ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

Detection and Prevention of Attacks from HTTP Server logs

Sandeep Kumar Tiwari, Monika Soni, Saurabh Sharma

Research Scholar, Department of Computer Technology & Applications, Gyan Ganga College of Technology Jabalpur (M.P.), India

Research Scholar, Department of Computer Technology & Applications, Gyan Ganga College of Technology Jabalpur (M.P.), India

India Professor, Department of Computer Science & Engg, Gyan Ganga College of Technology Jabalpur (M.P.), India

ABSTRACT: In Web site hacks are on the rise and pose a greater threat than the broad based network attacks as they threaten to steal critical customer, employee, and business partner information stored in applications and databases linked to the Web. We present an analysis of HTTP traffic in a large-scale environment which uses network flow monitoring extended by parsing HTTP requests the increasing shift towards web applications opens new attack vectors. Traditional protection mechanisms like firewalls were not designed to protect web applications and thus do not provide adequate defence. It is possible for a web site to be visited by a regular user as a normal (natural) visit, to be viewed by crawlers, bots, spiders, etc. for indexing purposes, lastly to be exploratory scanned by malicious users prior to an attack. An attack targeted web scan can be viewed as a phase of a potential attack and can lead to more attack detection as compared to traditional detection methods. In this work, we propose a method to detect attack-oriented scans and to distinguish them from other types of visits. In this context, we use access log files of Apache (or ISS) web servers and try to determine attack situations through examination of the past data and current web logs using timestamps. In addition to web scan detections, we insert a rule set to detect SQL Injection and XSS attacks. Our approach has been applied on sample data sets and results have been analyzed in terms of performance measures to compare our method and other commonly used detection and prevention techniques.

KEYWORDS: Apache Web Logs, HTTP, Timestamp, SQL Injection, XSS Attack, Server Logs

I. INTRODUCTION

In the beginning, computer browsers were used for accessing web applications, but now there are many small devices such as Smartphone, a tablet which is used for accessing web applications. Like the Internet, a web application has become an important component in corporate, public and government sectors. Web applications today are more functional and dynamic and are used on a daily basis for shopping, social networking, and banking, searching queries or locations, booking travel tickets or reserving appointments or for web mail. Development of web applications has brought some serious web vulnerabilities which have caused potential damage to person, organizations or governments. Modern web applications are database-driven. Web applications support features such as login, registration, online payment, and billing address. In order to access these features, the client must submit personal and confidential information such as name, username, bank account number, social security number, password, credit card number, and address that are stored in the database of the application. Attacks on these kinds of systems cost not only losing credentials, but also misuse of them. For example, if an attacker gets a username and password of a government employee, he or she can easily steal confidential government data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

.

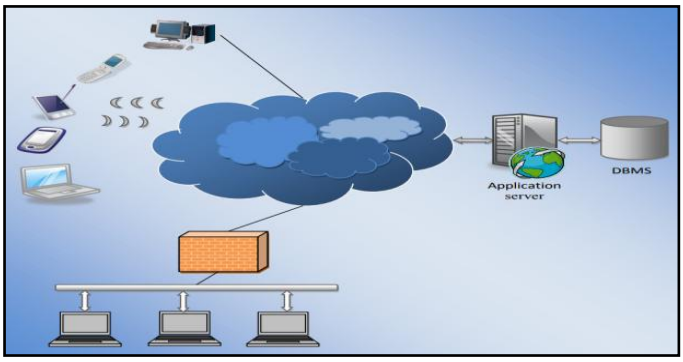

Figure 1.1 General Web Architecture

Intrusion Detection Systems (IDS), though a new field of research, has attracted significant attention towards itself and presently almost every day more researchers are engaged in this field of work. The current trend for the IDS is to make it possible to detect novel network attacks. The major concern is to make sure that in case of an intrusion attempt, the system is able to detect and to report it. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defence that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defence system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

II. WEB INTRUSION DETECTION

Web application design, programming, and maintenance require a different skill set. Even if you have the skills, in a typical organization these tasks are usually assigned to someone other than a system administrator. But the problem of ensuring adequate security remains. This final chapter suggests ways to secure applications by treating them as black boxes and examining the way they interact with the environment. The techniques that do this are known under the name intrusion detection. Attacks detected by IDS/IPS:
Intrusion detection has been in use for many years. Its purpose is to detect attacks by looking at the network traffic or by looking at operating system events. The term intrusion prevention is used to refer to systems that are also capable of preventing attacks. Today, when people mention intrusion detection, in most cases they are referring to a network intrusion detection system (NIDS). An NIDS works on the TCP/IP level and is used to detect attacks against any network service, including the web server. The job of such systems, the most popular and most widely deployed of all IDSs, is to monitor raw network packets to spot malicious payload. Host-based intrusion detection systems (HIDSs), on the other hand, work on the host level. Though they can analyze network traffic (only the traffic that arrives to that single host), this task is usually left to NIDSs. Host-based intrusion is mostly concerned with the events that take place on the host (such as users logging in and out and executing commands) and the system error messages that are generated.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

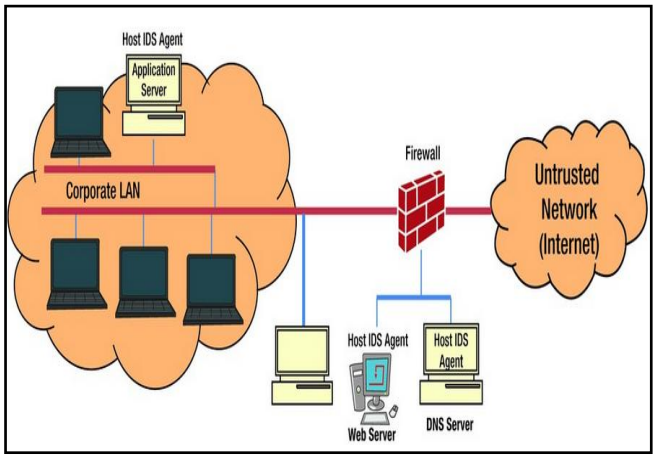

Figure 1.2 Host-Based Intrusion Detection Systems

An HIDS can be as simple as a script watching a log file for error messages. Integrity validation programs (such as Tripwire) are a form of HIDS. Some systems can be complex: one form of HIDS uses system call monitoring on a kernel level to detect processes that behave suspiciously.

Because many NIDSs are in place, a large effort was made to make the most of them and to use them for web intrusion detection, too. Though NIDSs work well for the problems they were designed to address and they can provide some help with web intrusion detection, they do not and cannot live up to the full web intrusion detection potential for the following reasons:

- NIDSs were designed to work with TCP/IP. The Web is based around the HTTP protocol, which is a completely new vocabulary. It comes with its own set of problems and challenges, which are different from the ones of TCP/IP.
- The real problem is that web applications are not simple users of the HTTP protocol. Instead, HTTP is only used to carry the application-specific data. It is as though each application builds its own protocol on top of HTTP.
- Many new protocols are deployed on top of HTTP (think of Web Services, XML-RPC, and SOAP), pushing the level of complexity further up.
- Other problems, such as the inability of an NIDS to see through encrypted SSL channels (which most web applications that are meant to be secure use) and the inability to cope with a large amount of web traffic, make NIDSs insufficient tools for web intrusion detection.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

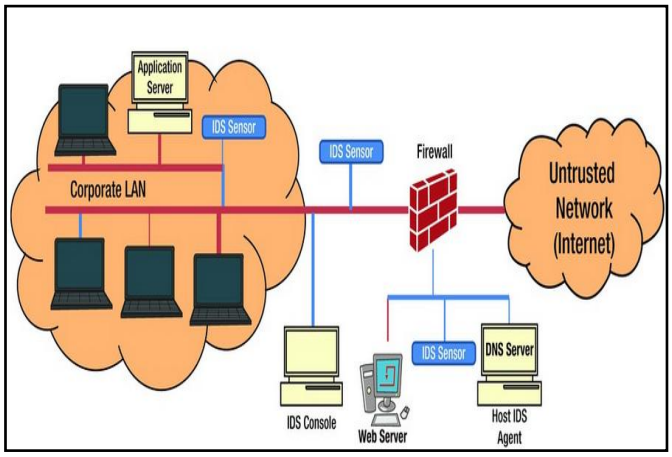

Figure 1.3 Network-Based Intrusion Detection and Prevention System

Vendors of NIDSs have responded to the challenges by adding extensions to better understand HTTP. The term *deep-inspection firewalls* refers to systems that make an additional effort to understand the network traffic on a higher level. Ultimately, a new breed of IDSs was born. *Web application firewalls* (WAFs), also known as *web application gateways*, are designed specifically to guard web applications. Designed from the ground up to support HTTP and to exploit its transactional nature, web application firewalls often work as reverse proxies. Instead of going directly to the web application, a request is rerouted to go to a WAF first and only allowed to proceed if deemed safe.

Web application firewalls were designed from the ground up to deal with web attacks and are better suited for that purpose. NIDSs are better suited for monitoring on the network level and cannot be replaced for that purpose.

Pros and Cons of HIDS and NIDS

- Don’t leave sensitive data in plaintext
- Encrypt private/confidential data being stored in the database.
- This also provides another level of protection just in case an attacker successfully exfiltrates sensitive data.
- Limit database permissions and privileges
- Set the capabilities of the database user to the bare minimum required.
- This will limit what an attacker can do if they manage to gain access.
- Avoid displaying database errors directly to the user
- Attackers can use these error messages to gain information about the database.
- Use a Web Application Firewall (WAF) for web applications that access databases. Provides additional levels of protection and mitigation against XSS attempts.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

IDS Type	Pros	Cons
Host IDS	Protects from attacks at the host level No Bandwidth Impact	Impacts host resources – CPU, memory Operating System dependent One agent can protect one host only
Network IDS	Protects network and network resources Protects against DoS attacks	Sensor hardware is process intensive Prone to false positives.

Table 1.2 Pros and Cons of HIDS and NIDS

III. PREVENTION OF WEB ATTACKS

3.1 Prevent Cross-Site Scripting Attacks

The following suggestions can help safeguard your users against XSS attacks:

i. Sanitize user input:

- Validate to catch potentially malicious user-provided input.

3.2 Prevent SQL Injection Attacks

- The following suggestions can help prevent an SQL injection attack from succeeding:
- Don't use dynamic SQL
- This provides protection to web-facing applications.
- It can help identify SQL injection attempts.
- Based on the setup, it can also help prevent SQL injection attempts from reaching the application (and, therefore, the database).
- Avoid placing user-provided input directly into SQL statements.
- Prefer prepared statements and parameterized queries, which are much safer.
- Stored procedures are also usually safer than dynamic SQL.
- Sanitize user-provided inputs
- Properly escape those characters which should be escaped.
- Verify that the type of data submitted matches the type expected.
- Encode output to prevent potentially malicious user-provided data from triggering automatic load-and-execute behaviour by a browser.

IV. PROPOSED ARCHITECTURE

In computer network, both service providers and clients should secure the resources from malicious attacks by unauthorized elements. As it is a requirement for networks environment to have Intrusion Detection and Prevention System to detect attacks on their services. The proposed intrusion detection and prevention system is host based Intrusion detection system (HIDS). This system is based on client's events monitoring process on server system. To implement the system, we are using virtualization software for deploying server over the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

Linux operating system. That complete virtualization is implemented on the windows operating system, which serves as the host operating system for Linux system. In the proposed system, server's logs files are used to analyze the events perform in service provider system or server system. These log files are the activities or events of clients in the network. These log files are analyzed by using rule based analysis in the server in real time. When system finds some malicious activities during log analysis, it generates alerts messages to admin then admin take necessary actions to block the client's system's activities by using IDPS's API.

The proposed framework is designed to show how the modules are integrated into the components and how they interact with each other to efficiently ensure the resilience of the enterprise network against intruders. Detailed below are the proposed design and the components

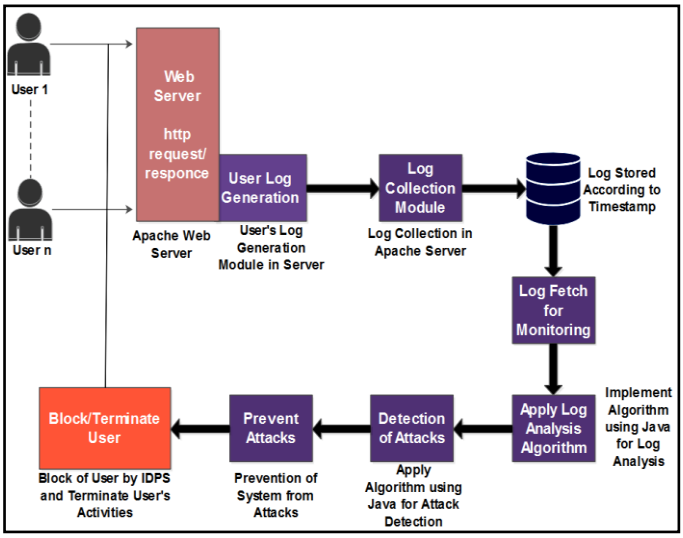

Figure 1.4 Proposed Architecture

V. WORKING STEPS OF PROPOSED METHODOLOGY

1. User request to Apache server for service. Grant server access for services.
2. Server start generate user's logs file for record performed user events and activities.
3. Logs are collected in Log Collection Module in apache web server.
4. User's logs are stored in database for further analysis.
5. Log files are called for log analysis and apply analysis algorithms on fetched logs.
6. Based on log analysis attacks are detected in real time
7. To prevent detected attacks, prevention system is called and based on this system decision will be taken for user connection.
8. If User is found suspicious it's connection will be blocked or terminated by server end to make system safe from attacks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

VI. RESULTS

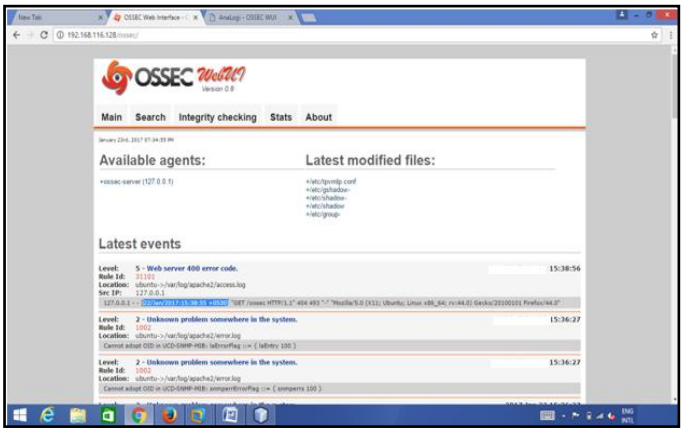

Fig 1.5 Log information captured in real time

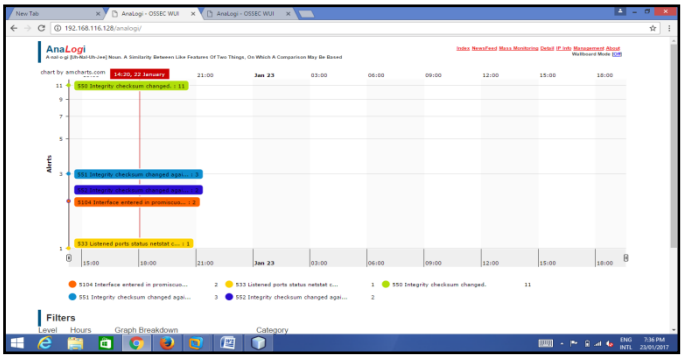

Fig 1.6 Graphical view of current activities in selected time duration

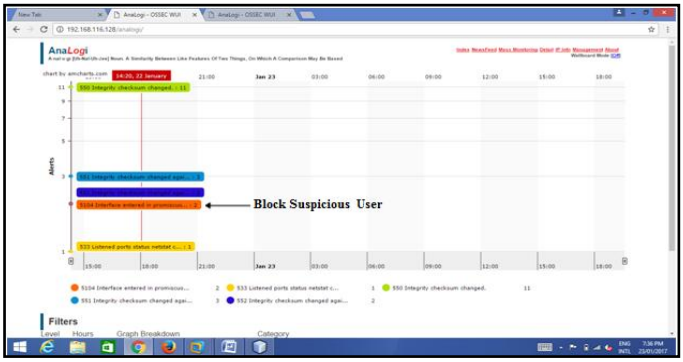

Fig 1.7 Blocked suspicious activities

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

VII. COMPARISON OF EXISTING WORK AND PROPOSED WORK

Parameters	Existing System	Proposed System
Real time analysis	No	Yes
Log data storage system	Only text file	Text file, database
Admin analysis module	No	Yes
Analogy	No	Yes
Analysis interval	Monthly	Every three hours
Precise suspicious alert information	No	Yes
Dependency of External Data Analysis	Yes	No
Type of System Generated Log Data	Unstructured Data	Structured Data
Frequently Used Node's Links Ignorance	Yes (Less Secure)	No (Fully Secure)
Evaluation of Suspicious Nodes	Manually Evaluation	Automatic Evaluation
Data Clustering	Required in Two Steps (Due to Unstructured Data)	Not Required (Structured Data Handling)

Table 5.1 Comparison of Existing Work and Proposed Work

7.1 Comparison Graph of Existing Work and Proposed Work

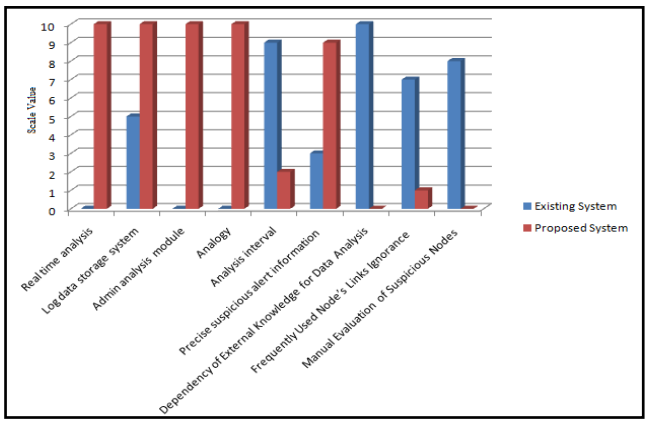

Fig 5.20 Comparison Graph of Existing Work and Proposed Work

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

VIII. CONCLUSION

Various cyber threats have brought about numerous damages ranging from privacy information leakage to financial loss, to leakage of confidential corporate information. Of the cyber threats, APT attacks are particularly known for attacking continuously until they acquire long-time access authority or leak information by successfully intruding specific organizations or institutes. They many challenges for security, since they conduct an attack after sufficiently analyzing the vulnerabilities of a target system. Thus, the proposed system is able to minimize the possibility of initial intrusion and damages of the system by promptly responding through rapid detection of an attack when the target system is attacked. Advanced Persistent Attack is a serious problem in network security. Although there have been several solutions recently proposed to solve the problem, we have analyzed that no solution offers a feasible solution. So, we have proposed an efficient and secure mechanism for detection and prevention of APT attacks that is able to cope up with APT attacks.

Future work should be based on scalable, structured and computationally techniques which do not require prior knowledge, not dependable on security expert to frequently update rules and are able to detect known and unknown attacks.

REFERENCES

1. Louis Marinos, "ENISA Threat Landscape 2015 JANUARY", European Union Agency For Network And Information Security, www.enisa.europa.eu, ENISA Threat Landscape 2015 | January 2016.
2. Danilo V. Bernardo, "Clear and present danger: Interceptive and retaliatory approaches to cyber threats", Applied Computing and Informatics (2015) 11, 144–157, @ Elsevier.
3. Roger Meyer, Detecting Attacks on Web Applications from Log Files, SANS Institute InfoSec Reading Room, © SANS Institute 2008.
4. Muhammet Baykara, Resul Das, "A Novel Hybrid Approach for Detection of Web-Based Attacks in Intrusion Detection Systems", International Journal of Computer Networks and Applications (IJCNA), Volume 4, Issue 2, March – April (2017).
5. Merve Bas Seyyar, Ferhat Özgür Çatak , Ensar Gül, "Detection of attack-targeted scans from the Apache HTTP Server access logs", Applied Computing and Informatics 14 (2018) 28–36.
6. Mohammed A. Saleh and Azizah AbdulManaf, "A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks", Hindawi Publishing Corporation Hindawi Publishing Corporation, Scientific World Journal Volume 2015.
7. Auxilia.M, Tamilselvan.D, "Anomaly Detection Using Negative Security Model in Web Application", 978-1-4244-7818-7/10/$26.00_c 2010 IEEE.
8. Katerina Goseva-Popstojanova, Goce Anastasovski, and Risto Pantev," Classification of malicious Web sessions", 978-1-4673-1544-9/12/$31.00 ©2012 IEEE.
9. Martin Hus´ak, Petr Velan, Jan Vykopal, "Security Monitoring of HTTP Traffic Using Extended Flows", **Conference:** 24-27 Aug. 2015, **IEEE Xplore:** 19 October 2015.
10. Mansour Alsaleh, Abdulrahman Alarifi, Abdullah Alqahtani and AbdulMalik Al-Salman, "Visualizing web server attacks: patterns in PHPIDS logs", Security and Communication Networks
Security Comm. Networks 2015; 8:1991–2003 Published online 22 December 2014 in Wiley Online Library, Copyright © 2014 John Wiley & Sons, Ltd.
11. Niklas Särökaari, "How to identify malicious HTTP Requests", Accepted: 13 November 2012, © 2012 The SANS Institute.
13. Jai Puneet Singh, "Analysis of SQL Injection Detection Techniques", Theoretical and Applied Informatics, Vol 28, No 1&2 (2016).
14. Haibin Hu," Research on the Technology of Detecting the SQL Injection Attack and Non-Intrusive Prevention in WEB System", American Institute of Physics, 020205 (2017).
15. Vrushali S. Randhe, Archana B. Chougule, Debajyoti Mukhopadhyay, "Reverse Proxy Framework Using Sanitization Technique For Intrusion Prevention In Database", CIIT 2013 International Conference, www.researchgate.net/publication, November 2013.
16. Harshad Gaikwad, Bhavesh B. Shah, Priyanka Chatte, "SQLi and XSS Attack Introduction and Prevention Technique", International Journal of Computer Applications (0975 – 8887) Volume 165 – No.2, May 2017.
17. K.A.Varunkumar, M.Prabakaran, Ajay Kaurav2, S.Sibi Chakkaravarthy, "Various Database Attacks and its PreventionTechniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 11 - Mar 2014.
18. Archana Gupta, Dr. Surendra Kumar Yadav, "An Approach for Preventing SQL Injection Attack on Web Application", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 5, Issue. 6, June 2016.