Effective Risk Based Vulnerability Management in Cloud Security

[1]Kedasu Abhigna, [2]T.N.C. Rishika, [3]Basa Pooja & [4]Mr. K. Anil Kumar

[1,2,3] Under Graduate, Department of Information Technology, Guru Nanak Institutions Technical Campus
4Assistant Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India.

ABSTRACT:

Nowadays the most important concern over flawed internet is security vulnerabilities and its management. Advancements in web application not only improved the way we share the data but also increased risks by attracting the attackers to intrude into the web application and exploit the user's dataThe field of cloud computing has become a highly popular means for the smooth provision of various Information Technology (IT)-enabled business services. In today's dynamic and rapidly changing computing era, most of the organizations have chosen it as basic technology resource. Consequently, due to the expansion in usability and functionality unique security vulnerabilities and threats are emerging which act as the most substantial obstruction for cloud computing thereby, requiring timely concern. Reducing vulnerabilities is one of the most effective ways to minimize the cyber risks that can occur to information systems. It is the necessary to understand and mitigate such threats and vulnerabilities so as to gain a better insight into the required techniques and infrastructure. This would help in making the cloud architecture less vulnerable which in turn will make our future easier and technologically sounds good. Vulnerability is the most controllable element of risk which can be identified and responded quickly than others, so that vulnerability management is the process that organizations assess deployed IT systems and decide the security state and corrective security measures to take and mitigate security threats against existing loopholes. Risk based vulnerability management process is characterized by four main components; inventory (systems), focus (identify information), assess (identify vulnerabilities), and respond (execute procedures). Our project focuses on exploring the various threats and vulnerabilities and its management associated with the cloud computing technologies.

KeyWords: Threats and Vulnerabilities, Vulnerability Management, SQL Injection, Detection and Prevention.

I. INTRODUCTION:

Now-a-days, There is huge increase in number of organizations moving their workloads to cloud. As cloud provides many services for organizations to develop their products and services such as SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), IaaS (Infrastructure-as-a-service). Cloud computing can be defined in many ways. There is no universal definition for it.Cloud delivery models as shown in Figure 1, allow consumers to access the services provided by cloud service providers. These are discussed in

detailbelow:

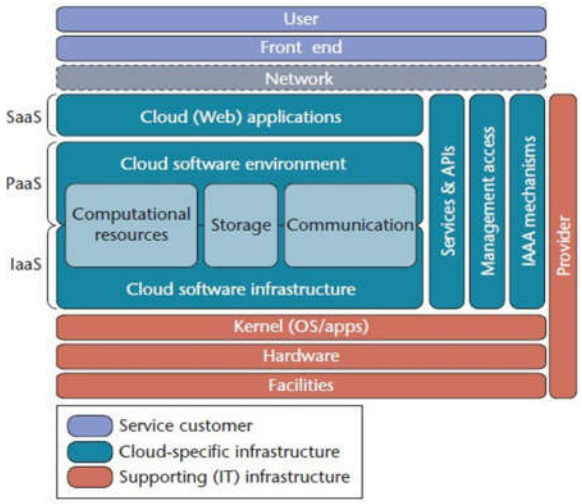


Figure 1: Cloud delivery models and architecture.

Web-based applications provide dynamic web pages for Internet users to access application servers via a web browser. The applications can be as simple as an email system or as complicated as an online banking system. Study has shown that the servers are vulnerable to web-based attacks.According to a report, the number of web attacks in 2011 increased by 36% with over 4,500 new attacks each day.Malware injection attack is one category of web-based attacks, in which hackers exploit vulnerabilities of a web application and embed malicious codes into it that changes the course of its normal execution. Like web-based applications, cloud systems are also susceptible to malware injection attacks. Hackers craft a malicious application, program, and virtual machine and inject them into target cloud service models SaaS, PaaS and IaaS, respectively. Once the injection is completed, the malicious module is executed as one of the valid instances running in the cloud then, the hacker can do whatever he desires such as eavesdropping, data manipulation, and data theft.

Among all of the malware injection attacks, SQL injection attack and cross-site scripting attack are the two most common forms. SQL injection attacks increased 69% in 2012.SQL injections target SQL servers that run vulnerable database applications. Hackers exploit the vulnerabilities of web servers and inject a malicious code in order to bypass login and gain unauthorized access to backend databases. If successful, hackers can manipulate the contents of the databases, retrieve confidential data, remotely execute system commands, or even take control of the web server for further criminal activities.A threat is a potential cause of an incident that may result in harm to a system or an organization. A vulnerability is a weakness in the asset or system which is exploited by a threat. So, we worked on the vulnerability management of the websites that are vulnerable to SQL Injections. We used a prevention and detection technique for the control of malicious attacks.This led to

the birth of web application security which is nothing but the practices of protecting the web services against the security threats that exploit loopholes that is present in application's code.In this paper we are emphasizing on the most common and dangerous security threat on internet i.e., SQL injection attack and a technique to prevent.

A. Our Contributions:

1. We have developed a simple vulnerable website which can be attacked by a SQL injection.
2. We have created an instance in open stack cloud service with Linux operating system.
3. By using LAMP server, we deployed our wed application into the cloud.
4. After a trail of SQL Injection, we have managed the web application with the detection and prevention technique.
5. We used bind parameter technique for the purpose of detection and prevention of the malicious attacks.

II. LITERATURE REVIEW:

In the past, hackers used multiple computers or a botnet to produce a great amount of computing power in order to conduct cyber-attacks on computer systems. This process is complicated and can take months to complete. Nowadays, a powerful computing infrastructure, including both software and hardware components, could be easily created using a simple registration process in a cloud computing service provider. By taking advantage of the prevailing computing power of cloud networks, hackers can fire attacks in a very short time. For example, brute force attacks and DoS attacks can be launched by abusing the power of cloud computing.

A brute force attack is a technique used to break passwords. The success of this attack is greatly reliant on powerful computing capability because thousands of possible passwords are needed to be sent to a target user's account until it finds the correct one to access. Cloud computing system provides a perfect platform for hackers to launch this type of attack. Thomas Roth, a German researcher, demonstrated a brute force attack in the Black Hat Technical Security Conference. He managed to crack a WPA-PSK protected network by renting a server from Amazon's EC2. In approximately 20 minutes, Roth fired 400,000 passwords per second into the system and the cost of using EC2 service was only 28 cents per minute.

A threat is a potential cause of an incident that may result in harm to a system or an organization. A vulnerability is a weakness in the asset or system which is exploited by a

threat. A threat agent carries out threats by exploiting one or more vulnerabilities. By conducting an exhaustive literature survey, various threats and vulnerabilities for cloud computing are identified. They are discussed in detail below:

Data Breaches (T01): A data breach is a security incident in which sensitive, private, or confidential data related to a person or organization has been accessed, copied, or transmitted by an unauthorized party. Data breach is a threat with severe risk and is ranked as number one among the threats in cloud computing.

Data Loss (T02): It is corruption or unavailability of data which results due to natural disasters like floods, earthquakes; and simple human errors like when a cloud administrator accidentally deletes files, hard drive failure, power failure, or due to malware infection.

Malicious Insiders (T03): Perhaps the most devastating threat with highest risk is a malicious insider. An insider threat can take different forms [5] like a former employee, system administrator, third-party contractor, or a business partner.

Denial of Service (T04): A DoS (Denial of Service) attack effects the availability of a system. In a DoS attack, there is only one source machine from which the attack originates and it is susceptible to mitigate. DoS attacks are designed to prevent legitimate users of a service from being able to access their data or applications.

Vulnerable Systems and APIs (T05): Cloud APIs (Application Programming Interfaces) represent an open door for public to your cloud application. Exploiting a cloud API can grant an attacker considerable access to cloud resources. Cloud Service Providers (CSP) exposes a set of software user interfaces or APIs that customers use to interact with cloud services. Those APIs should be designed to protect against accidental and malicious attempts.

III. EXISTING SYSTEM:

WAF:

Enabling web application firewall is not effective as above measures it helps to identify the SQLIA and sometimes prevent from SQLIA.Most WAFs use software, which in turn may have vulnerabilities, which can be abused.Web application firewalls also need to be maintained. Once they're set up, they need to be supported.If the rules are incorrect, legitimate traffic could be blocked, effectively breaking the application. when a WAF inspects traffic, they have only limited contextual information to work with as they only see one raw packet at a time.When analyzing

packets WAFs use a set of patterns to analyze incoming packets against. Depending on their configuration WAFs can either be overly permissive or worse, overly protective, generating false positives or false negatives.AWAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS Attack, rate limiting can be quickly implemented by modifying WAF policies.

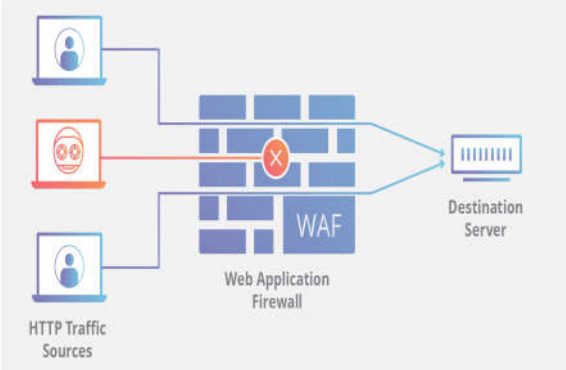


Figure 2: Implementation of Web Application Firewall.

IV.PROPOSED SYSTEM:

In this section we present the most popular technique, which is used to either detect or prevent classical types of SQLIA as follows:

Here, we used a technique to detect and prevent SQLIA at the runtime and it was developed based on SQL syntax-aware at the web application layer, and negative taint at the database layer. Applying negative taint in database layer helps the authors to identify untrusted data at the database layer, while performing syntax-aware evaluation in web application server of query strings, before executing the query in the database gives that model several significant advantages over techniques based on other mechanisms. The advantages of that model apart from efficiency are listed as follows:

This technique has been successful against all classical types of SQLIAs because the dynamic SQL statement is monitored through the database layer. Also, it does not change the web architecture.

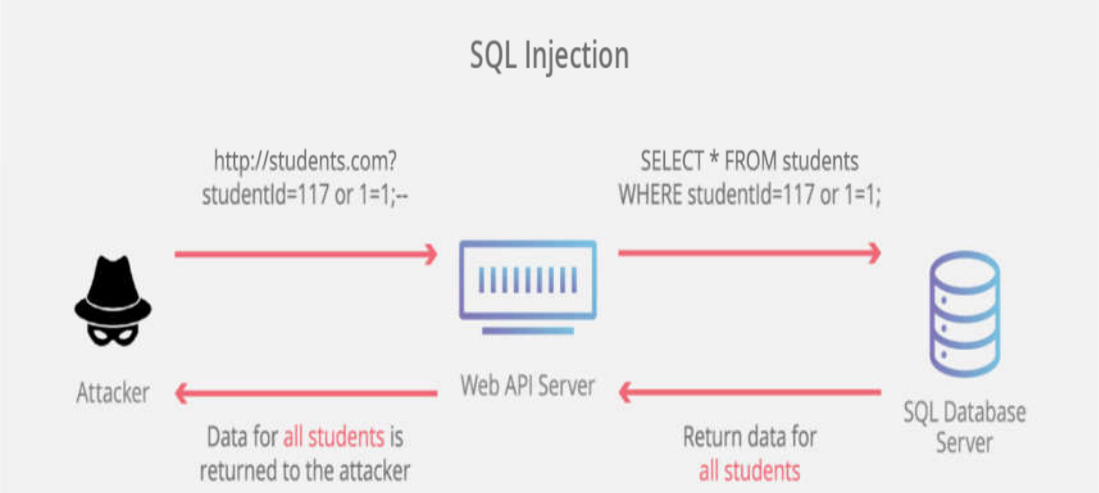
Figure 3: Overview of Proposed Approach.

SQL INJECTION:

What is SQL Injection?

SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a

Web form input box to gain access to resources or make changes to data. An SQL query is a request for some action to be performed on a database. Typically, on a Web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied.



However, most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.

SQL Injection Prevention System:

This paper proposes an effective method for preventing the SQL injection attack. The method involves the use of prepared statement which sanitizesthe input. This means it makes sure that whatever the user enters is treated as a string literal in SQL and NOT as a part of the SQL query.The user input is automatically quoted and the supplied input will not cause the change of the intent, so this coding style helps mitigate an SQL injection attack.Here is the part of the code in our web application which we included for blocking the hacker who sends the malicious queries to enter into the web application:

$pre_stmt = $con->prepare("SELECT * FROM users WHERE username = ? and password = ? ");

```
$pre_stmt->bind_param("ss",$_POST["username"],$_POST["password"]);
$pre_stmt->execute();
$result = $pre_stmt->get_result();
```

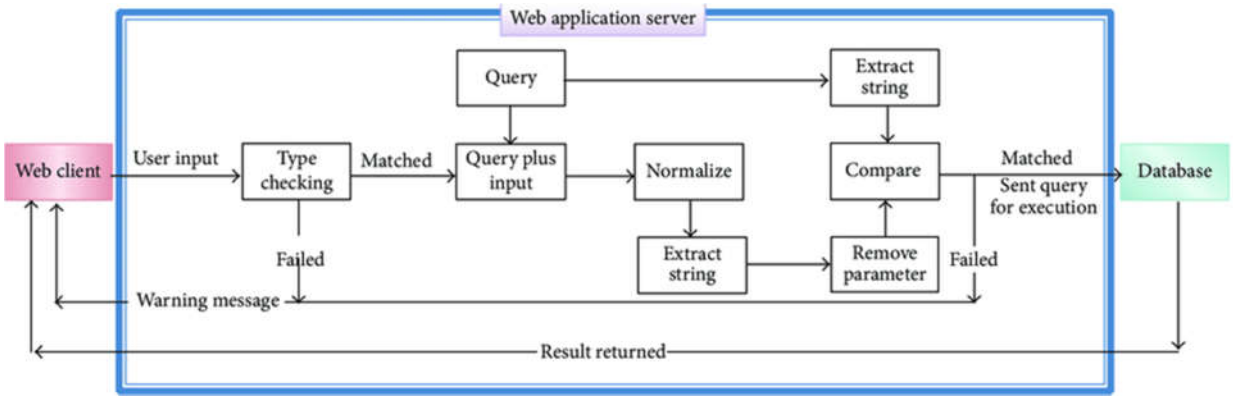
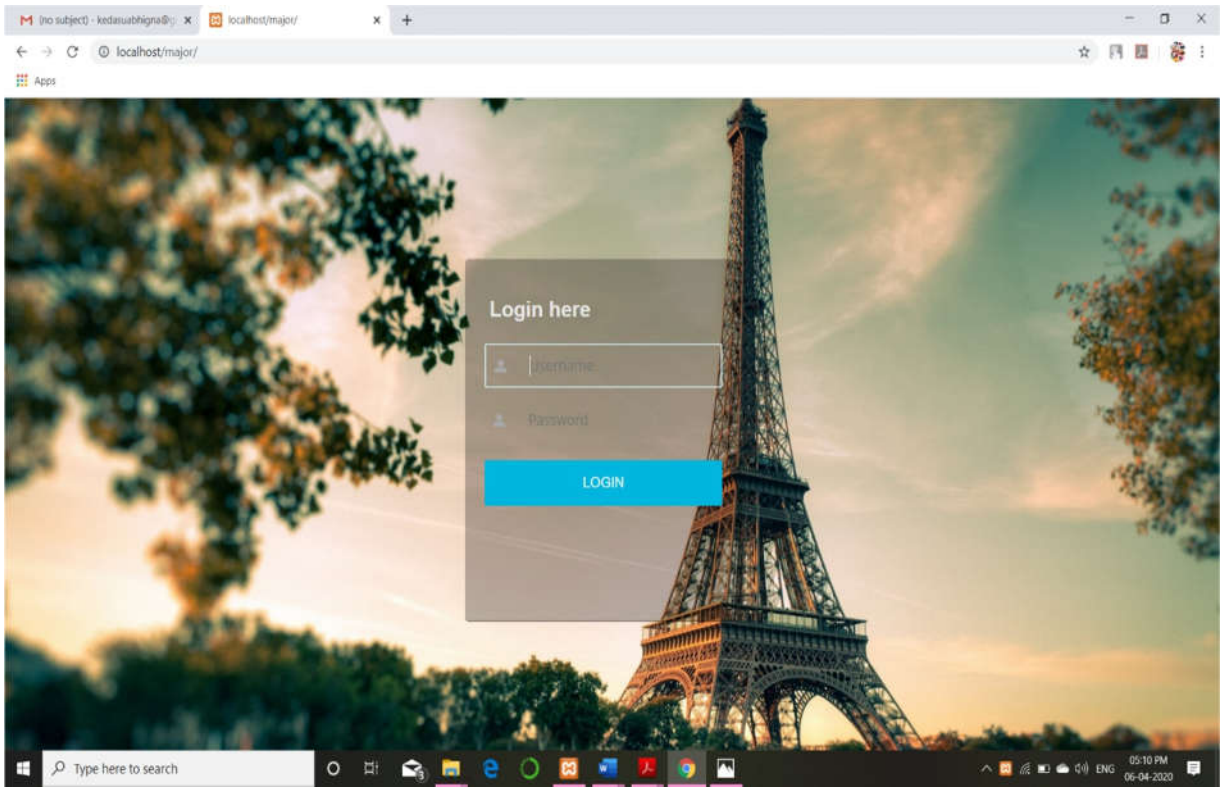


Figure 4:Detection of SQL Injection.

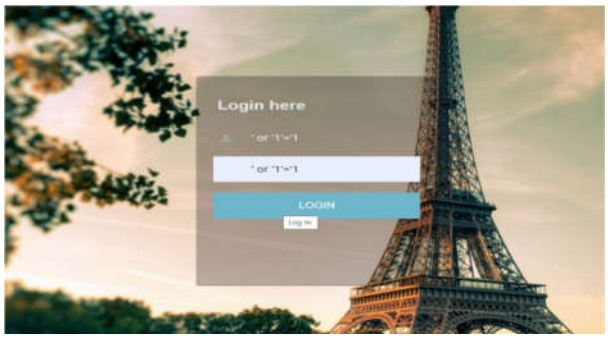
VI. MODULES:

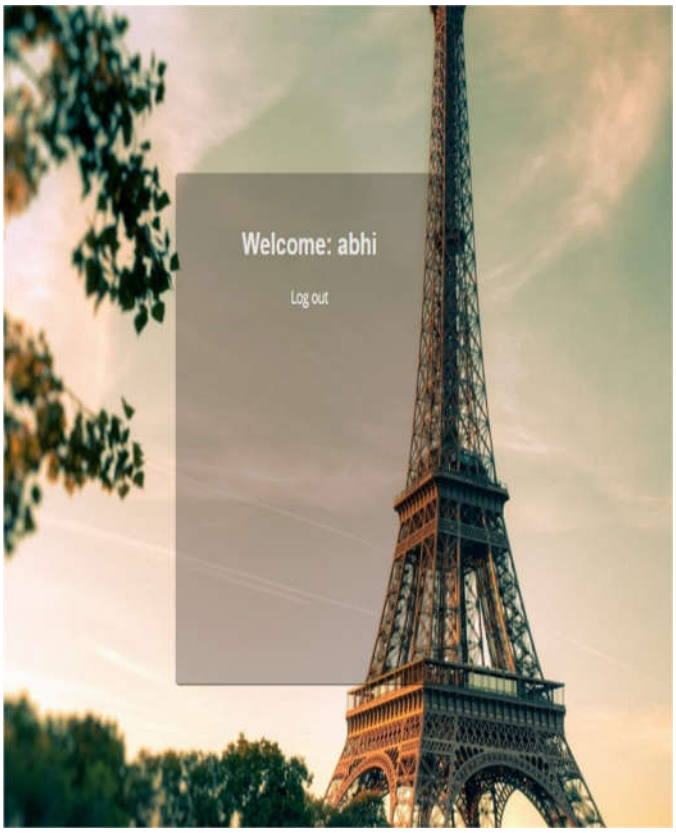
Login Module:

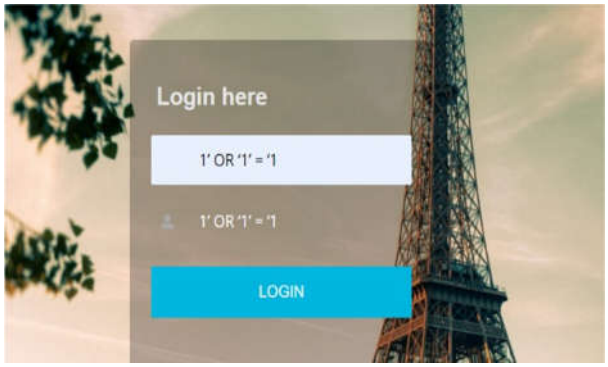


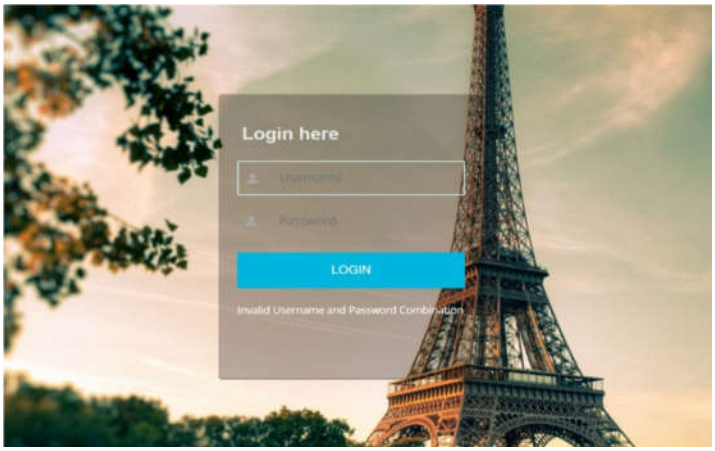
This login module is provided to enter into the website by using login credentials to access the website. The authenticate users can access the wed application with their valid credentials.

VII. RESULTS:


Login here
' or '1'='1
LOGIN


Welcome: abhi
Log out


Login here
1' OR '1' = '1
1' OR '1' = '1
LOGIN


Login here
LOGIN
Invalid Username and Password Combination

CONCLUSION:

In this modern era, with the advancement in technology a greater attention is drawn towards the security threats and its mitigation. An attacker adopts to illegal ways for performing operations what they are intended to.This led to the birth of web application security which is nothing but the practices of protecting the web services against the security threats that exploit loopholes that is present in software system. In this paper we have emphasized the widely used attack method by malicious users i.e., SQL injection and a technique to resolve it.

REFERENCES:

[1] X.Fu, X. Lu, B. Peltsverger, S. Chen, G. Southwestern, K. Qian, and S. Polytechnic, "A Static Analysis Framework For Detecting SQL Injection Vulnerabilities" 31st Annual International Computer Software and Applications Conference(COMPSAC 2007), IEEE, ***ISSN:*** *0730-3157, pages Number 1–8. , China ,2007.*

[2] Mei Junjin, "An Approach for SQL Injection Vulnerability Detection" Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations, IEEE computer society, Las Vegas, Pages 1411-1414, April. 2009.

[3] S. Manmadhan ,Manesh T. , "A METHOD OF DETECTING SQL INJECTION ATTACK TO SECURE WEB APPLICATIONS", International Journal of Distributed and Parallel Systems (IJDPS) ,Volume.3, Issue.6, November 2012.

[4] N.S. Ali, A. Shibghatullah, "Protection Web Applications using Real-Time Technique to Detect Structured Query Language Injection Attacks", International Journal of Computer Applications (IJCA), Volume 149, paperNo:6, September 2016.

[5] V. Nithya,,R.Regan, J.vijayaraghavan, " A Survey on SQL Injection attacks, their Detection and Prevention Techniques", International Journal Of Engineering And Computer Science (IJECS), Volume 2 Issue 4 Page No. 886-905, April, 2013.

[6] KuishengWang , Yan Hou ,"Detection Method of SQL injection Attack in Cloud Computing Environment ", IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC),2016.

[7] Rahul Johari, Pankaj Sharma,"A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection", International Conference on Communication Systems and Network Technologies,2012.

[8] Abdelhamid Makiou, YoucefBegriche, Ahmed Serhrouchni,"Improving Web Application Firewalls to Detect Advanced SQL Injection Attacks ", 10th International Conference on Information Assurance and Security,2010.