Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 2889-2896
© Research India Publications
http://www.ripublication.com

Prevention of XML based DOS attacks for A secure web service

Ramya.G.Franklin

Asst. Professor Faculty of Computing Sathyabama University
mikella.prabu@gmail.com

Abstract

In a network based information age web services is one of the emerging source for data sharing and access of different data from various domain network. The web service combines various data providers on the basis of request arise in tradition network. The usage of services extends its privacy and authentication to protect web service application from various vulnerable actions. The web service application composed of SOAP, XML and open standards allows communication in all type of networks without the human interaction. The implementation of web service security (WS-security) and WS-attacks is to meet the security challenges in IT framework. Denial of service attacks (DOS attacks) and XML signature wrapping attacks are examined by the execution of penetrating tests like spoofing, XML encryption, and Distributed Authorization models. Secure messaging also enabled to raise the trust factor. In this paper we also introduce Security Assertion Markup Language (SAML), is an open standard data format for authorized communication in different service providers. SAML is one of the OASIS product used to share the security identities of entity in SOA. The security based approach is used for ticket reservation application to enable ease communication and secure web technology.

Keywords:WS- attack, WS-security, SOAP, XML, DOS, SAML, SOA.

I. Introduction

The use of Internet framework leads to the raise of data users and data providers in wide manner. The trust factor and privacy level also increased with the web service usage. To provide the various challenging tasks against attackers in information security services. Also enable real world services to open standards and available SOA web services in dynamic network. Most of the well known organization adopts XML based approach and SOAP messaging to guide their major application. The secure SOA open standards enable the application more secure. The highly authorized organizations provides various security standards for web services but still there is some changeling security tasks like vulnerability, bug, threats, SQL injections integrated with some data providers which affects the trusted and secured web service. E-Messaging, online reservation, E-shopping is some of the applications on web services. WSDL are enabled to define the format of SOAP messaging in web service communication. The service communicates with all providers without any authentication check. UDDI also employed with WSDL to provide new services in real time application without the human interaction. In the Online Ticket booking application the reservation service finds the available information before initiating it. The web service policy listed the user information in UDDI registry to ensure all the entities. Once the service is requested, the UDDI search for capable service providers with user's needs and ensure the (URL) uniform Resource Location to access the service without the human interface. W3C service provider is used to send the web service messages in XML format across dynamic network.

II. Related Study

In recent years web services experience lots of security attacks in network communication. The request and responds are sending by the basis of SOAP messages. The SOAP is not securely defined. The SOAP messages can be view by any interface users in the open network. To protect web service several securing messaging are introduced by ***Christian Manika, JurajSomorosky and JorgSchwenk***(XML, HTTP, SSL, HTTPS, Encryption, WS-Security, SAML).

The weakness in the secure messaging leads to various attacks in web service Technology. The study on security risks provides web service for secure authentication. The penetration testing is discussed by***Christian Manika, JurajSomorosky and JorgSchwenk*** 's new approach of penetrating tools.

Chen-Yu Lee, Ching-Ru Chen,Hsing Lin, Jung-Chun Liu, introduce the detection of various soap attacks.

Application attacks are direct attack encountered on data bases or in authentication process. The interactions in web application are designed with low- level API. (***S. Cantor, J. Kemp, R. Philpott, and E. Maler***)The output and results are dynamically generated to the user's data set which is easy to attack and anyone can alter the document present in the specific applications.

The attacks on web service are common security issue that halts entire network from the communication. To improve the efficiency of network and data base WS- security is enabled on the typical HTTP. WSDL scanning, IP snooping are also studied to prevent various attacks(***Luigi Lo Iacono, Nils Gruschka***)

- ***Modified Message***: An attacker can update, alter, deletes or change the information of message content to be delivered
- ***Unauthorized user***: An unauthorized person views the information disclosed in the message body.
- ***Bugs***: Attacker can send the Bugs or false messages to the user and make them to believe the message is send form sender side.
- ***Third party***: Attacker between the client and server can view and interrupt the all the contents.
- ***Address spoofing***: An Attacker sends the request to the server or user with the defined message and IP format.
- ***Denial of service***. An Attacker makes the network or message unavailable to the user.

III. Proposed System

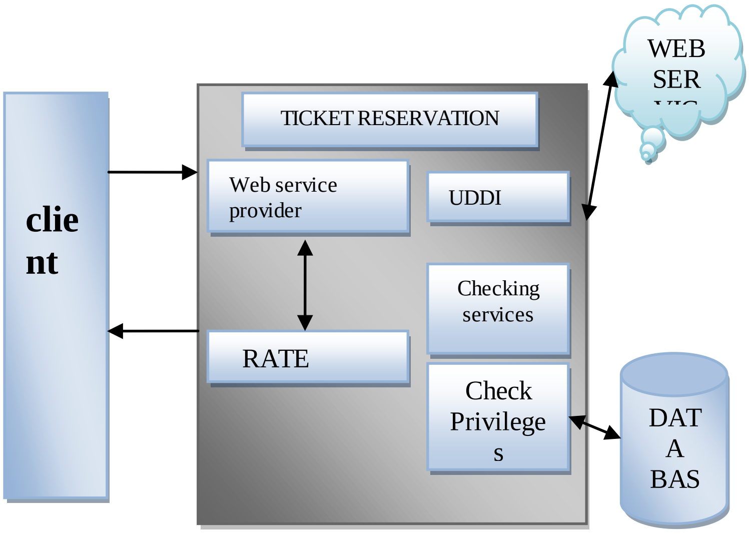
To overcome the security issues secure standards protocols are used for the communication. Cryptographic keys and certificate tokens are also introduced to check the authentication. Sandboxing is an additional feature added with Java and.Net platform to differentiate actions from the operating system. Well tested tools are implemented for developer's team for secure frame work. WS- service access policies and protocol bindings are introduced to protect XML form DOS attacks.

In the reservation process the service providers sends the request to the source to check the predictions provided by the clients. The reservation service must checks for the user credit details and account details provided by the bank by send the SOAP request. After checking the sufficient balance the reservation provider response to the client's request and determine whether the ticket is booked or not.

The process is followed as

- The user sends a SOAP request to the service provider to check the availability of tickets and also sends the registration request.
- The service provider sends the SOAP response to the user after checking the user's basic information and credit details.
- After getting the response from service provider the user now capable to access the various services provided by the reservation side by Admin(User login, Movie selection, movie booking, seat selection, movie timing,)
- Once the service is selected by the user the server side turns for Payment option, for this secure payment mode is enabled by sending security code user mobile to conform the payment.

If the server finds any treats or attacks the server stops the payment transaction and blocks the user.

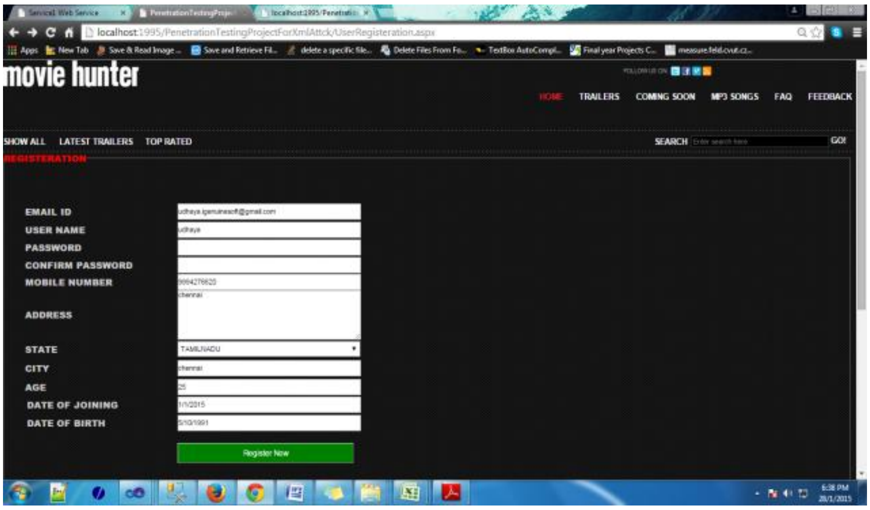


Web service framework mostly all the consumers faces the risk at the same time and the will not able to access the provider site. The general communication is and request are send in the form of XML quires with the use of HTTP/ HTTPs protocol. The attackers easily implemented the threats from distributed network and make the system fail. To overcome these attacks we build the strong firewalls between the each router and the system server. The firewall is a basic defender which protects the server and also defines the source of attacker's path to block them from rapid attack. The firewall is builds in between the client and server but much better to be placed between routers. The system architecture (3.1) illustrates how the attacker tries to attack the server and how we recover our server by building firewalls.

When the consumer sends the request to server the load balancer checks for the availability of the server. Once the request has been accepted router is enabled to locate the path between consumers and providers. If it finds the request has slow down the provider side, the firewall makes that request to XML vulnerability to check the request against various XML attacks and XML DoS attacks. To overcome this attacks all the requests are sends to the Requesting stack, if it finds positive response the request is forwarded for Response. The system finds the exact IP address and mentions that along with response. The response with IP header is in the Backend server (ie Database). The consumer schedules the request in a data structure framework. The data structure is to track the path of malicious requests. The requests with malicious messages and XML attacks are not included in the data structure quires. These requests are put in waiting list and it will not be processed by the provider. After getting the request the responds also forwarded to consumer to examine the response and deletes the request from the stack list.

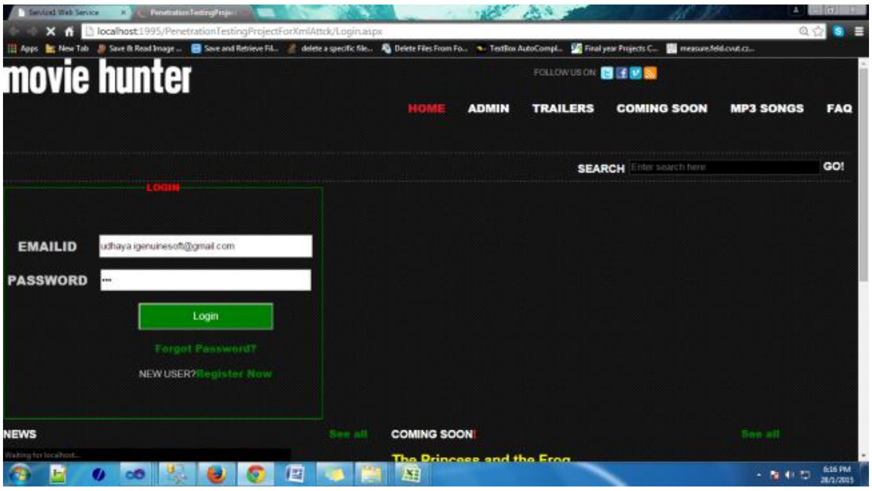
VI. Implementation and Result

In this paper, we implemented the secure tool for DoS attack and attacks on XML encryption. The application is developed in Microsoft.NET framework. All the application access the.NET framework for the subject code security and language security expectation. The libraries also provide all application to check the access policy for IT organizations.



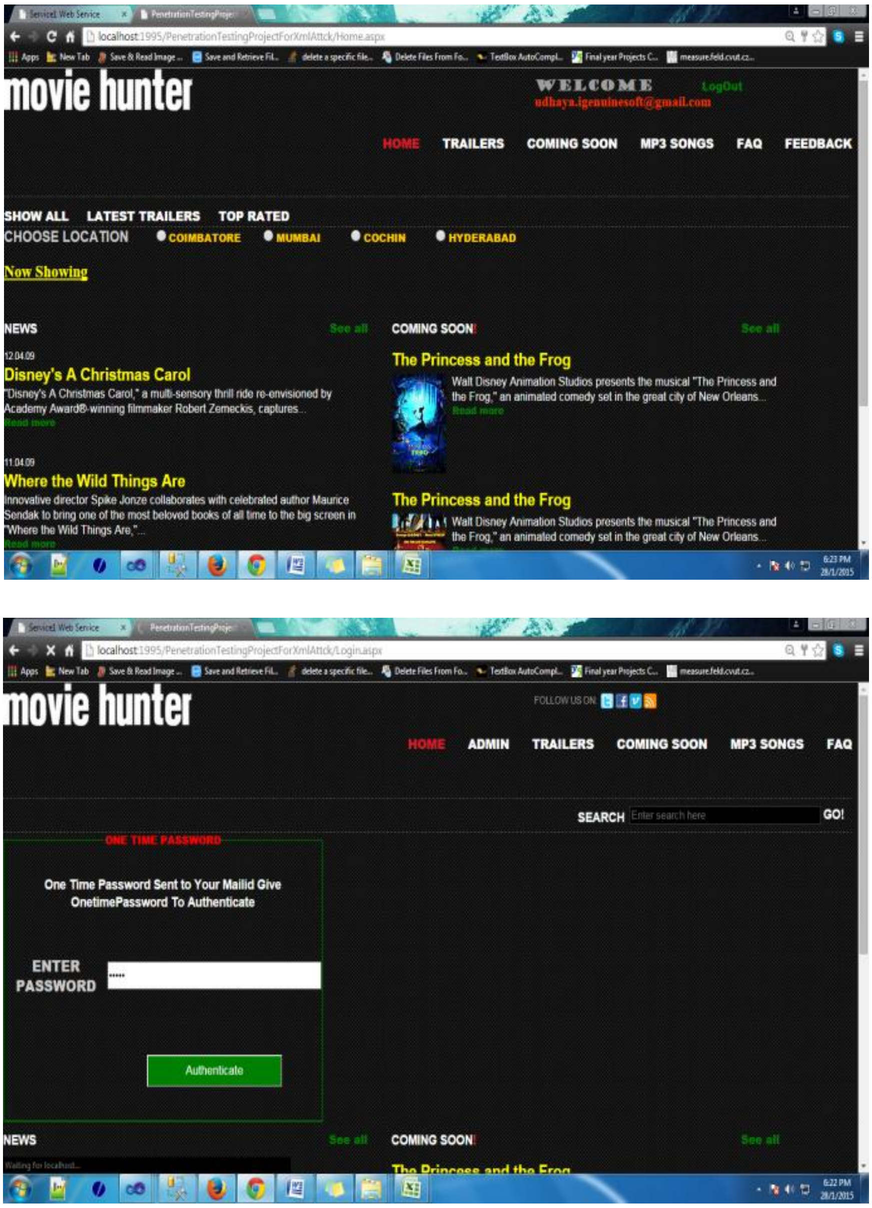
EMAIL ID udhaya.igenuinesoft@gmail.com
USER NAME udhaya
PASSWORD
CONFIRM PASSWORD
MOBILE NUMBER 9994276620
ADDRESS chennai
STATE TAMILNADU
CITY chennai
AGE 25
DATE OF JOINING 1/1/2015
DATE OF BIRTH 5/10/1991

Fig 6.1 Register new User



EMAILID udhaya.igenuinesoft@gmail.com
PASSWORD •••

Fig 6.2 User Login


localhost:1995/PenetrationTestingProjectForXmlAttck/Home.aspx
movie hunter
WELCOME LogOut
udhaya.igenuinesoft@gmail.com
HOME TRAILERS COMING SOON MP3 SONGS FAQ FEEDBACK
SHOW ALL LATEST TRAILERS TOP RATED
CHOOSE LOCATION ● COIMBATORE ● MUMBAI ● COCHIN ● HYDERABAD
Now Showing
NEWS See all
COMING SOON! See all

12.04.09
Disney's A Christmas Carol
"Disney's A Christmas Carol," a multi-sensory thrill ride re-envisioned by Academy Award®-winning filmmaker Robert Zemeckis, captures...
Read more

11.04.09
Where the Wild Things Are
Innovative director Spike Jonze collaborates with celebrated author Maurice Sendak to bring one of the most beloved books of all time to the big screen in "Where the Wild Things Are,"...
Read more

The Princess and the Frog
Walt Disney Animation Studios presents the musical "The Princess and the Frog," an animated comedy set in the great city of New Orleans...
Read more

The Princess and the Frog
Walt Disney Animation Studios presents the musical "The Princess and the Frog," an animated comedy set in the great city of New Orleans...

localhost:1995/PenetrationTestingProjectForXmlAttck/Login.aspx
movie hunter
FOLLOW US ON
HOME ADMIN TRAILERS COMING SOON MP3 SONGS FAQ
SEARCH Enter search here GO!
ONE TIME PASSWORD
Authenticate
NEWS See all
COMING SOON! See all
The Princess and the Frog

One Time Password Sent to Your Mailid Give OnetimePassword To Authenticate

ENTER PASSWORD •••••

Fig6.3 one time password

VII Conclusion

Denial of service attack and attacks on XML encryption is a destructive attack in the common web services. The attacker always waits for the source to place the bugs and threats by using RED and SAML protocols the attackers request is dropped to the stack list for deletion before forwarding that request to the providers. The request is sends from the consumer only when there is no presence of any attacks. It helps to increase the authenticity on rely of messages. For future data duplication will be initiated to prevent to loss of data in the web services communication.

References

[1] Christian Manika,Juraj Somorosky and Jorg Schwenk, “Penetration Testing Tool for Web Services Security,” in ICWS ’12: Proceedings of the IEEE International Conference on Web Services. Los Angeles, USA: IEEE, 2012

[2] Christian Manika,Juraj Somorosky and Jorg Schwenk, “A New Approach towards DOS Penetration Testing on web services,” in ICWS ’13: Proceedings of the IEEE International Conference on Web Services. Los Angeles, USA: IEEE, 2013

[3] M. Gudgin, M. Hadley, N. Mendelsohn, J.-J. Moreau, H. F. Nielsen, A. Karmarkar, and Y. Lafon, “Soap version 1.2 part 1: Messaging framework (second edition),” Tech. Rep., April 2007. [Online]. Available: http://www.w3.org/TR/soap12-part1/

[4] S. Cantor, J. Kemp, R. Philpott, and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard, 15.03.2005, 2005, http://docs.oasis-open.org/security/ saml/.0/saml-core-2.0-os.pdf.v2

[5] Lin Fan et. al. “A Group Tracing and Filtering Tree for REST DDoS in Cloud Computing”, International Journal of Digital Content Technology and its Applications vol 4, Number 9, Dec. 2010.

[6] Dinesh Kumar and Palvinder Singh Mann, “Improving Network Performance and Mitigate Attacks using Analytical Approach under Collaborative Software as a Service(SAAS) Cloud Computing Environment”, IJCST, vol. 2, Issue 1, ISSN: 0976 - 8491, March 2011.

[7] Chen-Yu Lee, Ching-Ru Chen, Hsing Lin, Jung-Chun Liu, “A Detection scheme for flooding attack on application layer based on semantic concept”, IEEE Trans. on Software Eng., Vol.24 (5):376-390, May 2011.

[8] Andrew Clark, Douglas Stebila, Hua Lin, Suriadi Suriadi, “Defending Web services against denial of service attacks using client puzzle”, IEEE Trans. on Cloud Security, Vol.35:400-411, May 2012.

[9] Luigi Lo Iacono, Nils Gruschka, “SOAP message security validation revisited”, IEEE Trans. on Cloud Computing, Vol.26 :276-290, November 2012.

[10] Ansari and A. Belenky, "Tracing multiple attackers with deterministic packet marking (DPM)", Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on, vol.1, no., pp. 49- 52 vol.1, 28-30 Aug. 2003.

AUTHORS' INFORMATION

Ramya G Franklin born in Nagercoil on 03.03.1981. She has completed Masters in Computer Applications from Madras university,Chennai,India in 2004. She has Completed her Masters in Computer science and Engineering from Sathyabama University,Chennai,India in the year 2010.