASIC CONCEPT

Web applications today are widely used and it gives a better environment to his intended users to fulfill their task. With the exponential growth in size and the use of the World Wide Wave(www) has gained popularity among the people, because the web services has provided facilities for the interaction with the user. Today all the private organizations as well as Govt organizations are using modern web applications to fulfill their task. It creats a relationship between the browser and the server so it is a two way flow of communication [9].The goal of security testing is to identify the threats, threats means a Set of circumstances that has the potential to cause harm to systems and organizations and protect an information system from unauthorized disclosure. It also detect the risks in an information system.The security concepts that needs to be covered by the security testing are CIA i.e Confidentiality,
Integrity and Availability.

A penetration testing is called as the simulation of an attack because the pen tester acts as an attacker to create a attack of the target system and measure its potential vulnerability and find the weak point where the pen tester can attack. After the pen tester fulfill his attack task then he will provide better protection of the system. Before attack the target system the pen tester analysis three types of questions. The question is that(i) where the pen tester will attack (ii) How the pen tester will attack.(iii) Why the pen tester will attack the system. Pen tester always simulates a attack of the targeted system and ultimately the pen tester uses various techniques like social engineering, brute force attack and stealing password. In penetration testing the password cracking mainly done through three techniques.

1) Dictionary Attack Uses a word list or dictionary file.
2) Hybrid Crack - Tests for passwords that are variations of the words in a dictionary file.
3) Brute Force - Tests for passwords that are made up of characters going through all the combinations possible.

Sql injection is an attack where the malicious user insert sql query into the web form in put box where the attacker can gain access the resource and making the database unsecured and unavailable to his intended users. All the queries which are inserted by the attacker are executed by database engine[13].The sql injection attack techniques are (i) Tautology (ii) End of Line Comment(iii) Illegal/Logically Incorrect Query(iv) Union Query(v) Piggy-backed Query(vi) System Stored Procedure(vii) Blind Injection. To explain an sql injection attack we take the example of login page where the page displays the user id and password. The simple query is SELECT*FROM USERS WHERE USERID=WHITEHAT AND PASSWORD= BLACK. But when the attack inject sql query into the input field then the query will be SELECT*FROM USERS WHERE USERID=" OR 1=1.Here the attacker is putting the user id 1=1 that means 1=1 is always true .After executing the attacker's sql query the database gives some response and the attacker is able to retrieve all the sensitive data from the database. The attacker can update ,modify, alter the data from the database table and the attacker is able to login without the knowledge of the authorized user[11].

III .RELATED WORK

Halfond et al[1] presented a technique for penetration testing which involves static and dynamic analysis to increase the efficiency both the information gathering and the response analysis phase. The author implemented static and dynamic analysis to improve penetration testing.For discovering input vectors the static analysis technique are used and for automatic the response analysis the dynamic analysis technique is used. The main objective of dynamic analysis is to find error while running the program. To measure the effectiveness of these techniques, an experiment was conducted for static and dynamic analysis based penetration testing on nine web applications.

Xiong et al [2] presented an approach of model driven frame work which integrates the software developement life cycle phases with penetration testing process . So the vulnerability can be easily detected and testing can be done repeatable manner and by the expert personnel. To measure the cost effectiveness, systematic and fully integrated into a systematic and fully integrated into a security oriented software developement life cycle,security experts are still required to maintain knowledge. In this paper the test cases are derived from models.

Stepien et al[6] presented an approach to penetration testing for inherent to penetration testing of web application which consists inherent features of TTCN-3 languages. This paper derives the functional test cases and has taken an example of a malicious bank website. This paper has described a message sequence diagram of a malicious bank website to show the XSS attacks. It generate the functional test cases.

Pietraszek et al[5] presented an approach of Taint based Technique in which the author modified a PHP interpreter to track taint information at the character level.Context-sensitive analysis is used in this technique to reject sql queries if an untrusted input has been used to create certain types of sql tokens. The advantages of this approach is that they require modifications to the run time environment, which decreases the portability.

Halfond et al.[4] developed Amnesia(Analysis For Monitoring and Neutralizing Sql Injection Attack).In this

paper the author proposed a model based technique that combines the static and dynamic analyses. In this paper the tool first identifies hotspot, where sql queries are issued to database engines. Non-deterministic finite automata is used at each hot spot to develop query model.

In this paper we have used UML 2.0 because UML 2.0 is given the detailed and more explanation .It contains activity diagram which shows the dynamic characterists of a system. In this paper activity diagram is used as modelling diagram as it shows the flow between various activities.

IV PROPOSED APPROACH

In this paper, we present an approach to increase the efficiency of penetration testing of web application and show the working procedure. We define the penetration testing phases along with the requirements of each phase. The phases are information gathering,automated scanning, discovered vulnerability, attack generation, response analysis, report and pentester database. The proposed model is described in the figure 1.In this paper the system under test is modeled using UML 2.0 Activity diagram.The penetration tester performs a lead role in performing variety of tasks. In figure 1 shows the important phases. First the pen tester select the target of the web application server where the sql injection vulnerability is found.

A: Information Gathering: The first stage is the information gathering, where the pen tester collects information about the target system where he can attack the system. In this phase the pen tester is using various techniques to gather information. There are two methods of information gathering phase i.e black box testing and white box testing.In black box testing the pentration tester requires no previous knowledge about the attacker activities, they use tools or scripts to collect information such as Nmap, SQLPing, Paros, Web scarab, fuzzer etc. All information contains sensitive and confidential[12]. The pen tester use The most common method is social engineering, or tricking an employee into revealing sensitive information such as a telephone number or a password, and personal details. Here the pen tester attacks as an attacker where he installs on an office computer a virus, worm, or “Spyware” program and then transmits useful information, such as passwords, back to the attacker. "Spyware” is a form of malicious code that is quietly installed on a computer without user knowledge when a user visits a malicious web site.So the pen test first role is to find out the bugs of his own system and then give protection to his system.

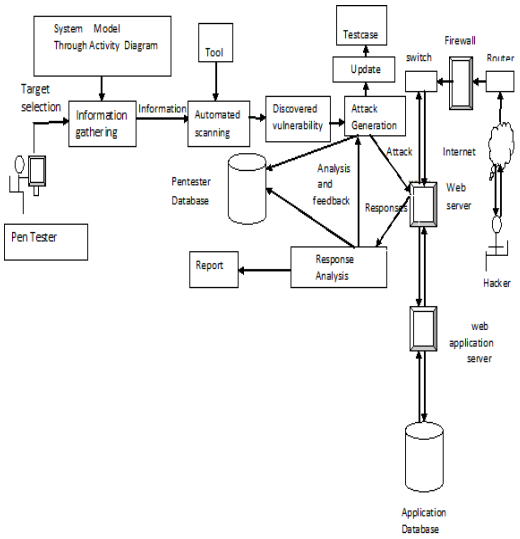

FIG 1: proposed model of penetration testing process

B: Automated scanning: The second phase is the automated scanning where the pen tester collects information about the vulnerable point through scanning in which he can find the loop holes of the entry point of the employ database or network or an business organizations. He can also bypass the firewall to retrieve sensitive information.The pen tester may take lot of time to bypass the firewall.so through automated scanning the pen tester can find the vulnerable entry points.There are various types of automated scanning is available. Some of them web crawler,fuzzer etc.

C: Discovered Vulnerability: The third phase is discovered vulnerability. Vulnerability can only be found through scanning it can be automate or it can be manual[1].First the pen tester use the scanning tool to find the vulnerable point to attack the target system. Using the information found from the previous phase the penetration tester can make a analysis about the target system and specify the script to test. The script content is very sensitive because it contents an algorithm for discovered vulnerability. So the discovered vulnerability phase plays an important role[14]. To serve the malicious purpose the penetration testers can write anomalous code to perform their task because the pen tester acts as an attacker. The pentester fulfill his task within the estimated time and evaluate the risk. The pen tester make the specific script, propose a solution to fix it and make a documentation for it.

Algorithm-1:Algorithm for Discovered Vulnerability
Input:Pentester=p,Information=I,
Database=DB,Password=PW,Userid=UD, Attack=ATK, No of information =K,T=Target system.
OUTPUT :Scan target URL, Find vulnerable URL.

1) P selects T and collects I and put it for scanning set FLAG=1
2) if(URL= ’?’)
3) Then set FLAG=0

4) return 'site is vulnerable'
5) retrive " user id " and "password" for corresponding admin.//select* from table where user id=Admin and password "OR 1=1"
6) for(I=1;I ← K;I+1)
7) do while
8) DB → I!=null //loop until information of DB!=null
9) end for
10) if (I → UD=DB → UD)
11) return "UD is match"
12) end if
13) else
14) return "UD is not matched"
15) if (p →PW !=I → PW)
16) Then (I → PW !=DB → PW)
17) return "password is not match"
18) end if
19) else
20) attack is possible
21) end if
22) else
23) "URL is protected"
24) stop

D: Attack Generation: The fourth phase is the attack generation of the target system. In this phase the pen tester generates the attacks in the web application through malicious code or putting sql query in the vulnerable url. The pen tester put the sql query in the vulnerable web site URL. The generated attack can make problems at the time of testing like it makes the database insecure, access sensitive information and confidential data. The main task of the organization is to protect and manage the penetration testing because before executing or running the script should be verified. The organization should maintain a log table to store the ongoing activities and it needs auditing regularly. During the scanning time each object should be tested carefully because it may create the violation of police and cause the penetration testing must be halted. So the pen tester play a vital role when generate an attack of the target database. In the attack generation phase we will implement the CRSScanner to check the sql injection vulnerability. The CRSScanner has 3 injection vulnerability they are (i) Crawling the whole web application (ii)Scanning for vulnerable points (iii) Generate Attack and Report[15].After the attack generated in the target system ,it will updated and generate the test cases.

This paper proposed an attack generation algorithm.

Algorithm-2 Algorithm For Attack Generation

OUTPUT: Scan target URL, Find vulnerable URL, store responses in the Pentester database. Generate the report.
1) insert the target URL and set its status =0.
2) if URL= '?' OR user id=2
3) status=0
4) query=select* from user where user id=2
5) STATUS=1
6) Result set rs = stmt. execute query
7) send query to database
8) collect the response of the above query and store it in the pen tester database.
9) while(DB → value!=no record)
10) string st = rs.get string("user id")
11) query 1 = select password from user where user id= +st && '1=1'
12) send query to Database.
13) end while
14) while(database has no record)
15) password = rs1.get string(user name)
16) store user name and password in the pen tester database.
17) end while
18) return attack is successful
19) update the attack responses in pentester database
20) Inform the attack generation that the attack was successful.
21) generate the report.
22) else
23) URL is protected

E: Response Analysis: The fifth phase of penetration testing process is response analysis phase. In the information gathering phase the pentester collects the information, i.e the identification of inputs and insert the inputs to the vulnerable URL. In this phase the aim of response analysis is to determine whether the performed attack is successful or not. The pen tester checks if the simulated attack was successful or it means that sql injection flaws identified by such penetration tester exists in the system. If the pen tester can't make any flaws in the system then the system is protected. After the successful attack the response analysis phase send the feed back to the attack generation phase. It is an iterative process because when the attack will generate in the target web application ,the web application will give responses. The response analysis phase collects the responses and analysis that the attack was successful. After that the response analysis phase gives the feed back to the attack generation phase and showing some error messages which is stored in the pen tester database as log table, it is an iterative process. The examples of error messages are showing in the Table 1.

Table 1: Log Table of error message.

S.no	Error message
1	"you have an error in your SQL syntax"
2	"Invalid parameter type"
3	"Unknown table"
4	"ODBC Microsoft Access Driver"
5	"Can not find record in"

F: Report : The report generation is the sixth phase. In this phase the report contains the overall working procedure of penetration testing. The final report should contain the information about the flaws, risks and vulnerable points and testing processes. Analysis of the final reports, the organization will discuss the problem and provide solutions and plan for recovery and estimate the cost.

G:Pentester Database: After the complete of the attack generation phase and the response analysis phase we will update the attack paths and database error messages in the database. we will store all the database error in the database log table. we will generate the attacks in the URL if the URL is not sanitized then it will provide an database syntax error. After putting the attack request in the URL ,the web page will give some responses if there exist any database error or not. Then we will store the results in the database which will handled by the pen tester it is also called as the log table which shows all the ongoing activities of the attacker and the attack responses. Both the attack generation phase and response analysis phase will update attacks and after successful of the attack the responses will be updated in the database. So this proposal will give better performances.

V .A Case study: Internet Banking Transaction. Now a day's security testing is playing a vital role because in web applications the vulnerabilities are found. The attacker is able to hack the information system and making the database insecure. The attacker can hijack the session id and making the network system unavailable to its intended users. This section depicts the details of our proposal for sql injection vulnerability through penetration testing. We have shown the UML 2.0 Activity diagram as a system model. We have taken the example of internet banking transaction. This paper we present an attack which means as an exploitation of vulnerability, where vulnerabilities are exploitation of weaknesses. Fig 2 A activity diagram of internet banking transaction.

We present our approach to a case study from the internet banking system. For making it easier and simpler, we take the example of customers access the internet banking system where the customer can access, view and update account information, of the internet banking system. For generation of test case from activity diagram, first it is converted to activity graph(AG). It is found that the number of test cases in AG is 23. In this case study the customer wants to access his account , first of all he will enter user id and password to see his account details if he will be the authorized user then he can access his account. After that the authorized user can view his account details, update account information and after finishing his work he will conform for logout. If he will not be the authorized user then it will deny for access. In this case the attacker can use sql injection attack to obtain user id and password of the internet banking customer. After that the attacker can update the account information of the online banking customer. so sql injection is an attack to obtain the confidential data from the database and make the database insecure.

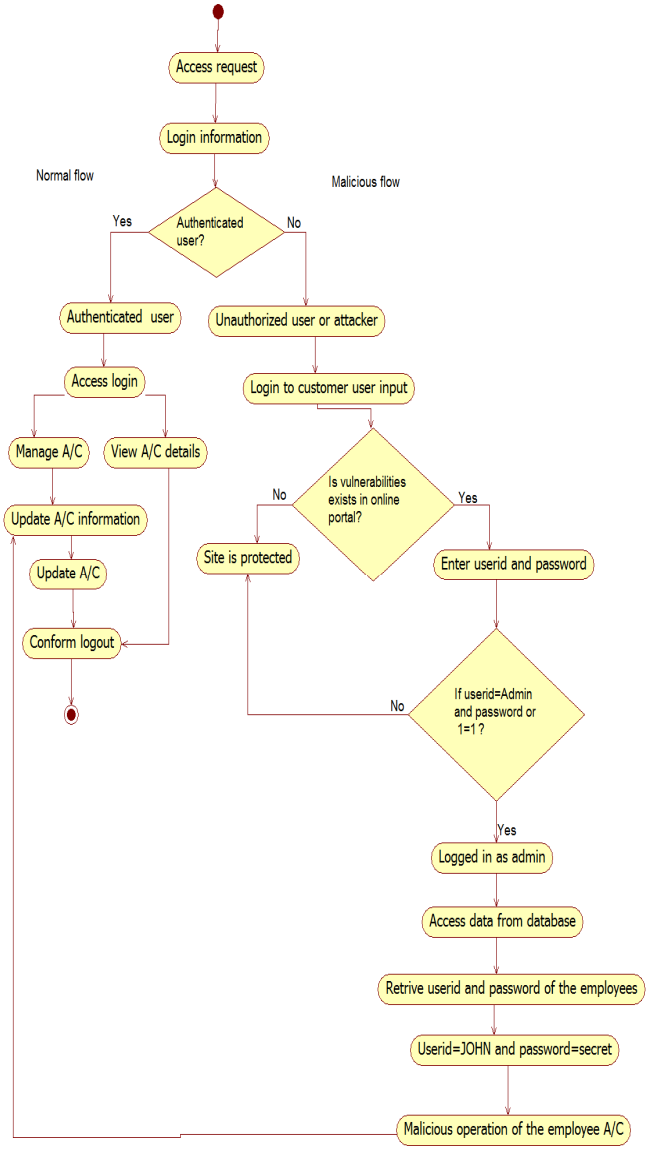

Fig 2: A activity diagram of internet banking transaction

In this case study we have tried to show how the attacker is able to obtain confidential information of the user. The Figure 3 is the activity graph of internet banking transaction system. In the activity diagram one part is the malicious flow

and the another part is the normal flow. The malicious flow is showing the attackers activities and the normal flow is showing the authorized users or genuine users activities. We have illustrated the test cases for sql injection attack. The Table 2 depicts the test cases.

Table 2: Test case for sql injection attack

Test Case	Test Case -01
Test Case Name	Sql Injection
Precondition	Internet Banking system is working, attackers try to access customer database.
Test Steps	Step and Condition
Attacker Action	Putting tautology condition in the user input field i.e user id and password to gain access to customer database.
System expected reaction	Detect this action log attack action and inform system administrator and customers.
Attacker Action	To access the password and user id from the database and exploit the customer information.
Expected Security Reaction	The system prevent attacker from obtaining customer's Id and password.

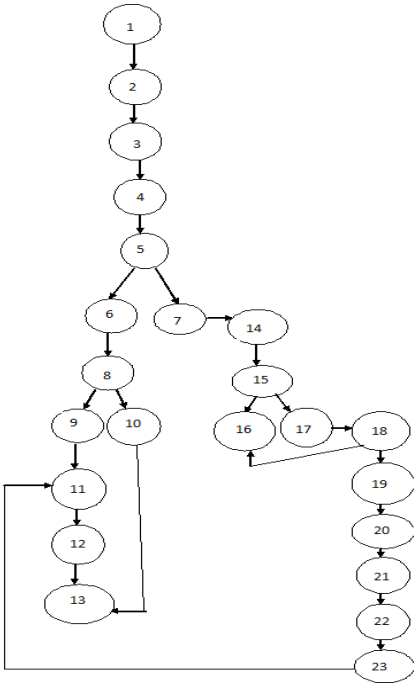

Fig. 3. Activity Graph Of Internet Banking Transaction

VI. COMPARISON

There are many security problems which are found in mainly in web applications, for that reason penetration testing can not be able to identify all the vulnerabilities .The white box and the black box testing is mainly used in penetration testing to detect vulnerabilities .If the penetration test will detect four weak point in a system to enter into the database that does not mean that hackers and intruders will not be find 5 weak points. This paper proposed a penetration testing frame work where it describes a pentester database to record all the error messages and all the ongoing activities made by the pentester .So our proposed model will give better result to detect sql injection attack.

VII. CONCLUSION AND FUTURE WORK

In this paper we presented an approach of penetration testing process to detect sql injection. Here we presented an activity diagram to model system functions. The result indicate that our method is better effective to solve all these problems simultaneously. The case study represented in this paper is relatively small. In the future research, we plan to apply this approach on a comparatively large application to review the scalability of the proposed approach and generate test cases and implement the tools. In our future work we will implement the tool in a testing environment and will give better result and giving protection to the system for various attacks. Our research outcomes help: to measure the security level of Web Applications using proposed tools to find or detect vulnerabilities of online applications and to protect the application through proper coding. In the future, we will improve the performance of the current system.

BIBLIOGRAPHY

[1] Halfond WGJ, Orso , Improving penetration testing through static and dynamic analysis, Software Testing, Verification, And Reliability(2011).
[2] Pulei Xiong, Liam Peyton, A Model-Driven Penetration Test Framework for Web Applications, 2010 Eighth Annual International Conference on Privacy, Security and Trust.
[3] Lashanda Dukes,Xiaohong yuan, A case study on web application security testing with tools and manual testing, 2013.
[4] Halfond WGJ, Orso A. AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks, Proceedings of the International Conference on Automated Software Engineering, Long Beach, CA, U.S.A., November 2005;174183.
[5] T. Pietraszek and C. V. Berghe , Defending Against Injection Attacks through Context-Sensitive String Evaluation, In Proceedings of Recent Advances in Intrusion Detection (RAID2005), 2005
[6] Bernard Stepien, Liam Peyton, Pulei Xiong , Using TTCN-3 as a Modeling Language for Web Penetration
[7] www.owasp.org
[8] A. Kie zun, P. J. Guo, K. Jayaraman, and M. D. Ernst, Automatic creationof SQL injection and cross site scripting attacks, in Proc. of ICSE, 2009.
[9] Lei Xu, Baowen, A frame work for web application testing, International Conference on Cyberworlds, 2004.

[10] Nuno Antunes, Marco Vieira, Evaluating and Improving Penetration Testing in Web Services, IEEE,2012.
[11] Halfond WGJ, Viegas J, Orso A, A classification of SQL-injection attacks and counter measures, Proceedings of the International Symposium on Secure Software Engineering, Washington, DC, U.S.A., March 2006.
[12] Halfond WGJ, Orso A, Manolios P. WASP: Protecting web applications using positive tainting and syntax-aware evaluation, Transactions on Software Engineering 2008; 34(1):6581.
[13] G . Buehrer, B. W. Weide, and P. A. Sivilotti, Using parse tree validation to prevent SQL injection attacks, in Proceedings of the 5th international workshop on Software engineering and middleware, 2005, p. 113.
[14] Sutton M, Greene A, Amini P. Fuzzing, Brute Force Vulnerability Discovery, Addison-Wesley: Reading, MA,2007.
[15] Arkin B, Stender S. McGraw G, Software penetration testing. IEEE Security and Privacy 2005; 3(1):8487.

AUTHORS PROFILE

Jyotsnamayee Upadhyaya is a student of M.Tech in Computer Science and Engineering and Specialization In Computer Science and Information Security(CS & IS), KIIT University,Bhubaneswar,Odisha,INDIA.Her research area is security testing .She can be reached at ujyotsnamayee@gmail.com.

Namita Panda is an Assistant Professor in the School of Computer Engineering, KIIT University, Bhubaneswar, Odisha, INDIA. She received her Master's degree from KIIT University Bhubaneswar. Her research areas include Object Oriented Software Testing, Parallel Processing and Computer Architecture. She has published papers in national and international level proceedings. She is having ten years of teaching experience. She is a member of ISTE. She can be reached at npandafcs@kiit.ac.in.

Arup Abhinna Acharya is an Assistant Professor and research scholar in the School of Computer Engineering, KIIT University, Bhubaneswar, Odisha, INDIA. He received his Master's degree from KIIT University Bhubaneswar. His research areas include Object Oriented Software Testing, Software Cost Estimation, and Data mining. Many publications are there to his credit in many International and National level journal and proceedings. He is having eleven years of teaching experience. He is a member of ISTE. He can be reached at aacharyafcs@kiit.ac.in.