ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2. Issue 10 October 2013 Page No. 3044-3050

Web Gate Keeper: Detecting Encroachment in Multi-tier Web Application

Sanaz Jafari ***Prof.Dr.Suhas H. Patil (GUIDE)***

Research Scholar Department of computer engineering Bharati Vidyapeeth Deemed University, Pune, India

Head Of the Department of Computer Engineering Bharati Vidyapeeth Deemed University, Pune, India

ABSTRACT

All different types of internet services which are very popular these days in the life of human, now a day's every person's life become nothing without internet services. For fulfilling the user requirements this work on both the ends like front end & back end. On front end user can access to the respective internet services & o back end according to the user requirement the data which is v\useful to the user is provided. This strategy is mainly focus on to detect intrusion in multi-tier web applications. Multi-tier web application include two ends that is front end as well as back end of the applications. The front end include web server which can responsible to run the application and gives that output to back end i.e. file server. This strategy is useful to identify the intrusion at both front end and back end of web application. It is used to monitor the behavior across front end web server and back end database server or file server using IDS. We will also able to detect intrusion in static and dynamic web application. IDS having maximum accuracy and is mainly responsible to identify intrusion.

Keywords - Container Architecture, Container ID, Intrusion Detection System, Pattern Mapping.

1. INRODUCTION

The internet usage & its different applications become the daily need for the human. Internet services helping human to make use of it in very fast access. To solve the problem of fulfilling the requirement of user's requirements for faster data retrieval, the web applications have moved towards multi-tier design where in the back-end server contains the data base and application interface or web server acts as the front end. The excessive use of internet & web based applications invites the attackers to attack. Web Gate Keeper provides Intrusion Prevention Systems at both the end. The prevention logic of our system works on session tracking and control. Through these Web Gate Keeper provides a secure environment for the application.

Web Gate keeper is an intrusion detection system which builds different models of normal behavior for multi-tiered web applications from both front-end web (HTTP) requests and back-end databas (SQL) queries. Unlike previous approaches tha correlated or summarized the alerts for the user ar generated by independent IDS's, Web Gate Keepe makes container-based IDS with Multiple inpu streams to produce alerts. The user who has th authority to access the respective system can use fi amount space which is provided by N-DRA system.

2. COMPARISON OF 3- ARCHITECTURE WITH OTHERS

3-Tier Architecture

A 3-Tier Architecture (3TA) is traditionally used when building web applications. It makes a logical separation between the presentation layer, the business logic layer, and the database layer. For instance, on the Java platform, the presentation layer could be implemented with JSP and JSF, the business layer with session EJB, and the data layer with entity EJB or Hibernate. It is important here to note that the 3TA introduces only a logical separation between layers. The 3 layers together make a given application, which gets deployed on a given server or cluster, and built by a given team. The 3TA can be seen as an implementation of the divide and conquer strategy for the use of the application architect, as it lets him think of his application in term of layers.

Most companies have been implementing applications following the 3TA for years and have now a collection of applications that all behave and look differently, and are hard to integrate. The 3TA introduces a welcome division between the presentation, business logic, and data layer, but is damageable in the sense that it leads architects to think in term of application silos.

Three-tiered architectures fully insulate clients from business rules, the underlying data storage, and concurrency issues, resulting in complete encapsulation. Because clients only interact with three-tiered architecture, changes can be made in the database without having to touch a single line of code at the client.

- Applications have an open architecture and are fully scalable.
- Applications built with three-tiered architecture are also much more maintainable. The architecture separates responsibility into loosely coupled layers (i.e., user interface, three-tiered architecture, and data storage). Because of this separation of responsibility applications can be modified more easily when the business needs change. Thin clients that run on the new network computers or on other devices such as mobile phones, or TV boxes, can be more easily implemented. The client needs contain only user interface code. All business logic and data storage code resides on other machines across the network.
- Data transfer between tiers is part of the architecture. Protocols involved may include one or more of SNMP, CORBA, Java RMI, .NET Remoting, Windows Communication Foundation, sockets, UDP, web services or other standard or proprietary protocols. Often middleware is used to connect the separate tiers. Separate tiers often (but not necessarily) run on separate physical servers, and each tier may itself run on a cluster.

Service Oriented Architecture

The Service Oriented Architecture (SOA) builds on top of the 3TA and addresses its shortcomings. Instead of looking at the IT infrastructure as set of application silos, SOA looks at a set of services and applications. Services implement some kind of functionality and are used by applications and other services. Services communicate between each other and with applications by exchanging XML documents. Comparing SOA to 3TA, SOA applications correspond to the 3TA presentation layer, while SOA services correspond to the 3TA business logic and data layers.

With SOA, all the complexity of the system is encapsulated in coarse grained services and applications are kept extremely simple. In fact, the only concern of applications is to display XML data they get from services and to send XML data to services based on user input.

3. OUTPUT SCREENS OF THE WEB GATE KEEPER

a) Login Screen:

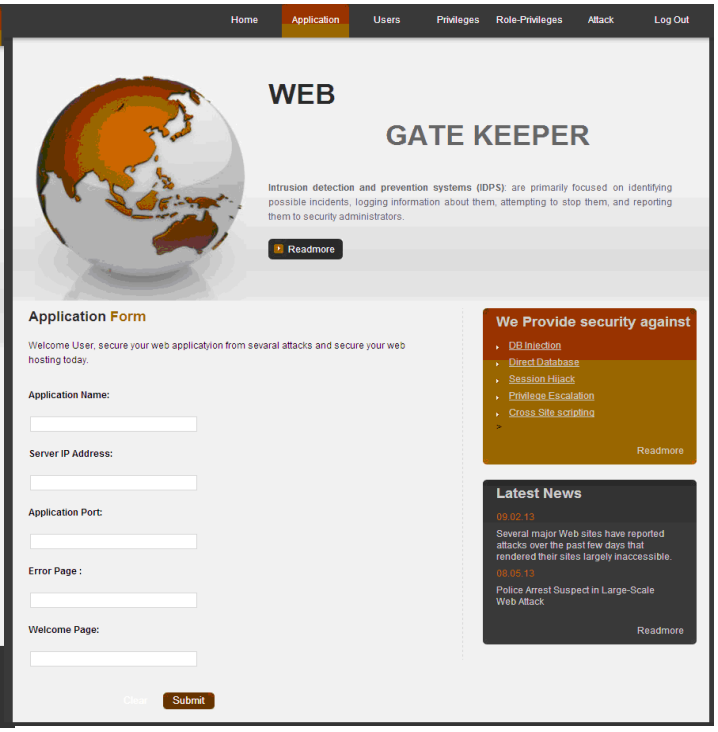
b) Register screen:

c) Forgot Password screen:

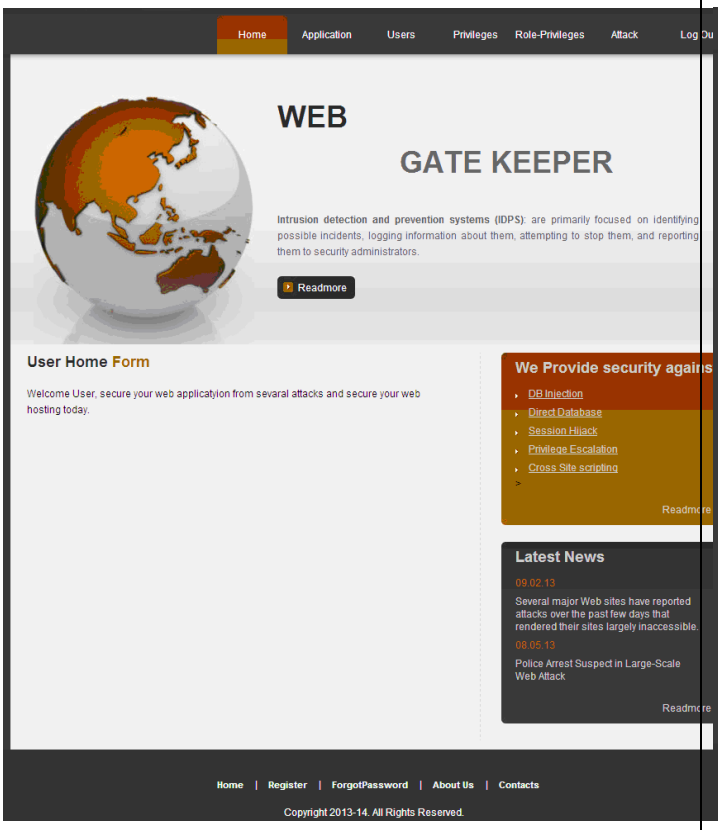
d) About Us screen:

e) Contact Us screen:

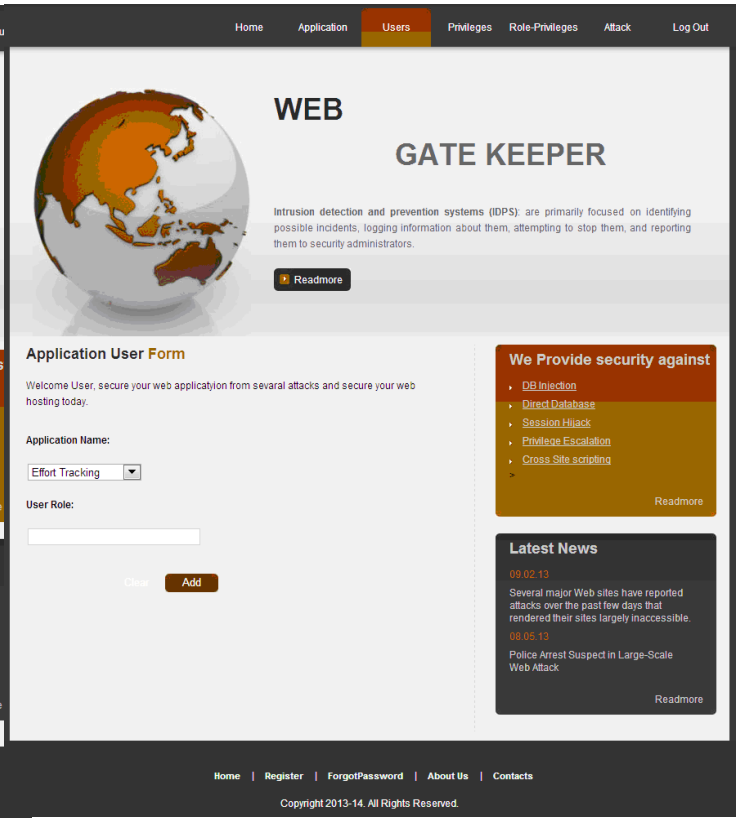
f) User Home Screen:



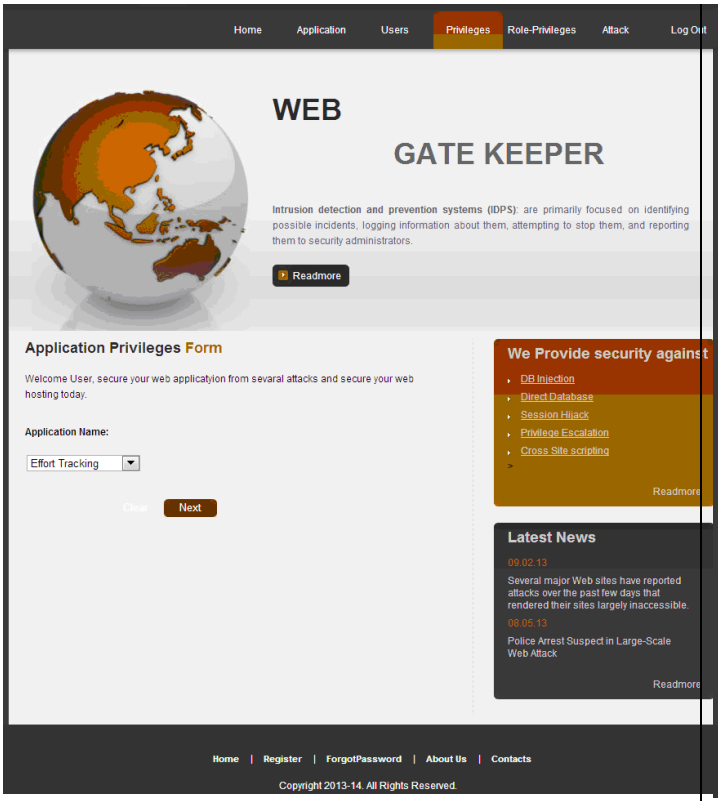
h) Application User Form Screen:

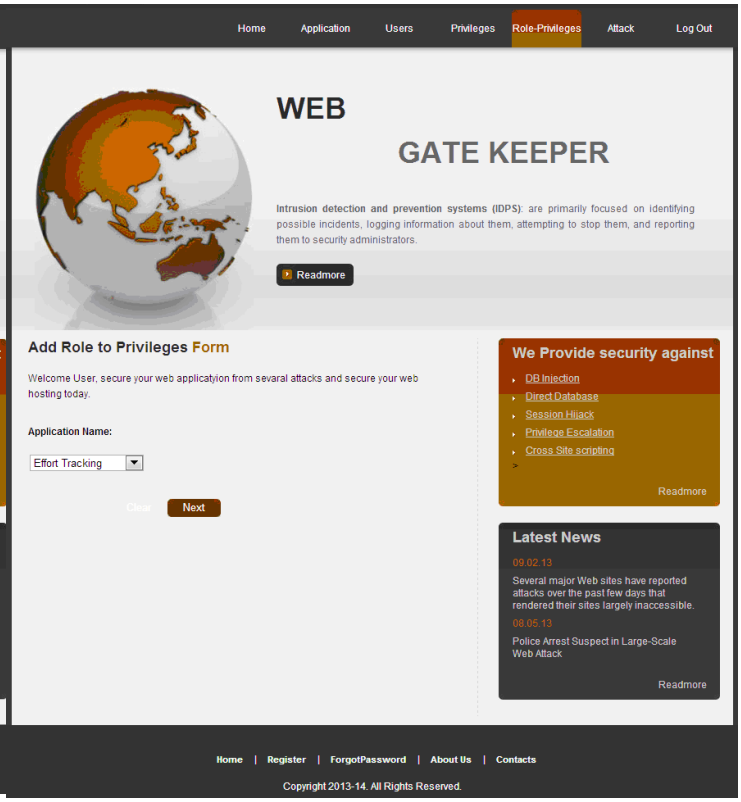


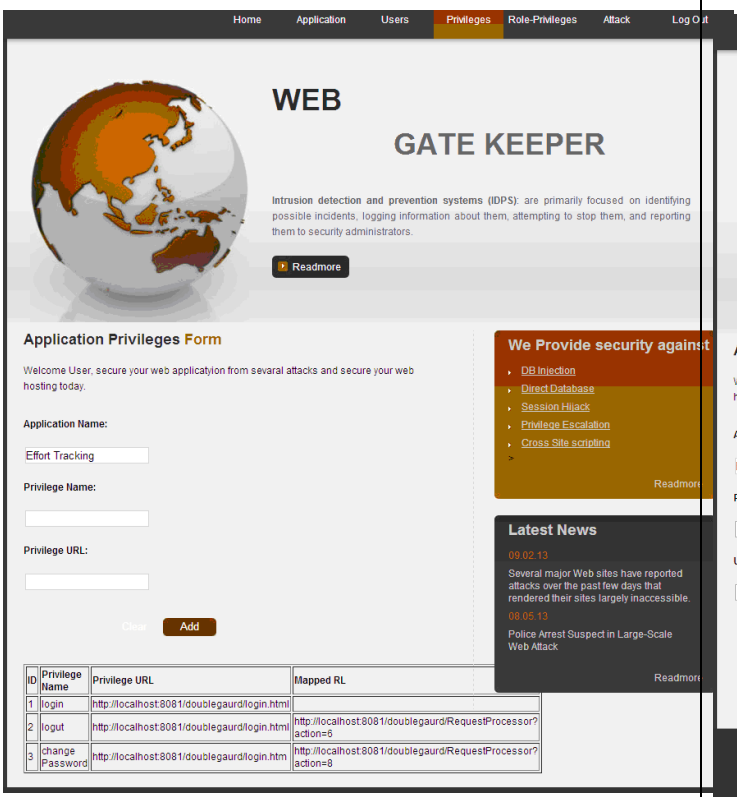
g) Application Form Screen:

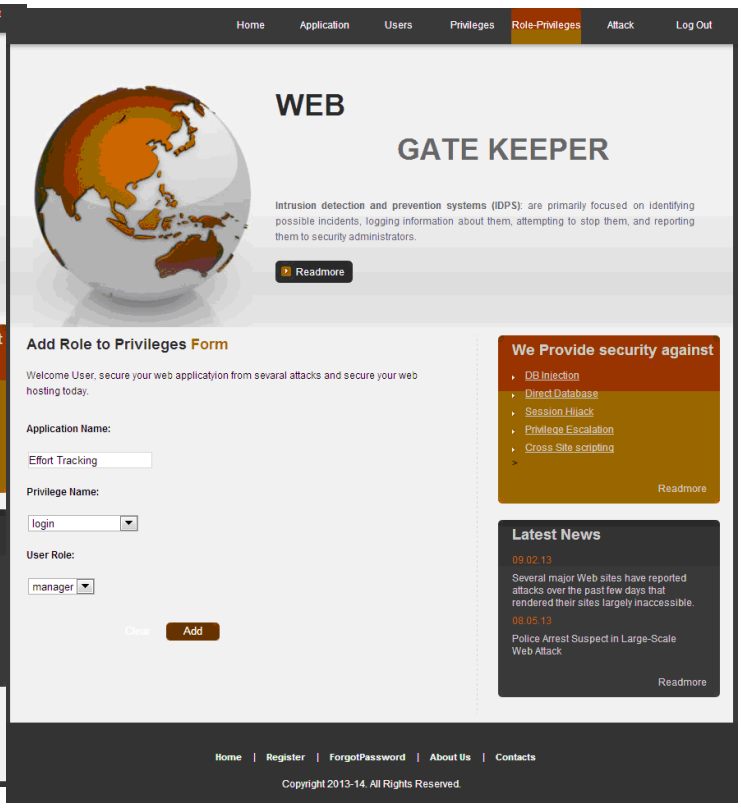


i) Application Privileges Form Screen:





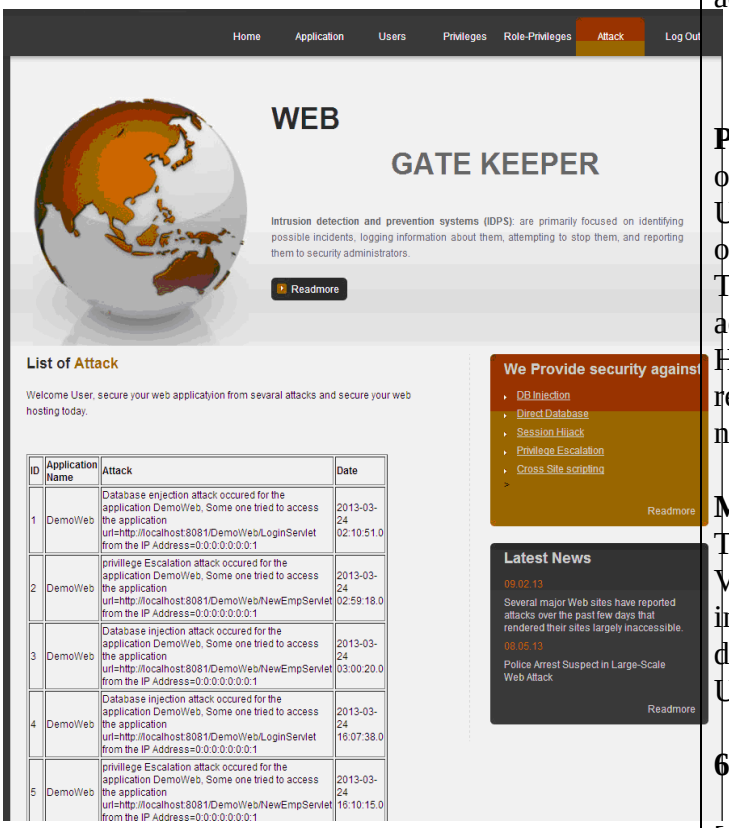




j) Add Roles to Privileges Form Screen:

k) Message Form Screen:

l) List of Attack Screen:



4. MAJOR CONSTRAINTS

- The PC or laptops should have enough memory to accommodate the required software.
- User Interface should be Microsoft standard.
- GUI should be self explanatory.
- Only authorized user can have access to web application on the basis of username and password

5. CONCLUSION

Web Gate keeper is an Encroachment detection system which builds different models of normal behavior for multi-tiered web applications from both front-end web (HTTP) requests and back-end database (SQL) queries. Unlike previous approaches that correlated or summarized the alerts for the user are generated by independent IDSs, Web Gate Keeper makes container-based IDS with Multiple input streams to produce alerts. The user who has the authority to access the respective system can use fix amount space which is provided by N-DRAC system. Web Gate keeper provides easy & fast access to internet services & its applications.

Prof. Dr. Suhas H. Patil is Head of the Department of Computer Engineering of Bharati Vidyapeeth University, Pune, India. He is having rich experience of Computer Engineering and Information Technology. He is having more than 22 years of academic experience. He obtained Ph.D. and M.E. He has published more than 130 research papers in reputed journals and proceedings of international and national conferences.

Miss. Sanaz Jafari is pursuing Master of Technology in Computer Department of Bharati Vidyapeeth University, Pune, India. Her areas of interest are Software Engineering. She is currently doing her thesis work at Bharati Vidyapeeth University, Pune, India.

6. REFRENCES

[1] Meixing Le, AngelosStavrou, Brent ByungHoon Kang," Double Guard: Detecting Intrusions in Multi-tier Web Applications", IEEE Transactions on dependable and secure computing, vol. 9, no. 4, July/ august 2012.

[2] F. Valeur, G. Vigna, C. Kru¨ gel, and R.A. Kemmerer, "A Comprehensive Approach to Intrusion Detection Alert Correlation," IEEE Trans.

Dependable and Secure Computing, vol. 1, no. 3, pp. 146-169, July-Sept. 2004.
[3] Openvz, http://wiki.openvz.org, 2011.
[4] Joomlacms, http://www.joomla.org/, 2011.
[5] http://www.dummies.com/how-to/ content/ examining-differenttypes-Of-intrusion-detection s.html
[6] http://advanced-network-security .blogspot .in/2008/04/threemajor- types-of-ids.html
[7] M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, "Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications," Proc. Int'l Symp. Recent Advances in Intrusion Detection (RAID '07), 2007.
[8] Karen scarfone,Petermell,"Guide to Intrusion Detection and Prevention Systems (IDPS)" , NIST National institute of standards & Technology (Technology Administration U.S. Department of commerce , Special Publication 800-94
[9]http://www.omnisecu.com/security/infrastructure-and-emailsecurity/ types-of-intrusion-detection-systems.htm.
[10]http://en.wikipedia.org/wiki/Multitier_architecture#Comparison_with_MVC_architecture.