

Security Enhancement for E-Learning Portal

A. Jalal, Mian Ahmad Zeb

Department of Computer Science
City University, Peshawar, Pakistan

Abstract

This paper describes the security feature of e-learning authentication. The main goal of this research is to achieve authentication to identify legal user. Internet is open for all users to access and share information. Simultaneously, the user hackers are also their, to examine a web application and infrastructure to understand its design, identify the potentially weak aspects, and use these weaknesses to break or exploit the application. Through authentication process, we could overcome the illegal usage of application. We proposed different algorithms for authentication that is RIPEMD -160. RIPEMD-160 capture overall secure authentication.

Keywords — e-Learning, RIPEMD-160, internet, Authentication

1. Introduction

Today internet is the most popular and cheap source of communication throughout the world. It facilitates the people having different comminutes (organizational institutions, educational departments' and other government offices) to convey its message to the people and communicate them. Now People have the access to internet, from home, office, and mobile. Internet have benefits and as well as drawbacks. The main feature that is security with ease, but with the passage of time a lot of other problems have been faced by internet, that are concerned to speed, reliability, feasibility etc. Most of the today's organization use internet for the e-Learning. E-learning most often means an approach to facilitate and enhance learning through the use of devices based on computer and communications technology. Such devices would include personal computers, CD-ROMs, Digital Television, P.D.A.s and Mobile Phones. Communications technology enables the use of the Internet, email, discussion forums, and collaborative software.

While using internet for e-Learning security is the most important feature, because if security is not considered than a lot of problems have to faced by organization. A lot of attacks are accepted by internet, because it is open for all kind data traffic. When an organization use internet to

facilitate its staff and improve its performance, it has the following drawbacks.

- Loss of confidentiality of business information i.e. financial records, strategic planning data, engineering models and prototypes, marketing plans, medical records, as well as inability to guarantee the integrity of such information;
- Loss of availability of mission-critical services i.e electronic mails;
- Exposure of critical data about your information infrastructure that can be used by your adversaries in planning their attacks;
- Legal liability, regulatory liability, or public loss of confidence when your adversaries use one of your computers to carry out attacks against other organizations;
- Vandalism of public information services (such as your public Web site) [1].

While communicating on internet we should consider the following components for reliability, performance, efficiency.

- The network on which we are communicating is reliable and secure
- It is more resilient against the attacker.
- There are procedures for security features like authentication and confidentiality
- The users are also trained to use portal and protect their system and data from the intruders.

According to other researchers, SQL injection or price manipulation [2] attacks could cripple the website, compromise confidentiality, and in the worst cases cause the ecommerce business to shut down completely. Web application vulnerabilities provide the potential for an unauthorized party to gain access to critical and proprietary information, use resources inappropriately, interrupt business or Commit-fraud.

2. Secure Authentication

Web application weaknesses (failure to provide strong authentication) are problematic for the end user to whom they claimed. Prior to accessing a Web application, a server may require the end user to authenticate themselves to identify the user or to determine the user's access privileges. Without such authentication employed, attackers could access to another user's account, view sensitive information or perform unauthorized functions.

To alleviate this risk:

- Employees have strong authentication, such as HTTPS, mean enabled SSL with encrypted credentials.
- Require re-authentication at specified time intervals or movement between Web pages. It avoids the access of interloper to get that hidden password.
- Enforce what authenticated users are allowed to do. Privilege mode defines rights.
- Regularly test authentication and all potential ways to circumvent authentication.
- Implement authorization (access control).

2.1 Session Security and Session IDs

Most Web sites maintain session state to determine access rights or user settings during the user's sessions. When users log in to an application, the Web server issues an identifier to the user known as a session ID. This session ID can be random and also set to expire at the completion of the session. However, the session ID can also be predetermined (or sequential) and persistent (or not set to expire). The server uses the session identifier with associated data with each successive request. Session tokens often are not properly protected allowing attackers to compromise passwords, keys, session cookies, or other tokens that can defeat authentication restrictions and assume other user's identities. For example, the user's session ID is displayed in the URL. Even if authentication is required, it may be possible for a user to authenticate using legitimate credentials, but then change the session ID in the URL line to access another user's data without requiring re-authentication.

To alleviate this risk:

- Assign random, non sequential session IDs and require re-authentication when accessing additional records.
- Protect account credentials and session tokens.
- Require all cookies have an expiration date so that session tokens are only valid for a predetermined period after the last request by the user.
- Change session tokens when the user moves from an SSL-protected resource to a non-SSL-protected resource.

- Invalidate the session token at the server-side when the user logs out.
- Confirm that the session token is non persistent and is never written to the browser's history or cache.

2.2 SQL Injection Vulnerabilities:

Many Web applications don't properly strip user input of unnecessary, special characters or validate information contained in a Web request before using these input directly in SQL queries. SQL Injection is an attack technique that takes advantage of the Web application to extract or alter information from the database. Hackers enter SQL queries or characters into the Web application to execute an unexpected action that can then act in a malicious way. Such queries can result in access to unauthorized data, bypassing of authentication or the shut down of a database even if the database resides on the Web server or on a separate server. Without proper controls in place, attackers can attack back-end components through a Web application. To alleviate this risk:

- Validate user input to ensure only legitimate data is sent to the Web server. Strip user input of and valid special characters before using that input directly in SQL queries. Check input for appropriate/expected length.
- Ensure the application will not process SQL commands from the user.
- Design and program Web applications in a manner that prevents client-supplied values from being treated as SQL syntax.
- Perform strict input validation on any client input.
- Apply default error handling.
- Implement logical security at the database level -- specify users, roles, and permissions at the database layer.
- Conduct regular testing and identification of potential SQL injection vulnerabilities. Often the most effective method of locating SQL injection vulnerabilities is by hand. Examine application inputs and insert special characters to understand database query syntax and the responses to such queries. Informative errors pages are displayed by default and often give clues to the SQL query in use.

2.3 Buffer Overflows

Web applications may be vulnerable to buffer overflows, which occur when a program attempts to store more data in a static buffer is designed to manage. The additional data overwrites and corrupts memory, allowing an attacker to insert arbitrary instructions on the Web server or to crash the system. Applications may not adequately prevent the introduction of arbitrary code into the system that could be executed with the administrator privileges of the operating system. For example, a hacker may enter a command-line executable statement, such as legitimate Web site form under the guise of an "http request" to gain access to the Web server. If your security configuration allows, the hacker would receive password file and have access to files, and ultimately access the usernames and passwords, which are stored on the Web server.

To alleviate this risk:

- Identify buffer overflows during testing by entering progressively larger values into form inputs, header and cookie fields.
- Prevent code insertion by unauthenticated sources.
- Validate input field length.

2.4 Cross-Site Scripting (XSS)

Web application can bring an attack to an end-user's browser by using the Web browser of other Web users who are viewing the page. A hacker could create a Web site that takes advantage of a cross site scripting flaw. An unknowing user could visit this hacker's Web site (for example, by clicking on a link within an e-mail they have received from a friend) and the hacker's malicious code could then be executed on the unknowing user's system. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

To alleviate this risk:

- Filter input so end-user data cannot be interpreted as scripted content.
- Perform data integrity checks on data prior to its submission to ensure the data is reasonable.
- When possible, restrict all end-user input to alphanumeric content.

2.5 URL Manipulation

Attacks try to manipulate or access important information, if the application implements GET request to send important parameters on the URL. The parameters can be manipulated to give undesired results.

To alleviate this risk:

The best solution is to avoid sending critical parameters in a query string. In addition, the application should validate the parameters with a session token.

2.6 Remote Command Execution

The most shocking web application vulnerabilities occur when the CGI script allows an attacker to execute operating system commands due to inadequate input validation. This is the most common case with the use of the "system call" in Perl and PHP scripts. Using a command separator and other shell meta characters, it is possible for the attacker to execute commands with the privileges of the web server;

2.7 Denial of service

Again, these kinds of attacks are nothing new, but what is different is they are targeting the application not the operating system. Curphey predicts that there will be a major denial of service attack at the application layer on a major online retailer this year.[4, 5]

3. Web Application Security

To provide security to our web communication, it is necessary that web applications should be secure. The Carnegie-Mellon's has contributed enormously to the development of security practices and frameworks. One of the most important methods they have created is the Security Knowledge in Practice method (or the SKiP method for short). It consists of steps to secure network software, to harden a network (make it difficult to break into), to detect and respond to network intrusions, and then to improve the system based on a review of events [6].

The following steps are included in the SKiP method:

1. Select system software from a vendor and customize it according to an organization's needs;
2. Harden and secure the system against known vulnerabilities;
3. Prepare the system so that anomalies may be noticed and analyzed for potential problems;
4. Detect those anomalies and any other system changes that could indicate evidence of an intrusion;
5. Respond to intrusions when they occur;
6. Improve practices and procedures after updating the system.
7. Repeat the SKiP process as long as the organization needs to protect the system and its information assets.

Internet system proliferated over the last few years and today it is possible to find a suitable solution for any budget size. It is important that not every solution is safe, and must be configured appropriately. One of the important steps is to identify different tasks which system must perform and configure it to fulfill essential functions while eliminating those which are unnecessary or vulnerable. Securing a system is a challenging task. It is often neglected, especially for an administrator. SKiP has recommended the following measures for network administrators [6].

- Eliminate services that are unneeded and insecurely configured.
- Restrict access to vulnerable files and directories.
- Turn off software “features” that introduce vulnerabilities.
- Alleviate vulnerabilities that intruders can use to break into systems.

4. Implementation of Security

Cyber Campus is a centralized learning management system which provides a user-friendly administrating, teaching and learning environment for instructors and learners. Cyber Campus consists of a web server and many client PCs as the interface from which instructors and learners interact with the server via WWW to offer e-learning services. Cyber Campus is an all-in-one web-based teaching and learning education system which integrates components including student management, course management, assessments, classroom allocation, communication, etc, into one complete package solution. It integrates web technology with database systems and provides a user-friendly administrating, teaching and learning environment. The system is designed by using the framework based on Web Content Component Model (WCCM), which is the suitable model of web application that supports maintenance of content oriented web applications [2]. Cyber Campus also implemented the following mechanisms to strengthen the security of the learning portal. These mechanisms include:

MySQL Access Privilege

The primary function of the MySQL access privilege is to authenticate a user connecting from a given host, and to associate that user with privileges on a database such as SELECT, INSERT, UPDATE, and DELETE. The MySQL privilege system ensures that all users may perform only the operations allowed to them. As a user, when they connected to a MySQL server, their identity is determined by the host from which the connection is made and the username is specified. The system grants privileges according to the identity and what the user wants to do. MySQL access control involves two stages [10]:

- Stage 1: The server checks whether the user is even allowed to connect;
- Stage 2: Assuming that the user can connect, the server checks each statement the user issues to see whether the user has sufficient privileges to perform it. For example, if the user tries to select rows from a table in a database or drop a table from the database, the server verifies that the user has the SELECT privilege for the table or the DROP privilege for the database. Different access privileges should be setup for different users to provide better security for the online learning portal. Cyber Campus has classified three access privileges for three different access

users (administrator, instructor and learner). These access privileges are defined depending on specific users and the users are identified by the location of the logon portal.

5. Alternative Security for web application

In addition to the security protections via the database privilege settings and the system access restriction based on the IP setting, Cyber Campus is designed and implemented with a multi-layered security infrastructure. In order to guarantee a secure access to the system, Cyber Campus uses Secure Socket Layer (SSL) to transfer sensitive data such as login name and password over the Internet via HTTPS. The importance of developing trusted certification services is that the service has to support digital signatures and permit users to authenticate the other side with whom they are communicating on the Internet.

In case the unavailability of SSL, the system supports a client's side MD5 function in JavaScript. Thus, instead of sending raw password to the server, the user's password is encrypted at the client's side before transmitting to the server. Raw passwords are not stored in the database; only encrypted passwords are stored and retrieved for comparison during the user authentication. In addition, MD5 is one-way encryption which avoids the raw passwords being stolen from the database. However, the JavaScript MD5 function only works when the JavaScript is enabled in the client's browser.

6. Recommended Authentication

As in case of unavailability of SSL for the security then we should use RIPEMD-160 hash function for the authentication. But still we need security to web application. To achieve strong security have no SSL then RIPEMD-160 would provide strong security than other hash function.

The use of RIPEMD-160 is for the prevention of impersonation and violation of data, this authentication is the assurance that the communicating entity is the one that it claims to be. Different algorithms are used for the authentication of legal users. We used RIPEMD-160 hash function for the authentication. Other hash functions are MD4, MD5 and RIPEMD with different key length. The weaknesses of MD4 are replaced by the MD5, while currently MD5 is becoming insecure one and under attacks. The other versions of RIPMD are 128,256,320. But the strengthened version of RIPEMD-160 and expected to be secure for the next ten years. [3]

Table 1. Comparison of MD5 and RIPEMD-160

	MD5	RIPEMD-160
Digest length	128 bit	160 bits
Basic unit of processing	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	160 (5 paired rounds of 16)
Maximum message size	2^{64}	$2^{64}-1$ bit
Primitive logical function	5	4
Additive constants used	64	9
Endianness	Little endian	Little endian

RIPEMD-160 and SHA-1 are more resistant to Birthday attack but they both showed more resistance in Dos attacks. Although both have bitwise logical operations but it didn't slow the speed than MD5.

7. Overall performance

Providing security to information by secure authentication having no SSL, but only web application that is SKiP method. There is proposal, according to which there should authentication for the legitimate user who can access the data. According to that proposal MD5 is hash function that provide authentication, it is resistant to impersonation and intrusion but through some special kind of hardware this hash function could be broken. So it is not secure one for strong authentication. I propose RIPEMD-160 to be built with in SKiP to provide secure transmission of information over the internet. It is more difficult for intruders to get ride of RIPEMD-160.

In case of availability of SSL with SKiP method to company RIPEMD-160 would make it secure. If method with SSL facility and also RIPEMD-160, then there would be a lot of problem for intruders to break the security lock. Comparison of algorithms showed greater difference with each other. We found that RIPEMD-160 has great advantages over the other hash functions.

Table 2. Results Produced by RIPEMD-160

Algorithm	Word	Cipher Text
RIPEMD-160 (For all small letters)	elearning	075b01f7346526c3a9a57fae798affc17cbc4e85
RIPEMD-160 (Making a minor change in word)	Elearning	39d7a15868186732e0dba87b787b46ac498b20a6
RIPEMD-160 (For mix word)	E-learning	28bdb78a299b5cbe65277ec356a64ea0e137cdd
RIPEMD-160 (Making a minor change in word)	e-Learning	0a7948fbc7abbf7a2bf97fd3af3c11223881a553

8. Conclusion

Internet is not secure source of transmitting information, especially for the online methods. We use web application to provide security to data. For this purpose, we use SKiP method that has the facility of SSL. But in case of unavailability of SSL, vulnerabilities are there to access the secret information. To protect them from intruders, we will use RIPEMD-160 hash function, to provide security to data and keep it secrete. MYSQL also helps to provide security to data by using user privileges.

9. Reference

- [1] CERT Security Improvement Module Deploying Firewalls, <http://www.cert.org/security-improvement/modules/m08.html>.
- [2] C Lim, M Yu, J S Jin. Generic e-learning data structure and Web teaching, 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE 2005), Hong Kong, March 2005, pp 564-569.
- [3] "A. Jalal, Mian Ahmad Zeb", Security and QoS Optimization for Distributed Real time Environment", Proc. of IEEE 7th International Conference on Computer and Information Technology (CIT2007), Japan, 16-19 Oct, 2007.
- [4] "THE TEN MOST CRITICAL WEB APPLICATION SECURITY VULNERABILITIES", OWASP FOUNDATION, 2002-2007.
- [5] "Dangerous, familiar application vulnerabilities top list" By Edward Hurley, News Writer, 27 Jan 2004.
- [6] Five common Web application vulnerabilities Sumit Siddharth, Pratiksha Doshi, April 2006.
- [7] The Learning Group About e-learning Benefits.htm
- [8] Vladimir Dimitrov, Hristo Turlakov, Luben Boyanov, "E-learning System for Course Works", of international workshop NGNT, pp: 57- 65.
- [9] "E-Learning: Benefits" <http://www.learngroup.com.au/cms/default.asp>.
- [10] "Benefits of e-Learning" <http://www.hyperstudy.com/>
- [11] [http://www2.le.ac.uk/institution/merlin/Disadvantages Of e-Learning backlinks](http://www2.le.ac.uk/institution/merlin/Disadvantages%20Of%20e-Learning%20backlinks).