



Università degli Studi "Roma Tre"
Dipartimento di Informatica ed automazione

Facoltà di Ingegneria

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

AUTENTICAZIONE
PER APPLICAZIONI WEB

Relatore
Ing. Paolo Merialdo

Correlatore
Ing. Daniela D'Aloisi

Candidato
Stefano Tortora

Anno Accademico 2002/2003

Indice

Indice.....	5
INTRODUZIONE.....	7
L'AUTENTICAZIONE	11
1.1 Introduzione alle applicazioni Web.....	11
1.2 Il problema dell'autenticazione.....	18
1.3 Protocolli d'autenticazione.....	21
1.3.1 Protocollo PAP.....	22
1.3.2 Protocollo CHAP.....	22
1.3.3 Vantaggi e Svantaggi.....	23
1.3.4 Altri protocolli.....	23
1.3.5 Note finali	26
1.4 Casi d'uso	27
1.4.1 Definizione: Casi d'uso.....	28
L'AUTENTICAZIONE IN SPOCK.....	31
2.1 Introduzione	31
2.2 Autenticazione preesistente.....	31
2.3 Conclusioni.....	34
CREAZIONE DELLA NUOVA AUTENTICAZIONE	36

3.1	Introduzione	36
3.2	Casi d'uso di SPOCK	37
3.2.1	Autenticazione	39
3.2.2	Cambia Password	43
3.2.3	Un altro esempio: Seleziona Risorse	46
3.2.4	Profili delle classi di SPOCK	49
3.3	Scelta degli strumenti appropriati	52
3.3.1	Perché Java.....	52
3.3.2	Perché PHP.....	53
3.3.3	Scelta finale	53
3.4	Nuova autenticazione	55
3.4.1	Modifica della precedente autenticazione.....	55
3.4.2	Innovazioni	60
3.5	Note conclusive	70
MODIFICHE E MIGLIORAMENTI DI SPOCK.....		73
4.1	Introduzione	73
4.2	Modifiche.....	74
Conclusioni		76
BIBLIOGRAFIA.....		79

INTRODUZIONE

Il lavoro descritto è consistito nella realizzazione di una procedura di autenticazione per un'applicazione web di grandi dimensioni: il sistema SPOCK.

SPOCK (Sistema per la Pianificazione, l'Organizzazione e il Controllo) è un sistema sviluppato internamente alla Fondazione Ugo Bordoni, dove questa tesi è stata svolta, per la gestione dei propri progetti.

Il suo scopo è quello di offrire un supporto nella stesura, aggiornamento, modifica e gestione dei progetti e della modulistica allegata.

L'intera applicazione SPOCK è stata realizzata attraverso l'utilizzo del linguaggio di programmazione PHP¹ immerso in codice HTML²; sono presenti anche alcuni programmi javascript. I dati su cui SPOCK lavora sono mantenuti in un database MySQL³. L'integrazione tra HTML, PHP e MySQL è piuttosto diffusa nelle applicazioni *web-based*, grazie alla facilità con la quale si riesce ad interagire programmando in PHP con database di questo genere.

La precedente procedura d'autenticazione presente in SPOCK era abbastanza inefficiente e poco sicura. Era scaturita quindi la necessità di una nuova metodologia. Il tema principale che ha accompagnato lo svolgimento del tirocinio è stato quello della sicurezza.

¹ PHP sta per: Hypertext Preprocessor", è un linguaggio di scripting general-purpose Open Source molto utilizzato; è specialmente indicato per lo sviluppo Web e può essere integrato nell'HTML. La sua sintassi è basata su quella di C, Java e Perl. L'obiettivo principale del linguaggio è quello di permettere agli sviluppatori web di scrivere velocemente pagine web dinamiche.

² È bene precisare che l' HTML non è un linguaggio di programmazione ma un semplice sistema di contrassegno, i cui tag vengono riconosciuti ed interpretati dai browser Web.

³ MySQL è un DBMS basato su SQL, linguaggio per database più utilizzato al mondo.

SPOCK è stato il sistema su cui si è applicata la procedura di autenticazione oggetto del lavoro di questa tesi. Lo scopo primario è stato quello di progettare una metodologia di autenticazione per sistemi basati su web che fosse sicura e riusabile. Il lavoro della tesi è stato quindi quello di dar vita ad un modello per la creazione di sistemi di autenticazione per qualsiasi applicazione web, fosse essa disponibile in internet o in intranet.

La sicurezza, che non era stata considerata nella versione precedente di SPOCK, è diventata uno dei requisiti fondamentali da rispettare.

La tesi è stata così suddivisa: nel primo capitolo, dopo un'introduzione sulle applicazioni web, sono affrontati sia il problema dell'autenticazione sia i modi per determinare quale è la forma d'autenticazione più consona per il sistema che si deve sviluppare in base a dei parametri quali il livello di sicurezza richiesto, il budget disponibile e così via. E' in seguito fatta un'introduzione su un metodo utilizzato per comprendere meglio le specifiche richieste dall'utente e facilitare la fase di programmazione del sistemista e vale a dire i casi d'uso.

Nel secondo capitolo è testata e analizzata la precedente autenticazione e nel dettaglio è descritto come è stata creata e realizzata la sua architettura.

Nel capitolo successivo è invece introdotta la nuova autenticazione; nella prima parte sono sviluppati tre casi d'uso: il primo, per ovvi motivi, riguarda l'autenticazione; il secondo riguarda l'operazione di cambio password, essendo anche questa critica; il terzo invece descrive un'operazione tipica che un utente connesso a SPOCK dovrà affrontare. È stato scelto l'inserimento di questa terza operazione per far capire quali effettivamente siano le specifiche richieste e il metodo utilizzato dal sistema per affrontare questo tipo di operazioni. Segue, quindi, l'analisi di tutti i passi che erano stati affrontati nel precedente capitolo cercando, ove possibile, soluzioni migliori e spiegando

come sono state attuate. Per ultimo sono trattati i passi che non erano stati in precedenza affrontati e spiegati nel dettaglio.

Nell'ultimo capitolo sono state prese in considerazione tutte quelle modifiche apportate a SPOCK che però non riguardavano direttamente l'autenticazione; il lavoro fatto in questa sezione è stato quello d'aggiornare parti del sistema in modo che risultasse più incline possibile a modifiche e aggiornamenti.